THE GUIDE TO SANCTIONS

FOURTH EDITION

Editors
Rachel Barnes KC, Paul Feldberg, Anna Bradshaw, David Mortlock, Anahita Thoms, Wendy Wysong and Ali Burney

The Guide to Sanctions

The Guide to Sanctions

Fourth Edition

Editors

Rachel Barnes KC

Paul Feldberg

Anna Bradshaw

David Mortlock

Anahita Thoms

Wendy Wysong

Ali Burney

Published in the United Kingdom by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.globalinvestigationsreview.com

Enquiries concerning reproduction should be sent to: insight@globalinvestigationsreview.com.
Enquiries concerning editorial content should be directed to the Publisher –
david.samuels@lbresearch.com

ISBN 978-1-80449-256-7

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

Akrivis Law Group, PLLC

Baker & Hostetler LLP

Baker McKenzie

Barnes & Thornburg LLP

BDO USA, PA

Bonifassi Avocats

Cravath, Swaine & Moore LLP

Dechert LLP

Eversheds Sutherland

Forensic Risk Alliance

Global Law Office

Jenner & Block LLP

Linklaters LLP

McGuireWoods LLP

Miller & Chevalier Chartered

Navacelle

Peters & Peters Solicitors LLP

Ropes & Gray LLP

Steptoe & Johnson

Sullivan & Cromwell LLP

Three Raymond Buildings

Willkie Farr & Gallagher LLP

Publisher's Note

The Guide to Sanctions is published by Global Investigations Review (GIR) – the online home for everyone who specialises in investigating and resolving suspected corporate wrongdoing.

When this Guide was launched, I wrote that we were living in a new era for sanctions: more countries were using them, with greater creativity and (occasionally) self-centredness. I had no idea how true this statement would prove to be. Recent events have supercharged their use, to the point where sanctions never sleep. And that was before Russia invaded Ukraine . . .

Sanctions have become everybody's go-to tool. And little wonder. They are powerful; they reach people otherwise beyond reach. They are easy – they can be imposed or changed at a stroke, without real legislative scrutiny. And they are cheap for governments (as in the cost of making them versus their wider impact); once they exist, others do all the real heavy lifting.

It is on the heavy lifting part where this book can help. The pullulation of sanctions regimes, and sanctions, has created day-to-day headaches and challenges for all nearly all businesses and their advisers. Hitherto, no book has addressed this complicated picture in a structured way. *The Guide to Sanctions* corrects that by breaking down the main sanctions regimes and some of the practical problems they create.

For newcomers, it will provide an accessible introduction to the territory. For experienced practitioners, it will help them stress-test their own approach. And for those charged with running compliance programmes, it should help them to do so even better. Whoever you are, we are confident this book has something for you.

The Guide is part of the GIR technical library, which has developed around the fabulous *Practitioner's Guide to Global Investigations* (now in its fifth edition). *The Practitioner's Guide* tracks the life cycle of any internal investigation, from discovery of a potential problem to its resolution, telling the reader what to think

about at every stage. You should have both books in your library, as well as the other volumes in GIR's growing library – particularly our *Guide to Monitorships* and our new book on money-laundering and anti-money laundering regimes.

We supply copies of all our guides to GIR subscribers, gratis, as part of their subscription. Non-subscribers can read an e-version at www.globalinvestigationsreview.com.

I would like to thank the editors of *The Guide to Sanctions* for shaping our vision (in particular, Paul Feldberg, who suggested the idea), and the authors and my colleagues for the elan with which it has been brought to life.

We hope you find the book enjoyable and useful. And we welcome all suggestions on how to make it better. Please write to us at insight@globalinvestigationsreview.com.

David Samuels
Publisher, GIR
September 2023

Contents

Foreword

The term 'sanctions' is not new. The 90s have been called the 'decade of sanctions' of the UN Security Council. Today we are observing the unprecedented expansion of economic, financial, trade, cyber, targeted, individual and other types of sanctions (restrictive measures) applied by states and regional organisations unilaterally without the authorisation of the UN Security Council. Compliance with unilateral sanctions is enforced by multiple tools, including secondary sanctions exposure, criminalisation of sanctions circumvention and maximum pressure campaigns. Pecuniary penalties as a result of civil charges, even after securing settlement agreements with the US Office of Foreign Assets Control, may reach billions of US dollars.

Complicated, confusing and overlapping sanctions regulations, the proliferation of penalising mechanisms, the high risk and severity of penalties, unclear, lengthy, costly and complicated licensing procedures, uncertainties around the scope of humanitarian carve-outs, broad interpretations of the sanctions regimes, complications in delisting procedures and high legal costs all heighten risks and result in the growing de-risking and over-compliance by all actors in sanctioning, sanctioned and third countries.

It is a principled position of the mandate that any unilateral measures can only be taken by states and regional organisations without the authorisation of the UN Security Council if they fully correspond to criteria of countermeasures or retortions under the law of international responsibility. Any other measures qualify as unilateral coercive measures and are illegal under international law. These unilateral measures, independent of their legality, also have enormous humanitarian effects, which are often neglected or considered to be unintended by the sanctioning parties.

At the same time, as a Special Rapporteur I receive multiple complaints not only about the direct impact of sanctions but also often of over-compliance with all types of sanctions for many, if not all, of the reasons stated above.

De-risking and over-compliance have negative effects on all nationals or residents of countries under sanctions, often involving discrimination on the grounds of nationality, place of birth, residence, registration, IP address or any other nexus with these countries. It results in the isolation of countries, their companies and individuals, breach of trade and cooperation networks, and creates challenges to, or uncertainties of, access to justice and to remedies for those affected, and thus a lack of accountability.

I can also cite the detrimental effects on all basic human rights arising from impediments to the delivery of goods that are not subjected to sanctions, including those that are explicitly exempted from sanctions regimes via humanitarian carve-outs, such as food, medicine, fertilisers, medical equipment and spare parts, as well as many other goods necessary for the maintenance and development of critical infrastructure, thus rendering humanitarian provisions de facto almost non-existent. Financial institutions, manufacturers and delivery and insurance companies refer to broad and unclear interpretations of sanctions limitations by states or the compliance sector. They also mention the risks involved in delivering goods that may be perceived as 'dual use' (relevant to many types of medicine, rescue equipment and even simple consumer goods such as toothpaste), the impossibility or challenges of bank transfers, insurance or deliveries due to other elements of sanctions regulations, or the simple risk-aversion by refraining from dealing or cutting ties with any actor suspected of, or perceived as, having relations with the country under sanctions.

In particular, multiple reports refer to the challenges of delivering humanitarian assistance to the countries under sanctions even in the course of global public health crises, including the covid-19 pandemic, or epidemics (dengue), or in the aftermath of natural disasters such as earthquakes. They also refer to sanctions-induced challenges of effectively implementing humanitarian resolutions of the UN Security Council. Over-compliance and its serious adverse impact on humanitarian work persist even after the adoption of specific, targeted and often time-limited humanitarian carve-outs, such as those adopted for Syria by the US, UK and EU in response to its catastrophic earthquakes in February 2023 (UN Security Council Resolutions 2664 and 2615).

Information about the scope of international and unilateral sanctions, counter-sanctions, legal regimes of different countries, and legal assessment of, and challenges in, litigation in sanctions cases is often fragmentary or politicised. As a Special Rapporteur I very much welcome reflections and open dialogue on

all aspects relevant to sanctions and their impact, as well as discussions about mechanisms to ensure protection of the rights of all those affected by unilateral measures, analyses on the various challenges pertaining to humanitarian carve-outs and licensing, and mechanisms of litigation, accountability, responsibility and redress.

In terms of the serious practical implications of international and unilateral sanctions, compliance and over-compliance, I believe that the experience and views of practitioners exposed in *The Guide to Sanctions* will contribute to the international ongoing debate around the above-mentioned and other relevant issues.

Alena Douhan
UN Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights
September 2023

Introduction

Rachel Barnes KC, Anna Bradshaw and David Mortlock[1]

Since the publication of the previous edition of this book, we have seen the largest multilateral campaign of economic and trade sanctions since the Second World War, following Russia's invasion of its neighbour Ukraine in February 2022. The sanctions measures imposed on Russia by the coalition of nations led by the EU, the UK, the US and Canada are unprecedented in the modern era. If the aim was to force Russia to change its foreign policy, end its aggression in Ukraine and bring the war to a swift conclusion, these sanctions have so far failed. Central Bank of Russia reserves have been frozen to a value of €300 billion, Russian banks have been excluded from the SWIFT messaging system and Russian military supplies have been significantly impaired – yet the Russian economy contracted by a modest 2.1 per cent in 2022.[2] For 2023, the International Monetary Fund predicts a 1.5 per cent drop in GDP.[3] In the meantime Russia has pivoted away from the G7 and the EU (and their respective currencies) towards China, India, Turkey, the UAE and Iran. Is it simply the case that it will take time for the sanctions to take effect – or are they an ineffective tool? Was a quick resolution and a change of policy an unrealistic goal in the first place and is it the case that the potential power of sanctions instead lies in their consistent application over time? These are questions that can only, if ever, be answered with the benefit of hindsight, but we can at least now begin to collate the trends and developments sparked in sanctions law, policy and practice.

---

1 Rachel Barnes KC is a barrister at Three Raymond Buildings, Anna Bradshaw is a partner at Peters & Peters Solicitors LLP and David Mortlock is a partner at Willkie Farr & Gallagher LLP.

2 www.consilium.europa.eu/en/infographics/impact-sanctions-russian-economy/.

3 www.imf.org/en/Countries/RUS.

Starting with targeted asset freezes, heated debates have arisen on the extent to which sanctions could – or should – result in permanent rather than just temporary deprivation of private property. In most sanctioning countries, there have, at the very least, been calls for the reconstruction of Ukraine to be paid for with frozen funds – including suggestions that the external reserves of Russia's Central Bank be used in the reconstruction effort. As appealing as this idea may sound, it is fraught with legal difficulties. The features that make asset freezes such a powerful legal tool – the ability to adopt measures quickly, based on behaviour that falls short of criminal conduct with minimal evidential thresholds – would no longer be available if assets were not temporarily frozen but permanently expropriated, in compliance with internationally agreed minimum protections for procedural rights. In most (if not all) western jurisdictions, assets can only be confiscated or otherwise 'recovered' by the state if they can be shown to have been acquired through criminal or (at the very least) unexplained conduct or used as an instrument to further unlawful conduct. By contrast, a sanctions asset freeze does not require or constitute proof of any criminal or other wrongful activity. Any change to this position would require a dramatic departure from the same international law that we consider to have been violated by Russia's invasion of Ukraine. Examples are rare and likely to attract litigation.

At the other end of the spectrum, the exponential increase in the numbers of asset freeze targets has forced debate on the criteria that should govern delistings, and how these can be calibrated to further the objectives pursued by sanctions. Designation challenges have, to date, rarely featured public denunciations of the invasion of Ukraine – as few are likely to be in a position to do so without exposing their families, friends and livelihoods to risk of irreparable harm. Offering to remove targets from sanctions lists in return for payments or divestments of assets is equally difficult to reconcile with the rule of law and separation of powers.

In addition to the new kinds of sanctions measures and export controls adopted in response to the Russian invasion of Ukraine, we have seen significant developments triggered by the acts of the People's Republic of China (PRC). The first edition of *The Guide to Sanctions* was published as the United States was ramping up sanctions in response to the PRC's passage of a national security law for the Hong Kong Special Administrative Region of the PRC (Hong Kong SAR). Since then, the chief executive of Hong Kong SAR and numerous PRC and Hong Kong SAR officials have been blacklisted and named as Specially Designated Nationals by the US Treasury's Office of Foreign Assets Control (OFAC). In those days, China's Xinjiang Province had yet to become a household name, and few outside the Washington, DC, beltway had ever heard of a 'Communist Chinese military company'.

The US spearheaded efforts to cut off the flow of certain advanced technologies to the PRC. The Biden administration has expanded on its predecessor's targeting of investments in Chinese defence and surveillance technology firms, and prohibited US persons from transacting in publicly traded securities of entities operating in the defence or surveillance technology sectors of the Chinese economy. These entities are identified on a specific list of Chinese military-industrial complex companies. Following the expansion of the Export Administration Regulations' Foreign-Produced Direct Product Rule (FDPR) to target Huawei, the Biden administration has also committed to that strategy. A package of export controls issued in October 2022 restricts the flow of certain advanced semiconductors to the PRC, alongside the export of semiconductors from certain non-US manufacturing facilities. The expanded FDPR catches advanced semiconductors and other computing inputs produced using US technology, severely limiting the PRC's options for acquiring the highest-end chipsets. In August 2023 the Biden administration took its first steps towards establishing an outbound investment control mechanism, initially focusing on investment in Chinese semiconductor and advanced computing technology. Pressure on the Chinese technology sector is likely to continue as there are both commercial and national security reasons for seeking to limit China's advances in artificial intelligence and quantum computing.

Above all, the US continues to lead the way on sanctions policy. Since the publication of the second edition of *The Guide to Sanctions* in 2021, the US Treasury Department has published the findings of a 'top to bottom review' and committed to doing more to lessen the unintended consequences on humanitarian organisations and vulnerable peoples. Unlike previous administrations, the Biden administration has also shown a marked preference for multilateralism, with human rights emerging as a shared theme. Still, the White House has shown little interest in rolling back most of the Trump administration's signature China-related sanctions. While there were reports in early 2022 of Iran and the United States coming closer to a nuclear deal, the United States has yet to agree to re-enter the Joint Comprehensive Plan of Action, and Russia has made demands in multilateral negotiations to protect its trade with Iran from the effects of the Ukraine-related sanctions.

The UK's autonomous sanctions framework continues to mature. In 2021, the UK government launched an ambitious new human rights sanctions programme accompanied by the designation of targets in China (Xinjiang), Myanmar, North Korea, Russia and Saudi Arabia – as well as an equally ambitious anti-corruption programme with targets in South Africa, Russia, South Sudan and Latin America. Although the scope of both programmes is more limited than their US sanctions

counterparts, the UK is seeking to carve out a role for itself as a global sanctions policymaker. At the same time, the UK has sought to ensure alignment with other western sanctioning jurisdictions by introducing an 'urgent procedure' for designations, replicating decisions by key allies such as Canada, the EU and the US. Policy divergence is nonetheless expected to continue – in both the focus of the UK's designations and the speed with which they are adopted, as well as in the steps taken by the UK to ameliorate negative consequences of sanctions by issuing both general and specific licences.

While the UK's export control regime remains closely aligned with the EU's following Brexit, there are some key differences that add a layer of complexity and additional requirements, not least flowing from the UK's status as a 'third country' requiring authorisations and licences for EU-to-UK exports of controlled goods and vice versa. Divergences are also emerging in respect of dual-use goods and technologies. As covered in Chapter 8, the political realities of Brexit within the UK continue to evolve, with Northern Ireland aligning with the EU under the Northern Ireland Protocol, while England, Scotland and Wales (Great Britain) proceed under their own regime.

Finally, the design and application of the UK's autonomous regime has yet to receive significant judicial scrutiny. Whereas we are starting to see the UK courts hear the first legal challenges brought to designation decisions, we have yet to see corresponding challenges to licensing decisions and enforcement actions. The relevant government agencies are gradually increasing their reliance on general licences, but delays in processing specific licence applications still create real humanitarian and commercial prejudice. While litigation has resulted in much-needed judicial interpretations of provisions of UK sanctions law, the relative paucity of meaningful guidance from the UK authorities (as compared to their US and EU counterparts) increases the compliance burden and contributes to the over-compliance and de-risking that the UN's Special Rapporteur on unilateral coercive measures and human rights warns of in her thought-provoking foreword to this fourth edition of *The Guide to Sanctions*.

By contrast, the EU sanctions policy has at times appeared to lag behind that of the US and the UK. In large part, this perceived difference in reactivity is attributable to the unanimity required on the part of all 27 EU Member States for decisions in the area of the EU's Common Foreign and Security Policy. While proposals to introduce qualified majority voting remain under consideration, the EU has been seen to act swiftly to impose several packages of hard-hitting sanctions against Russia. Disagreements on Russian energy and Russian oil have not prevented the Member States from ultimately finding consensus on imposing sanctions in these and other areas, including financial services, aviation and the

military, as well as on Russia's Central Bank and top leaders. By contrast to other major western sanctioning powers, the EU has, in the context of its Russia sanctions regime, introduced a range of measures to restrict professional and business services, extend reporting obligations and improve the enforcement of sanctions.

The EU has also joined other jurisdictions in introducing a global human rights sanctions regime, first used in March 2021. In a coordinated response with the United States, the EU imposed sanctions on Russian individuals for their role in the arbitrary arrest, prosecution and sentencing of Alexei Navalny. Although the EU has not yet followed the US, Canada and the UK in introducing a thematic or activities-based sanctions regime for global corruption, the designation criteria under country-specific regimes capture serious human rights violations and activities undermining democracy.

Since the publication of the first edition of *The Guide to Sanctions*, the EU has implemented the most significant reform to its export control regime since 2009. In May 2021, the EU adopted a revised version of its Dual-Use Regulation, updating the EU system to include sensitive dual-use goods and technologies such as cyber-surveillance tools.

With increasing sanctions policy divergence comes greater scope for conflict of laws. The EU and the UK continue to operate 'blocking' legislation in respect of US-specified sanctions on Iran and Cuba, and further variations on blocking and counter-sanctions have emerged in the PRC and, latterly, in the Russian Federation. There are few remedies available to businesses and individuals left to navigate conflicting obligations, and the judgment of the Court of Justice of the European Union in *Bank Melli Iran v. Telekom Deutschland* illustrates well how the legal limits of sanctions are compounded by their practical limits.[4]

The expanding role of sanctions

Whether expressive of the internal politics of nations or the broader geopolitical scene, sanctions, and disagreements about sanctions, have become a defining feature of international law and relations in the twenty-first century. Conceptualised in the early and mid-twentieth century as a non-forcible, multilateral means of responding to threats against international peace and security, in the twenty-first century economic sanctions are again taking on an increasingly unilateral character, with major sanctions programmes, including those imposed against Russia in early 2022, administered well outside the purview of the UN

4 Case C-124/20, *Bank Melli Iran v. Telekom Deutschland GmbH*, judgment of the Court (Grand Chamber) of 21 December 2021.

Security Council. The growth of sanctions as tools of foreign policy and security can be explained, in part, by the rapid globalisation of trade and financial services, which has increased the opportunities for nation states to exercise economic leverage over foreign adversaries. The fragmentation of international accord as a consequence of the Cold War and, later, the Iraq, Afghanistan and now the Russia–Ukraine wars, among other factors, has prevented effective regulation by the international community of individual states' use of sanctions. The UN Human Rights Council's Special Rapporteur on unilateral coercive measures and human rights conducts useful analyses of the negative consequences of this fragmentation but is ill-equipped to do more, without an expanded mandate. We are especially grateful to the current Special Rapporteur, Professor Alena Douhan, for her timely and insightful foreword to this fourth edition of *The Guide to Sanctions*.

Since the early 2000s, targets of sanctions have overwhelmingly included non-state actors – both entities and individuals – as both multilateral and unilateral sanctions programmes have attempted to get 'smarter'. In some contexts, the adoption of sanctions might be perceived as an inappropriate substitute for law enforcement measures (without commensurate due process) when directed at persons accused of (but not necessarily ever convicted, or even prosecuted or investigated for) criminal offences such as drug trafficking, corruption and embezzlement. Examples include designations made under the EU's (and formerly the UK's) 'misappropriation' sanctions regimes under which former government ministers in Tunisia, Egypt and Ukraine and their family members were designated based on allegations of misappropriation of state assets made by the incoming governments following a regime change by the state assets. In the US, activities-based sanctions regimes have captured a broader range of criminal conduct, including the US 'Kingpin' sanctions against suspected drug traffickers and the US Transnational Criminal Organizations sanctions. In most sanctioning jurisdictions there is, as yet, little clarity on the objectives that are appropriate for sanctions to pursue and the criteria that must be met, if any, for activity to be targeted in furtherance of those objectives.

As sanctions are extended to capture more activity and the numbers of designations increase, the impact of sanctions on commercial activity becomes more apparent. Sanctions are predominantly enforced in private, by the withdrawal of goods and services by private actors. It follows that the impact of sanctions is a function of the magnitude and importance of commercial activity to be withdrawn, and the degree to which individuals and entities are incentivised do so. These factors account for the relative strength of US sanctions, and further leverage is achieved by 'secondary sanctions' exposure for persons outside US jurisdiction and the size of the civil and criminal penalties levied for breaches.

Many countries are, however, starting to flex their enforcement muscles. Since the UK's Office of Financial Sanctions Implementation was created in 2016, it has issued nine civil monetary penalties for financial sanctions, alongside a range of other enforcement tools. Legislation has been proposed to harmonise the penalties available under the national laws of the EU Member States for EU sanctions breaches and circumvention.

A practitioner's guide

Our goal with this 'practitioner's guide' is to collate and disseminate the accumulated experiences of a relatively small – but rapidly growing – community of international sanctions experts. Their contributions are intended to offer some assistance with what are often difficult judgement calls involved in day-to-day sanctions practice. While they are political tools, sanctions are also legal measures and must be approached in the context of the legal systems in which they operate. We have selected topics relevant to a range of practice areas, with insights from the perspective of corporations and financial institutions – as relayed by their advisers. In a practice area where there is no 'right' answer to many problems, and in which an understanding of the commercial, technical and geopolitical context may be just as crucial as the law, we hope this guide continues to be a much-needed resource.

We intend this guide to fulfil multiple aims. For the reader who is new to the topic of sanctions, we hope to provide an accessible introduction to the essential legal frameworks and the challenges they present for practitioners the world over. For the seasoned experts, the guide should serve as a convenient compendium of relevant developments, and the sheer scale of changes in law and policy since the previous edition demonstrates the value of taking stock.

The 24 chapters in this fourth edition take a thematic approach to sanctions, categorised broadly across legal regimes and selected practice topics. Chapters 1 to 6 offer an overview of the major features of the EU, UK and US sanctions regimes and their enforcement. While individual perspectives shine through, each chapter follows a similar outline, for ease of comparison. Chapters 7, 8 and 9 provide an overview of EU, UK and US export controls – a technically complex and increasingly pervasive topic as the scope of sanctioned goods and technology expands, often in conjunction with prohibitions on related assistance. Chapters 11 and 12 offer perspectives from the Asia-Pacific region, particularly China and Hong Kong, where practitioners face corresponding challenges of navigating overlapping and potentially conflicting requirements. Chapter 13 considers the practical applications of international sanctions and export controls in France. Chapter 14 offers a principled guide to building sanctions compliance programmes by

reference to risk, incorporating guidance from OFAC and other leading sanctions authorities. Chapter 15 discusses the challenges of implementing effective sanctions screening across complex organisations. Chapters 16, 17 and 18 explore sanctions in the context of three areas likely to be encountered by practitioners – corporate transactions, litigation and disputes, and compliance. Chapter 20 brings attention to the impacts on sanctions and export controls on increasingly stretched global supply chains. Chapter 21 focuses on the emerging and increasingly strategic world of cyber-related sanctions. Chapter 22 examines the role of forensics and technology in sanctions compliance, with recommendations of best practices. Chapters 23 and 24 discuss strategies for representing sanctioned persons, from both a UK and US perspective.

This edition of *The Guide to Sanctions* explores new topics in two new chapters: Chapter 10 provides an overview of sanctions in Latin America, and Chapter 19 explores sanctions and export controls considerations for higher education and research institutions.

Change is an almost constant feature in sanctions law, as regimes develop in response to events in states' international relations and domestic politics. Inevitably, the sanctions regimes described in this guide will have developed by the time of publication.

Debts of gratitude

On behalf of the editors, we extend our deepest thanks to Professor Alena Douhan, UN Special Rapporteur on unilateral coercive measures and human rights, for her foreword to this fourth edition and for her invaluable work in highlighting the difficult and pressing human rights issues currently facing vast numbers of people affected by the implementation of sanctions, that are so often overlooked by policymakers. We also thank Global Investigations Review, in particular Mahnaz Arta, Georgia Goldberg and Ouassila Mebarek, for their consistent and ever-enthusiastic support of this guide, and for once again gently nudging the contributors (editors included) to bring the project to a successful and timely conclusion. To each of the contributors, we thank you for sharing your time and unique expertise, generously reflected in the thoughtful and thought-provoking pieces that follow.

Part I

Sanctions and Export Control Regimes Around the World

CHAPTER 1

EU Restrictive Measures

Renato Antonini, Eva Monard, Byron Maniatis and Elli Zachari[1]

Authorising EU restrictive measures

Sanctions at EU level constitute a political tool under the EU's Common Foreign and Security Policy (CFSP). Being political decisions, the EU treaties do not provide the same safeguards as they do for legislative acts, nor do they regulate the conditions or instances of sanctions imposition, the decision being subject to negotiations between Member State representatives in the Council of the European Union (the Council).

The procedure to adopt sanctions is triggered by a proposal from the High Representative of the Union for Foreign Affairs and Security Policy (HRFASP).[2] Relevant preparatory bodies of the Council, such as the Council working party responsible for that geographical region, the Working Party of Foreign Relations Counsellors (RELEX) and, if required, the Political and Security Committee (PSC), will examine and discuss the proposed measures. The Committee of the Permanent Representatives of the Governments of the Member States to the European Union II[3] will take the final decision within the Council by unanimity.[4] Once agreement is reached, the Council will adopt the decision to impose EU restrictive measures, which will then be published in the Official Journal.

---

1 Renato Antonini and Eva Monard are partners, Byron Maniatis is a senior associate and Elli Zachari is a legal consultant at Steptoe & Johnson LLP.

2 See Article 27(1) of the Treaty on European Union, OJ C 326, 26 October 2012 (TE).

3 Foreign Affairs Council – Committee of the Permanent Representatives of the Governments of the Member States to the European Union II.

4 See Article 2 et seq. of the Council's Rules of Procedure, OJ L 325, 11 December 2009. See also Articles 24(1) and 31(1), TEU.

If the decision entails economic or financial measures (such as asset freezes or trade sanctions), the Council will have to subsequently follow the procedure laid out in Article 215 of the Treaty on the Functioning of the European Union (TFEU) and adopt an implementing regulation by qualified majority. The subsequent adoption of an implementing regulation for economic or financial measures is necessary, as the Council's decisions are binding only on EU Member States, whereas regulations are binding upon any person or entity within the EU.

The procedure for adoption of the implementing regulation is triggered by the joint proposal from the HRFASP and the Commission, which will be analysed by the relevant Council preparatory bodies – the working party responsible for the relevant geographical region, RELEX and, if required, PSC. The Foreign Affairs Council will need to approve the text by qualified majority. Once adopted, the regulation is published in the Official Journal of the European Union and the Council informs the European Parliament about the act.

The two procedures usually take place in parallel, such that the Council's decision and the implementing regulation are adopted together.

Design and implementation

First, restrictive measures are a tool for the EU to advance one or more of its CFSP objectives as laid out in Article 21(2) of the Treaty on European Union (TEU). For example, restrictive measures can be deployed as a means to safeguard EU values and fundamental interests, or to support democracy, the rule of law and human rights.[5]

Second, although sanctions are applied through non-legislative acts, their design and implementation must comply with EU principles, international law and fundamental rights. This is clearly set out in the Sanctions Guidelines adopted by the General Secretariat of the Council.[6]

As such, the restrictive measures should be proportionate, in accordance with the EU principle laid out in Article 5(4) of the TEU. The imposed measures should not go beyond what is necessary to attain their objective. Proportionality is reflected in the incremental manner in which the EU adopts sanctions, by gradually increasing the degree of restrictions until the CFSP objective is attained.

---

5 See Article 21(2), TEU.

6 See Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy (doc. 15579/03), paragraphs 8–12, https://data.consilium.europa.eu/doc/document/ST-5664-2018-INIT/en/pdf.

In addition, the restrictive measures adopted must comply with international law. For example, the measures must respect the fundamental right to an effective remedy under Article 13 of the European Convention on Human Rights and the international obligations assumed under the World Trade Organization agreements.

Lastly, the restrictive measures must respect the EU's fundamental and human rights. This requirement was made evident in the *Kadi I* and *Kadi II* cases,[7] where the EU Court of Justice annulled the restrictive measures implementing a United Nations Security Council resolution for a breach of the rights of defence, in particular the right to be heard, and the right to an effective judicial review.

Designation process

Required information

First, the Council will strive to obtain as much information as it can on the identity of a person or entity. With regard to natural persons, the Council will seek to obtain the name and surname of the person, any aliases, gender, date and place of birth, nationality, address and identification or passport number.[8] Concerning entities, the Council will aim to obtain their name, place of business and registration, and date and number of registration.[9]

In addition, the Council decides on specific listings based on the listing criteria set out in the relevant Council decision and regulation imposing the measures in question. The Council must rely on a sufficiently solid factual basis proving that the listing criteria are met.[10] The Council's decision will be accompanied by explanations concerning the listing, in accordance with the duty to state reasons.[11]

Any information and evidence that helps create a sufficient factual basis can inform the Council's assessment. The information and evidence that was relied upon by the Council will not be shared with the 'designated person', although the latter will receive a notification concerning its listing. In the case of a dispute before the EU courts, the Council will have to produce, at the court's request, all

7 Case C-402/05 P, *Kadi v. Council and Commission*, ECLI:EU:C:2008:461; Case C-584/10 P, *Commission and Others v. Kadi*, ECLI:EU:C:2013:518 (*Kadi II*).

8 See EU Best Practices for the effective implementation of restrictive measures, paragraph 5, https://data.consilium.europa.eu/doc/document/ST-10572-2022-INIT/en/pdf.

9 ibid.

10 See, to that effect, Case C-539/10 P, *Al-Aqsa v. Council* and *Netherlands v. Al-Aqsa*, ECLI:EU:C:2012:711, paragraph 68.

11 See Article 41 of the Charter of Fundamental Rights.

the information and evidence (whether confidential or not) that formed the basis of the decision.[12] The court will verify the accuracy of the alleged facts in light of the information and evidence provided by the Council and the designated person.

Entities subject to restrictive measures

When economic sanctions are imposed, as well as targeting the funds and economic resources of designated persons and entities, the restrictions will generally also include the assets of affiliated entities, which are owned or controlled by the designated persons or entities. This is also the case regarding the prohibition on making available funds and economic resources to listed persons or entities.

The notions of 'ownership' and 'control' are defined in the EU Best Practices for the effective implementation of restrictive measures (the EU Best Practices).[13] According to the EU Best Practices, ownership is presumed if a designated person or entity is in possession of more than 50 per cent of the proprietary rights of a company, or has a majority interest in it.[14] Controlling a person refers to a designated person being able to effectively assert a decisive influence over the conduct of another entity, with a broad list of non-exhaustive criteria contained in the EU Best Practices as well as other EU guidance.[15]

EU restrictive measures can also include the freezing of assets of natural or legal persons, entities or bodies 'associated' with designated persons. While the criterion of association is not defined by law, the EU courts have held that association occurs whenever there is a common interest between the designated person and a third person or where there is an economic or capital link between the designated person and a third person.[16] Conversely, the EU courts have held that

12 See *Kadi II*, paragraph 120; Case T-212/22, *Violetta Prigozhina v. Council*, ECLI:EU:T:2023:104, paragraphs 37, 38.

13 EU Best Practices (footnote 8), paragraphs 62, 63.

14 Note that the legislation that the EU Best Practices refer to, namely Council Regulation (EC) No. 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism, refers to 'being in possession of 50% or more of the proprietary rights of a legal person, group or entity, or having a majority interest therein'.

15 See, for instance, https://ec.europa.eu/info/files/200619-opinion-financial-sanctions_en.

16 *Violetta Prigozhina v. Council* (footnote 12), paragraphs 93, 94. See also Case T-66/14, *Bredenkamp and Others v. Council and Commission*, ECLI:EU:T:2016:430, paragraphs 35–37.

family ties are not sufficient by themselves to meet the criterion of association, as restrictive measures cannot be applied independently of the personal behaviour of a person or entity.[17]

On 'association', it is also worth noting that the EU's sanctions lists (i.e., the Annexes to the relevant sanctions regulation) often explicitly name the persons or entities that are considered to be associated with a listed person.[18] However, according to the Commission,[19] strictly speaking, only the persons and entities that are listed themselves (these typically appear under the 'Name' column in the relevant Annex) are directly subject to an asset freeze and a prohibition to make funds and economic resources available, and not the persons or entities associated with them (which are mentioned in the 'Identifying information' or 'Reasons' column). That being said, according to the Commission, '[o]perators need to exert the highest caution when dealing with associated persons or entities', especially as they may be 'deemed to be owned or controlled by listed persons or entities'.[20]

Finally, restrictive measures can target natural or legal persons acting 'on behalf' or 'at the direction' of a designated person. The notions of acting 'on behalf' or 'at the direction' are distinct from those of 'ownership' or 'control'. However, the Commission has interpreted the two notions as being on 'equal footing' in terms of their effects.[21]

Ownership and control analysis

As explained above, ownership is assessed based on proprietary rights. If a person or entity is in the possession of more than 50 per cent of the proprietary rights of another entity, or has a majority interest therein, ownership is presumed.[22]

---

17 Case C-376/10 P, *Pye Phyo Tay Za v. Council of the European Union*, ECLI:EU:C:2012:138, paragraphs 63–66; *Violetta Prigozhina v. Council* (footnote 12), paragraph 95.

18 See, for instance, the second column titled 'Identifying information' in Annex I to Council Regulation (EU) No. 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0269-20230426.

19 See 'Commission Consolidated FAQs on the implementation of Council Regulation (EU) No. 833/2014 and Council Regulation (EU) No. 269/2014', 22 June 2022, https://finance.ec.europa.eu/system/files/2023-07/faqs-sanctions-russia-consolidated_en.pdf (last updated 6 July 2023, accessed 7 July 2023).

20 ibid.

21 Commission Opinion of 17 October 2019 on Article 5(1) of Council Regulation (EU) No. 833/2014 (C(2019) 7476 final).

22 See EU Best Practices (footnote 8), paragraphs 62, 63. See also Article 1(5) of Regulation (EC) No. 2580/2001.

Control is assessed case by case, on the basis of a number of criteria laid out in the EU Best Practices.[23] Control can be established when the designated person:

1 has the right or exercises 'the power to appoint or remove a majority of the members of the administrative, management or supervisory body of such legal person or entity';
2 has appointed solely as a result of the exercise of its 'voting rights a majority of the members of the administrative, management or supervisory bodies of a legal person or entity who have held office during the present and previous financial year';
3 controls alone, 'pursuant to an agreement with other shareholders in or members of a legal person or entity, a majority of shareholders' or members' voting rights in that legal person or entity';
4 has 'the right to exercise a dominant influence over a legal person or entity, pursuant to an agreement entered into with that legal person or entity, or to a provision in its Memorandum or Articles of Association, where the law governing that legal person or entity permits its being subject to such agreement or provision';
5 has the power or right 'to exercise a dominant influence referred to in point [(4)], without being the holder of that right';
6 has 'the right to use all or part of the assets of a legal person or entity';
7 manages 'the business of a legal person or entity on a unified basis, while publishing consolidated accounts'; and
8 shares 'jointly and severally the financial liabilities of a legal person or entity, or guaranteeing them'.

Meeting any of the above criteria would be sufficient for an authority to consider that a legal person or entity is controlled by another, unless the former manages to prove otherwise. Both ownership and control may be rebutted on a case-by-case basis.

It is also worth mentioning that other guidance by the European Commission[24] lists additional criteria that can be taken into account to establish control. These are somewhat broader, as they include, for instance, 'having influence as regards corporate strategy, operational policy, business plans, investment, capacity, provision of finance, human resources and legal matters'.[25]

23 Paragraphs 62, 63. See also Article 1(6) of Regulation (EC) No. 2580/2001.
24 'Commission Opinion of 19.6.2020 on Article 2 of Council Regulation (EU) No. 269/2014'.
25 ibid.

Licensing

Overview

When restrictive measures are imposed, they are generally accompanied by a series of exemptions and derogations. The implementation and enforcement of EU sanctions is the responsibility of the EU Member States. Their national authorities are also competent to grant authorisation (licensing) for specific derogations provided for in the relevant sanctions regimes. Under the EU Best Practices, national authorities should exchange information with each other on whether an authorisation is granted,[26] and similar requirements are sometimes found in specific EU sanctions legislation. The exchange of information is intended to allow Member States to coordinate the granting of authorisations and to prevent forum shopping.

In terms of sanctions designations, authorisations for a particular derogation can be requested by either the designated person or another interested person. Generally speaking, a licence is granted by national competent authorities to safeguard a fundamental right of the designated persons or another interest of general or EU importance (such as food security). Depending on the specific derogations of each sanctions regime, the competent authorities will assess one of the following when granting an authorisation:

- the basic needs of the designated persons, including in relation to payments for foodstuffs, rent or mortgage, medicines and medical treatment, taxes, insurance premiums and public utility charges;
- the protection of the right of defence in relation to expenses associated with the provision of legal services;
- right of ownership of the designated person or entity (as the freezing of assets does not affect the ownership of the designated person or entity, but the ability to use the funds);
- right of ownership of the non-designated legal person or entity where the frozen funds are held;
- right of ownership of both the designated person or entity and a non-designated person or entity in relation to contracts concluded between them before the designation;
- international law on diplomatic and consular relations;
- human safety and environmental protection; or

26 See EU Best Practices (footnote 8), paragraph 86.

- humanitarian purposes, such as delivering or facilitating the delivery of assistance, including medical supplies, food or the transfer of humanitarian workers and related assistance, or for evacuations from a targeted country.[27]

When a request for an authorisation is submitted, the national competent authorities can undertake any investigations they consider necessary and may consult with other Member States. Before granting an authorisation, national authorities must consider whether any accompanying additional limitations or requirements are necessary to fend off the risk of circumvention (e.g., making economic resources available each month instead of a large quantity at once). All licences must be granted in writing and prior to making use of the economic resources. Failure to comply with the requirement will be considered a breach of the relevant regulation and may lead to criminal penalties for the persons or entities involved.

When third parties are creditors with a valid claim against the designated person, they will also be able to obtain authorisation in accordance with the applicable rules of the relevant national authority. The competent authorities shall notify the designated person and shall examine the validity of the claims. In doing so, the competent authorities will examine the evidence provided by both the interested party (as a creditor) and the designated person (as a debtor), to decide whether there is a valid legal obligation and a risk of circumvention.

Licensing also exists for certain trade sanctions, and the conditions and procedure may vary depending on the sanctions regime and specific restriction in question.

Trends and commonalities

The Russian invasion of Ukraine and the resulting recurrent waves of EU sanctions packages being imposed on Russia have resulted in a transformation of EU sanctions policy. The level of restrictive measures imposed on such a close trading partner is unprecedented. As compared to other sanctions packages, the EU sanctions on Russia have been imposed at an extraordinary pace. It has also resulted in a heightened focus on the implementation and enforcement of EU restrictive measures, at EU Member State level, as well as by the European Commission. The European Commission has made many efforts to increase sanctions coordination between EU Member States (for example, the Freeze and Seize Task Force, to

27 EU Best Practices (footnote 8), paragraph 76.

coordinate actions to freeze and, where applicable, confiscate assets of Russian and Belarussian oligarchs,[28] and the EU Sanctions Whistleblower Tool, through which past, ongoing or planned EU sanctions violations can be reported).[29]

In parallel, as a result of the EU sanctions on Russia, the substance of EU sanctions has evolved in ways that would, in the past, have been inconceivable (for example, stand-alone sanctions on certain key services, such as legal advisory services).[30] Other important examples are the introduction of the notion of 'deemed exports' in the context of EU sanctions, or the facilitation of sanctions circumvention as a basis for EU sanctions designations. Many of these novel notions have been introduced through an unprecedented level of sanctions guidance issued at EU level.[31]

Another trend is an increasing focus on addressing the circumvention of restrictive measures, beginning in 2022, when the Commission issued a notice advising EU economic operators, importers and exporters to take adequate due diligence measures to prevent circumvention of the EU sanctions on Russia.[32] Around the same time, pursuant to Commission guidance regarding due diligence in the context of the EU sanctions on Russia, EU operators have been recommended to put in place a risk-based approach that consists of risk assessment, multi-level due diligence and ongoing monitoring.[33] Subsequently, in the context of the eight EU sanctions packages on Russia, new listing criteria were added allowing for the designation of persons or entities that facilitate the circumvention of EU sanctions against Russia.[34]

Finally, the Commission is currently preparing its 11th sanctions package against Russia, which reportedly may target third countries as well as foreign entities that enable the circumvention of EU sanctions. With these measures, the EU

28 See https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2373.

29 See https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/overview-sanctions-and-related-resources/eu-sanctions-whistleblower-tool_en.

30 See Council Regulation (EU) No. 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, Article 5n(2).

31 Renato Antonini, Eva Monard and Byron Maniatis, 'The Russia factor: a transformation of EU sanctions policy', *Export Compliance Manager*, Issue 28, November 2022.

32 Commission Notice to economic operators, importers and exporters, 2022/C 145 I/01.

33 Commission's Russia Sanctions FAQs, Section 2, FAQ 2, referring to previous guidance on due diligence for business with Iran.

34 Council Regulation (EU) 2022/1905 of 6 October 2022 amending Regulation (EU) No. 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, Article 1.

would take another step away from its traditional concept of non-extraterritoriality of EU sanctions. However, this proposal is controversial and it is uncertain whether it would be adopted.[35]

Case studies

Luxembourg

On 20 December 2022, the Ministry of Finance in Luxembourg granted a general authorisation for the release of funds deposited by the sanctioned Russian National Settlement Depository through Clearstream, a clearing house located in Luxembourg.[36]

The authorisation was granted under the provision of Article 6b(5) of Regulation (EU) No. 269/2014, which allows the release of certain frozen funds for the termination by 7 January 2023, of operations, contracts or other agreements concluded before 3 June 2022.

As such, the authorisation enabled any interested persons (investors or entrepreneurs) to rely on it and obtain, until 7 January 2023, the transfer of their financial resources from the Russian National Settlement Depository to other depositories, for operations, contracts or agreements that were concluded prior to 3 June 2022.

Finland

On 22 March 2023, the Finnish Ministry of Foreign Affairs granted an individual export authorisation for a Cyprus-flagged ship carrying fertiliser,[37] after detaining it to investigate the origins of its cargo and possible violations of EU sanctions. The subsequent investigation carried out by Finnish authorities confirmed that there was a link between the shipment of fertiliser and a sanctioned individual.

The authorisation was granted under Article 6e(1a) of Regulation (EU) No. 269/2014, which allows the release of economic resources belonging to designated persons and entities to promote and safeguard food security.

---

35 See Renato Antonini, Eva Monard and Byron Maniatis, 'The Notion of Circumvention Under EU Sanctions', *Export Compliance Manager*, Issue 33, May 2023.

36 See 'General authorization pursuant to Article 6b paragraph 5 of Council Regulation (EU) No. 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, as amended' (Ref: 841x12c14), https://mfin.gouvernement.lu/dam-assets/dossiers/sanctions-financi%C3%A8res-internationales/documentation/general-authorization-ru-sanctions-269-2014-art6-para-5.pdf (last accessed 7 July).

37 See https://valtioneuvosto.fi/en/-/ministry-for-foreign-affairs-granted-an-authorisation-for-russian-fertiliser-cargo-stopped-at-port-of-kotka.

Of note, to promote food security and further streamline the supply of products, the Commission issued a guidance note[38] on measures designed to allow non-designated EU entities engaged in agricultural and food trade – owned or controlled by Russian entities – to decouple from sanctioned designated persons. Once an entity implements the Commission's recommended measures, it will be presumed that the designated person or entity cannot exert further control over it. As such, the non-designated entity will be discharged from the obligation to obtain authorisation from national competent authorities.

Challenging designations

Delisting takes place whenever the initial listing reasons are no longer met. This can happen if a listing was made erroneously (e.g., against the wrong person or entity), due to a subsequent change of facts or as a result of further evidence that proves that listing was not called for in the first place.[39]

A request for delisting must be addressed to the General Secretariat of the Council, together with any supporting evidence.[40] The relevant process is typically set out in the notice to the listed persons informing them about their designation and specifying the date by which the delisting request must be made.[41] The request should be made in writing to the Council of the European Union or via email and must comply with the review process laid out in the relevant notice.

A preliminary assessment of a delisting request will be conducted by the European External Action Service (EEAS) and the Council Legal Service. Following that, the Council Secretariat will forward the request and the preliminary analysis to the appropriate regional working party for consideration.[42]

A listing or delisting decision may be subject to an action for annulment before the General Court of the European Union. The legal basis for lodging a claim is provided in Articles 275 and 263 of the TFEU, which allow the EU courts to review the legality of these decisions.

---

38 Guidance Note – Ensuring food security through the implementation of firewalls in cases of EU entities trading in agricultural and food products and controlled by a designated person or entity, https://finance.ec.europa.eu/system/files/2023-05/230503-guidance-firewalls_en.pdf.

39 EU Best Practices (footnote 8), paragraph 18.

40 See European Council website, www.consilium.europa.eu/en/policies/sanctions/adoption-review-procedure/, and Annex I to the Council's Guidelines, paragraphs 19, 20, https://data.consilium.europa.eu/doc/document/ST-5664-2018-INIT/en/pdf.

41 See, for instance, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2023.198.01.0004.01.ENG&toc=OJ%3AC%3A2023%3A198%3ATOC.

42 See Annex I to the Council's Guidelines (footnote 38), paragraphs 19, 20.

In the case of a wrongful listing, an interested party would have the possibility to lodge an action for damages under Article 340 of the TFEU before the General Court, to receive compensation for the damages suffered as a result of the listing. For example, damages can result whenever the assets of a person or entity are frozen. The action for damages must be lodged within five years of the listing taking place.[43] The person claiming the damages will need to demonstrate: (1) unlawful conduct of the institution in the light of EU law; (2) the existence of real and certain damage; and (3) the existence of a causal link between the conduct and the damages claimed.

Monitoring, appraisal and termination of restrictive measures

Monitoring of EU restrictive measures is carried out periodically by the Council, assisted by the EEAS, the Commission and the EU heads of missions, in accordance with the specific provisions of the regulations. This allows the Council to further tailor the measures, to ensure their effectiveness in relation to the desired objectives.

RELEX meets regularly in its specific 'Sanctions formation' to discuss sanctions implementation and exchange experiences in the application of restrictive measures with experts from Member States. Among other things, RELEX will collect information on alleged circumvention of sanctions, exchange information and experiences on implementation of specific measures, and assist in evaluating the results and challenges of implementing the restrictive measures.[44]

EU sanctions are adopted for a limited period (e.g., one year), following which the application of restrictive measures comes to an end. Before the expiry date, the Council will have to decide whether or not to further extend the measures. If, during the monitoring of sanctions, the Council considers that the objectives of the sanctions were attained and that the application of restrictive measures is no longer required, it will decide not to extend the measures.

---

43 See, for example, Case C-45/15 P, *Safa Nicu Sepahan Co. v. Council of the European Union*, ECLI:EU:C:2017:402.

44 See Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy (doc. 15579/03), paragraphs 94, 95, https://data.consilium.europa.eu/doc/document/ST-5664-2018-INIT/en/pdf.

Remedies against a Council decision to extend the restrictive measures are provided in Articles 275 and 263 of the TFEU. However, even if an application for annulment is successful, it is likely that by the time the applicant obtains the annulment of the decision to extend the measure, another decision on extension would have already taken place.

Recent trends

Belarus

EU sanctions against Belarus have been in place since 2006; they were previously imposed in response to human rights violations taking place in Belarus (violent repression and intimidation of peaceful demonstrators, opposition members and journalists, among others). In 2022, the EU imposed additional sanctions against Belarus, this time in response to the country's involvement in Russia's war against Ukraine. These measures included additional trade restrictions, individual designations and a SWIFT ban on certain Belarussian banks.

On 3 June 2022, the EU adopted its new round of restrictive measures against Belarus, targeting an additional 12 individuals and eight entities for internal repression and human rights abuses.[45] In addition, on 27 February 2023, the Council decided during its annual review to extend until 28 February 2024 the restrictive measures adopted for internal repression and support for the war against Ukraine. In total, the measures concern a freeze of assets of 195 individuals and 35 entities. Several trade sanctions were also imposed.

The restrictive measures against Belarus have not changed greatly since 2022, unlike those against Russia, which is likely in view of what appeared to be limited escalation of Belarus' support to Russia. However, in early 2023, there were discussions among EU diplomats about aligning the sanctions against Belarus with those that are in place against Russia. Furthermore, it is possible that the EU will adopt additional restrictive measures, following Belarus' decision to allow Russia to deploy its tactical nuclear weapons on its territory.

China

Since the imposition of sanctions against four Chinese officials and one entity for alleged human rights violations on 22 March 2021,[46] the EU has not imposed any new restrictive measures. However, it has been reported that the adoption of

45 See Council Decisions 2022/885, 2022/884, 2022/883, 2022/882 and 2022/881 of 3 June 2022.

46 See Council Regulation (EU) 2020/1998 concerning restrictive measures against serious human rights violations and abuses.

the EU's 11th sanctions package against Russia may target a number of Chinese companies alleged to have supported Russia's war efforts. In addition, the EU may impose additional restrictive measures on exports, following the EU's 'de-risking' approach announced by the Commission's President Ursula von der Leyen during the EU Parliamentary debate, 'The need for a coherent strategy for EU–China Relations'.[47] Lastly, additional restrictions may be indirectly imposed by the EU against China, following the enforcement of the anti-circumvention tool announced in the EU's 11th sanctions package against Russia. This effectively enables the EU to target third countries that enable Russia to circumvent sanctions.

Myanmar

Over recent years, the EU has been steadily increasing the restrictive measures against Myanmar. On 20 February 2023, the EU decided to adopt a sixth round of sanctions against it, targeting an additional nine individuals and seven entities for grave human rights violations and threats to peace, security and stability.[48] On 28 April 2023, the Council decided to extend the restrictive measures applicable against Myanmar until 30 April 2024.[49]

Russia

Prior to 2022, the EU had existing sanctions in place against Russia, which had been imposed in response to Russia's annexation of Crimea in 2014. However, since Russia's invasion of Ukraine in February 2022, those measures have been increased exponentially and are considered to be unprecedented for a number of reasons.

Breadth and variety of measures imposed

The restrictive measures imposed on Russia since 2022 have been unique in terms of their breadth and variety. Between February 2022 and February 2023, 10 sanctions packages were adopted in total, which were extensive and diverse both in terms of the types of measures imposed and the sectors targeted.

Notably, this was the first time that the EU had imposed such comprehensive sanctions measures against a major trading partner. In 2021, before the adoption of the recent sanctions, Russia was the EU's fifth largest trading partner,

47 EU Parliamentary debate, 'The need for a coherent strategy for EU–China Relations', dated 18 April 2023.

48 See Council Implementing Regulation (EU) 2023/378 of 20 February 2023.

49 See Council Decision (CFSP) 2023/887 of 28 April 2023.

while the EU was Russia's largest trading partner. Given the interconnectedness of the two economies, the far-reaching sanctions adopted by the EU have had a significant impact not only on the Russian economy but also on the EU economy, especially due to the long-standing reliance of the EU on Russia's energy imports.

Significant sanctions despite unanimity requirement

Another notable element of the recent EU sanctions against Russia is the fact that the Member States succeeded in negotiating such severe measures rather rapidly, despite the unanimity requirement, which has historically slowed down the sanctions adoption process. This is even more remarkable considering the close links between the EU and the Russian economy and the diverging economic interests of Member States.

Moreover, even when certain Member States expressed opposition to some of the measures proposed, the EU has come up with new ways of finding compromise, either by adopting new forms of restrictions (other than outright bans) or introducing special exemptions or derogations for specific Member States. An example of the foregoing were the EU sanctions against Russian imports of oil, which were controversial among certain Member States. To achieve unanimous approval, the EU imposed a ban on seaborne oil to enter into force by the end of 2022, while pipeline crude oil was temporarily exempted, as a concession to Hungary. Moreover, special temporary derogations were recognised for both Bulgaria and Croatia. In addition, the EU did not ban the transport of oil to third countries because of economic concerns expressed by Greece, Malta and Cyprus, but introduced a price cap instead.

Increased focus on implementation and enforcement

The 2022 restrictive measures on Russia have also prompted an increased focus on the implementation and enforcement of measures, both on the part of the Commission and of the competent authorities of EU Member States. While in the past, the enforcement of sanctions has not been a key priority, authorities in Member States have significantly increased their enforcement efforts since the Russian invasion of Ukraine.

The Commission has issued an unprecedented level of guidance in relation to the restrictive measures on Russia[50] to facilitate the different Member States's interpretation of the measures in a way that is as harmonised as possible. The Commission has also taken several steps to coordinate enforcement of the measures by the EU Member States (for instance, by setting up the Freeze and Seize Task Force and launching the EU Sanctions Whistleblower Tool,[51] through which EU sanctions violations can be anonymously reported).

Recently, the EU has been increasingly concerned with, and seeking to come up with ways to tackle, sanctions circumvention. The 11th sanctions package that is currently being negotiated is reported to be significant in that regard, by introducing a number of novel instruments to address this issue, including introducing restrictions to trade with third countries that are deemed to be enabling Russia to circumvent sanctions, and imposing additional restrictions on the transit of certain goods through Russia.

Conclusion

Sanctions have become an increasingly important area of EU law and policy in recent years, especially with the EU making unprecedented use of these measures since the beginning of Russia's invasion of Ukraine. The impact of the EU's Russia sanctions policy is likely to have a lasting change on EU sanctions, including existing and future measures imposed on other countries. Going forward, the EU's sanctions policy is likely to focus on enforcement and tackling circumvention, with the focus remaining on Russia. However, other third countries that the EU considers are facilitating Russia's war are increasingly in the EU's cross hairs. The question remains as to what extent the EU will continue to increasingly rely on sanctions to tackle further foreign policy concerns.

50 See the Commission's guidance on the Russia sanctions, which currently extends to 365 pages, https://finance.ec.europa.eu/system/files/2023-06/faqs-sanctions-russia-consolidated_en.pdf.

51 See footnote 29.

CHAPTER 2

EU Sanctions Enforcement

Stéphane Bonifassi and Julie Bastien[1]

Introduction

For sanctions to achieve their objectives, they must be effectively enforced. As Mairead McGuinness, European Commissioner for Financial Services, Financial Stability and Capital Markets Union, stated:

> *The full force of our sanctions can only be realised through proper implementation. We need to act to prevent any loopholes or circumvention, and the best way to do that is by working together at an EU level to coordinate our work.*[2]

There are currently 48 sanctions regimes in force in the EU.[3] Because of the increase of sanctions regimes and of their complexity, enforcement has become a core challenge.

The need for the proper enforcement of sanctions has become abundantly clear with the unprecedented evolution of EU restrictive measures in the framework of the sanctions regime developed pursuant to Russia's war against Ukraine.

---

1 Stéphane Bonifassi is the founding partner and Julie Bastien is an associate at Bonifassi Avocats.

2 'Statement by Commissioner McGuinness on the outcomes of the first meeting of the high-level meeting on sanctions implementation', 24 October 2022, https://finance.ec.europa.eu/news/statement-commissioner-mcguinness-outcomes-first-meeting-high-level-meeting-sanctions-implementation-2022-10-24_en.

3 EU Sanctions Map, www.sanctionsmap.eu/#/main (as at June 2023).

The EU enforcement framework

Sanctions are adopted by the Council of the European Union through a decision by the Common Foreign and Security Policy (CFSP) under Article 29 of the Treaty on the European Union (TEU).

While certain measures are directly implemented by Member States pursuant to CFSP decisions (such as travel bans), other types of measures may require the adoption of a Council Regulation under Article 215 of the Treaty on the Functioning of the European Union (TFEU).

Council regulations providing for sanctions are directly applicable in Member States and are binding on any person or entity with EU Member State nationality, located within the EU, or with respect to business done in the EU.

Role of Member States

Implementation and enforcement of EU sanctions is primarily the responsibility of Member States.[4]

Member States apply restrictive measures and grant derogations on the freezing of assets, trade-related prohibitions or other restrictive measures, within the framework designed by the Council of the European Union, through their national competent authority or authorities, as listed in the annex to the relevant Council regulation.

Member States also have an obligation to inform other Member States and the European Commission of any authorisation or derogation granted and generally to share with each other any information relevant to the enforcement of sanctions, including relevant information received by Member States from any person or entity under their jurisdiction.[5]

Member States are also responsible for the sanctioning and investigating of breaches of EU sanctions within their jurisdiction. For this purpose, Member States may need to adopt legislation at the national level. Council regulations providing for sanctions systematically include an obligation for Member States to 'lay down the rules on sanctions applicable to the infringements of the provisions

4 See, for instance, 'Communication from the Commission to the European Parliament and the Council Towards a Directive on criminal penalties for the violation of Union restrictive measures', COM(2022) 249 final, 25 May 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022DC0249.

5 See, for instance, Article 13 of Council Regulation (EU) No. 1210/2003 of 7 July 2003 concerning certain specific restrictions on economic and financial relations with Iraq and repealing Regulation (EC) No. 2465/96.

of the [Regulation] and shall take all measures necessary to ensure that they are implemented'. Sanctions laid down by Member States must be 'effective, proportionate and dissuasive'.[6]

In principle, Member States are free to decide on the nature of the sanctions. However, in Council Regulation (EU) No. 269/2014, addressing Russia's invasion of Ukraine, the Council of the European Union adopted a more detailed provision on 3 June 2022:

> *Member States shall lay down the rules on penalties, including as appropriate criminal penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive. Member States shall also provide for appropriate measures of confiscation of the proceeds of such infringements.*[7]

There is a significant disparity among Member States on the type and content of sanctions laid down.[8] In view of this disparity and in the context of the complex enforcement of EU restrictive measures against Russia, in May 2022 the European Commission issued a proposal for a Council decision[9] on adding the violation of Union restrictive measures to the areas of crime laid down in Article 83(1) of the TFEU. On 28 November 2022, the Council adopted Decision (EU) 2022/2332 pursuant to the Commission's proposal.[10]

---

6 id., at Article 15, Paragraph 1.

7 Article 15, Paragraph 1 of Council Regulation (EU) No. 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine as modified by Council Regulation (EU) 2022/880 of 3 June 2022 (emphasis added).

8 For an overview of the relevant national legislation, see the Annex to the Genocide Network's report, 'Prosecution of sanctions (restrictive measures) violations in national jurisdictions: a comparative analysis', December 2021, https://data.consilium.europa.eu/doc/document/ST-7274-2022-INIT/en/pdf.

9 Proposal for a Council Decision on adding the violation of Union restrictive measures to the areas of crime laid down in Article 83(1) of the Treaty on the Functioning of the European Union, COM/2022/247 final, 25 May 2022.

10 Council Decision (EU) 2022/2332 of 28 November 2022 on identifying the violation of Union restrictive measures as an area of crime that meets the criteria specified in Article 83(1) of the Treaty on the Functioning of the European Union.

On 2 December 2022, following the adoption of this Decision, the European Commission adopted a proposal for a directive on the definition of criminal offences and penalties for the violation of Union restrictive measures.[11] The Council shared its view on the Commission's proposal on 17 May 2023.[12] No directive has yet been adopted, but a directive would provide an obligation for Member States to make the violation of EU sanctions a criminal offence under their national law and would set forth common penalties, as opposed to the current framework of individually fixed sanctions.

Role of the EU Commission

Pursuant to Article 17 of the TEU, the European Commission ensures the application of treaties and measures adopted by certain institutions and oversees the application of EU law. Within this framework, the Commission oversees the uniform application of sanctions by Member States. If a Member State does not enforce EU sanctions, the European Commission could launch an infringement procedure under Article 258 of the TFEU (this has not occurred to date).

The Commission monitors the enforcement of sanctions by Member States through information that national competent authorities and economic operators provide pursuant to various information obligations under Council regulations. In particular, this information may concern frozen funds and economic resources, enforcement difficulties experienced by the national competent authority, or derogations granted. The Commission can also request additional information. Information provided to or received by the Commission in this context shall only be used for the purposes for which it was provided or received.

The Commission may provide guidance to Member States on the implementation of sanctions, which can take the form of FAQs[13] or opinions.[14]

---

11 Proposal for a Directive of the European Parliament and of the Council on the definition of criminal offences and penalties for the violation of Union restrictive measures, COM/2022/684 final, 2 December 2022.

12 Council of the European Union, Proposal for a Directive of the European Parliament and of the Council on the definition of criminal offences and penalties for the violation of Union restrictive measures, 17 May 2023, 9312/23.

13 See, for instance, 'Commission Consolidated FAQs on the implementation of Council Regulation No. 833/2014 and Council Regulation No. 269/2014', 22 June 2022, https://finance.ec.europa.eu/system/files/2023-07/faqs-sanctions-russia-consolidated_en.pdf (last updated 6 July 2023, accessed 7 July 2023).

14 See, for instance, 'Commission Opinion of 19.6.20 on Article 2 of Council Regulation (EU) No. 269/2014', C(2020) 4117 final.

On 4 March 2022, the European Commission introduced the EU Sanctions Whistleblower Tool, which allows anyone to voluntarily and anonymously report a violation of EU restrictive measures. The Commission examines reports and conducts a preliminary inquiry into the reported sanctions violation. If the Commission considers that the information provided by the whistle-blower is credible, the anonymised report is shared, along with any additional information, with the national competent authorities in the relevant Member State or States. The Commission may provide further assistance to the investigation and periodically follow-up on the investigation until a conclusion is reached.[15]

In March 2022, to ensure coordination in the implementation of individual sanctions against Russia, the Commission also set up a 'Freeze and Seize Task Force' composed of the Commission, national contact points from each Member State, Eurojust, Europol and other EU agencies and bodies. The Task Force's objective is to explore the interplay between sanctions and criminal law measures and to provide a platform where Member States can explore whether any listed individuals or companies have been involved in criminal proceedings. The Task Force coordinates actions by Member States to freeze and, where necessary, confiscate assets of listed persons and entities.[16]

The Commission also created the new position of EU Sanctions Envoy, whose role is to ensure continuous, high-level discussions with third countries to avoid the evasion or circumvention of sanctions. On 23 February 2023, the first Sanctions Coordinators Forum, gathering Member States and several third-countries partners, was held.[17]

Role of the Council of the EU

The Council of the European Union adopts restrictive measures and designs the enforcement framework.

---

15 See European Commission, EU Sanctions Whistleblower Tool, https://eusanctions.integrityline.com/app-page;appPageName=What%20happens%20with%20the%20report.

16 Press Releases, European Commission, 'Enforcing sanctions against listed Russian and Belarussian oligarchs: Commission's "Freeze and Seize" Task Force steps up work with international partners', 17 March 2022, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_1828; '"Freeze and Seize Task Force": Almost €30 billion of assets of Russian and Belarussian oligarchs and entities frozen by the EU so far', 8 April 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2373.

17 See 'Statement by EU Sanctions Envoy David O'Sullivan on the first Sanctions Coordinators Forum', 23 February 2023, https://finance.ec.europa.eu/news/statement-eu-sanctions-envoy-david-osullivan-first-sanctions-coordinators-forum-2023-02-23_en.

Within the Council, the Working Party of Foreign Relations Counsellors (RELEX) deals with legal, financial and institutional issues of the CFSP. Sanctions are among the Working Party's priorities. The main task of the RELEX 'Sanctions formation' is to share best practices and to revise and implement common guidelines to ensure effective and uniform implementation of EU sanctions regimes.[18] In June 2022, the Council updated the EU Best Practices for the effective implementation of restrictive measures.[19]

Furthermore, in an unprecedented move, on 6 October 2022, in the context of the sanctions regime against Russia, the Council adopted a new designation criterion targeting 'natural or legal persons, entities or bodies facilitating infringements of the prohibition against circumvention of the provisions of [regulations and decisions related to restrictive measures against Russia]'.[20] This means that, on the basis of information provided by Member States, the Council will be able to adopt restrictive measures against persons and entities that facilitated the circumvention of the restrictive measures provided for within the sanctions regime.

Role of the EU courts

EU courts have a limited role in the enforcement of sanctions. They do not have 'jurisdiction with respect to the provisions relating to the [CFSP] nor with respect to acts adopted on the basis of those provisions'.[21] Pursuant to Article 275, Paragraph 2 of the TFEU, EU courts only have jurisdiction to review 'the legality of decisions providing for restrictive measures against natural or legal persons', which can lead to a person being delisted.

Moreover, national courts can refer preliminary questions to the Court of Justice of the European Union (CJEU) on the validity of an act adopted on the basis of provisions relating to the CFSP, provided that the request for a preliminary ruling relates either to the monitoring of that decision's compliance with Article 40 of the TEU or to the reviewing of the legality of restrictive measures against natural or legal persons, as described above.[22]

---

18 See www.consilium.europa.eu/en/council-eu/preparatory-bodies/working-party-foreign-relations-counsellors/.

19 'Update of the EU Best Practices for the effective implementation of restrictive measures', 10572/22, 27 June 2022, https://data.consilium.europa.eu/doc/document/ST-10572-2022-INIT/en/pdf.

20 Council Regulation (EU) 2022/1905 of 6 October 2022 amending Regulation (EU) No. 269/2014.

21 Article 275, Paragraph 1, Treaty on the Functioning of the European Union.

22 CJEU (Grand Chamber), 28 March 2017, *Rosneft*, C-72/15, ECLI:EU:C:2017:236, section 81.

Consequently, the CJEU has rendered certain judgments on preliminary rulings that have some relevance to the enforcement of sanctions.

In *Rosneft*, the Court ruled that the principles of legal certainty and *nulla poena sine lege certa* do not preclude a Member State from imposing criminal penalties that are to be applied in the event of an infringement of the provisions of Council Regulation (EU) No. 833/2014 (providing for sectorial restrictive measures against Russia), to ensure its effective implementation, even though the scope of the provisions of the Regulation and of the associated criminal penalties have not been clarified.[23]

In *Afrasiabi and others*, the Court clarified the interpretation of the prohibitions related to the freezing of assets of designated persons, binding on all persons under EU jurisdiction: the prohibition to, directly or indirectly, make funds or economic resources available to a designated person; and the prohibition to participate, knowingly and intentionally, in activities of which the object or effect is to circumvent the first prohibition.[24]

Criticism of the EU enforcement framework

Lack of consistency

As described above, the enforcement of EU sanctions is a decentralised process that essentially relies on 27 individual Member States and their respective national competent authorities. There is a lack of harmonisation among Member States, which, depending on their resources and political impetus, enforce EU sanctions to different degrees. While some Member States have developed specific frameworks and bodies for the enforcement of EU sanctions,[25] others struggle to efficiently pursue their enforcement. This lack of consistency can create avenues for sanctions evasion.

In addition to the varying extents to which Member States enforce sanctions, differences can also be seen in their interpretation of sanctions.

For instance, to determine the scope of the freezing of funds and economic resources of designated persons, national competent authorities and economic operators must assess whether the designated person or entity has ownership or

23 id., sections 158–170.

24 CJEU, 21 December 2011, *Afrasiabi and others*, C-72/11, ECLI:EU:C:2011:874.

25 A case in point is the adoption of the Sanctions Enforcement Acts I and II by Germany in May 2022, which granted additional powers to the authorities to enforce restrictive measures and which created a new federal body, the Central Office for Sanctions Enforcement.

control over specific funds or economic resources.[26] Despite guidance issued by the European Commission and the Council, this assessment can lead to different results among Member States, which means that an individual company can be treated as frozen in some Member States and not in others.

Furthermore, the publicity of penalties for sanctions violations and of derogations granted by national competent authorities is inconsistent among Member States, which hinders economic operators in grasping the scope of their obligations and rights under the different EU sanctions regimes.

This lack of harmonisation and coordination leads to legal uncertainty and weakens EU sanctions regimes.

Scope for evasion

The lack of consistency in the enforcement of EU sanctions among Member States leaves room for sanctions evasion. The scope for evasion is also increased by the limited scope of application of EU sanctions regimes.

Contrary to US sanctions regimes, which, through the notions of secondary sanctions and US nexus, apply to numerous operators beyond the limits of the US territory, EU restrictive measures do not apply extraterritorially.[27] The EU has been rather opposed to the extraterritoriality of sanctions.[28] EU restrictive measures only apply on Union territory, to EU citizens wherever they are located and to third-country nationals outside the territory of the Union in respect of business conducted within the Union.[29]

Because of this limited scope of application, it has been observed that some third-country individuals, companies or even third countries themselves, act as transit destination for products covered by prohibitions under EU sanctions regimes.

---

26 See, for instance, Article 2 of Council Regulation (EC) No. 1183/2005 of 18 July 2005 imposing certain specific restrictive measures directed against persons acting in violation of the arms embargo with regard to the Democratic Republic of the Congo.

27 See, for instance, 'Frequently asked questions: Restrictive measures (sanctions)', European Commission, 26 February 2022, https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1401.

28 See, for instance, Council Regulation (EC) No. 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom.

29 See, for instance, Article 24 of Council Regulation (EU) 2016/44 of 18 January 2016 concerning restrictive measures in view of the situation in Libya and repealing Regulation (EU) No. 204/2011.

To address these schemes, in the context of the sanctions regime against Russia, the Union has recently decided that, as a last resort measure, it would be possible to prohibit the sale, supply, transfer or export of certain goods and technology to some specifically designated third countries whose jurisdiction is demonstrated to be at risk of being used for circumvention.[30]

Investigating suspected breaches

The investigation of suspected sanctions violations relies on Member States and, to some extent within the framework of the whistle-blower tool, the European Commission.

Reporting, professional secrecy and legal professional privilege

Regulatory reporting

Council regulations providing for sanctions contain a reporting obligation binding on all persons under EU jurisdiction. 'Natural and legal persons, entities and bodies shall supply immediately any information which would facilitate compliance with' the regulations to their national competent authority and 'shall cooperate with the competent authority in any verification of this information'.[31] This obligation often specifies that the information may concern accounts and amounts frozen.

Council Regulation (EU) No. 269/2014, which addresses actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, provides for a reinforced reporting obligation, which also expects any person and entity to report:

- information on funds and economic resources of designated persons or entities that have not been treated as frozen by the natural and legal persons or entities obliged to do so; and
- information held on funds and economic resources of designated persons or entities that have been subject to 'any move, transfer, alteration, use of, access to, or dealing' in the two weeks preceding the listing of those persons or entities to the competent authority of the Member State where they are resident or located, within two weeks of this information being required.[32]

---

30 Article 12f of Council Regulation (EU) No. 833/2014, as amended by Council Regulation (EU) 2023/1214 of 23 June 2023; see Recital 13 of Regulation (EU) 2023/1214.

31 See, for instance, Article 8, Paragraph 1 of Council Regulation (EU) 2019/1716 of 14 October 2019 concerning restrictive measures in view of the situation in Nicaragua.

32 Article 8, Paragraph 1 of Regulation (EU) 269/2014.

Furthermore, some regulations provide for other specific reporting obligations, which are binding on certain categories of persons.

For instance, in the sanctions regime against North Korea, there is an obligation for credit and financial institutions to report any suspicious transactions, including attempted transactions, and to notify the competent authorities 'where there are reasonable grounds to suspect that funds could contribute to the DPRK's nuclear-related, ballistic-missile-related or other weapons of mass destruction-related programmes or activities'.[33]

The sanctions regime against Russia contains further specific reporting obligations:

- any person or entity shall inform the national competent authority within two weeks of all transactions for the purchase, import or transfer into the Union or into third countries of natural gas condensates of subheading CN 2709 00 10 from liquefied natural gas production plants, originating in or exported from Russia;[34]
- any person or entity, including the European Central Bank, national central banks, financial sector entities, insurance and reinsurance undertakings, central securities depositories and central counterparties shall provide information on assets and reserves of the Central Bank of Russia that they hold or control or are a counterparty to, and report an extraordinary loss or damage to these assets and reserves, to the national competent authority;[35]
- credit institutions must supply information to the national competent authority regarding deposits of Russian nationals or natural persons residing in Russia, or by legal persons, entities or bodies established in Russia, exceeding €100,000;[36] and
- central securities depositories shall report any information on extraordinary and unforeseen loss and damage concerning designated persons' funds and economic resources within the territory of the Union.[37]

---

33 Article 23, Paragraph 1(e) and (f) of Council Regulation (EU) 2017/1509 of 30 August 2017 concerning restrictive measures against the Democratic People's Republic of Korea and repealing Regulation (EC) No. 329/2007.

34 Articles 3m, Paragraph 11 and 3n, Paragraph 12 of Council Regulation (EU) No. 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

35 id., Article 5a, Paragraphs 4a and 4b.

36 id., Article 5g.

37 Article 8, Paragraph 1b of Council Regulation (EU) No. 269/2014.

Moreover, under this sanctions regime, designated persons and entities themselves must report their funds and economic resources located within the territory of the Union to the national competent authority.[38]

Certain businesses and professions are bound by additional reporting obligations under national law.

Professional secrecy and legal professional privilege

Reporting obligations under EU sanctions apply without prejudice to the applicable rules concerning confidentiality and professional secrecy. This means that, where a person is bound by confidentiality or professional secrecy, they are not expected to breach these rules to comply with the EU sanctions reporting obligation.

Nevertheless, the general reporting obligation provided for by the Council of the European Union under the sanctions regime addressing Russia's invasion of Ukraine applies '*notwithstanding* the applicable rules concerning reporting, confidentiality and professional secrecy, and consistent with respect for the confidentiality of communications between lawyers and their clients guaranteed in Article 7 of the Charter of Fundamental Rights of the European Union'.[39]

The European Commission has provided further guidance on the application of this reporting obligation and has explained that the obligation would 'trump relevant agreements entered into by the EU operators in question, who would be obliged to report all relevant data including names, individual assets and dates of transfers'.[40]

Recent investigations and enforcement decisions

One of the flaws of EU sanctions enforcement is the limited number of published decisions concerning breaches and the lack of a centralised platform on which to find these decisions. This notably leads to a lack of legal certainty regarding what may constitute an 'effective, proportionate and dissuasive' penalty as required under Council regulations and undermines the deterrence effect that these penalties may have.

---

38 id., Article 9, Paragraph 2. Two challenges against this obligation are pending before the General Court of the European Union.

39 id., Article 8, Paragraph 1, as amended by Council Regulation (EU) 2023/1215 of 23 June 2023 (emphasis added).

40 Commission consolidated FAQs (footnote 12), Question 30.

Set out below are a few recent decisions and investigations on EU sanctions breaches.

The Netherlands

In a case involving an alleged breach of the prohibition to make funds or economic resources available to listed terrorist organisations under Council Regulation (EC) No. 881/2002, on 10 January 2023 the Dutch Supreme Court ruled that the applicable standard of proof for intentional violations of EU restrictive measures under Dutch law is generally low. It ruled that, for an international violation of EU restrictive measures to be established, it is not necessary to demonstrate that the defendant had the intent to breach the legal provisions concerned; it is sufficient to demonstrate the defendant's intention with regard to the constituent elements of the relevant prohibition.[41]

In another case, in 2022 a Dutch bank notified the Financial Intelligence Unit of suspicious transactions by a company exporting radio electronic components, steel and metal products, and cables and wiring. The company, which was significantly increasing its turnover, was exporting to non-sanctioned third countries. In September 2022, with the support of Europol's European Financial and Economic Crime Centre, the Dutch Fiscal Information and Investigation Service arrested a 55-year-old individual, the founder of the company, believed to have been supplying Russia with microchips by pretending that these goods had a different destination than the actual final one (Russia) to circumvent EU restrictive measures against Russia.[42]

Lithuania and Belarus

In February 2023, following an investigation conducted by Lithuania and Belarus exposing how EU sanctions against Grodno Azot, one of the largest fertiliser manufacturers in Belarus, have been evaded by changing the name of the fertiliser

41 Judgment, https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:HR:2023:2; 'Dutch Supreme Court confirms low standard of proof for intentional EU sanctions violations', Derk Christiaans, Paul Amberg and Sietske Brinksma, Sanctions & Export Controls Update, 20 January 2023, https://sanctionsnews.bakermckenzie.com/dutch-supreme-court-confirms-low-standard-of-proof-for-intentional-eu-sanctions-violations/.

42 Press Release, Europol, 'Suspect arrested in the Netherlands for circumventing EU trade sanctions against Russia', www.europol.europa.eu/media-press/newsroom/news/suspect-arrested-in-netherlands-for-circumventing-eu-trade-sanctions-against-russia; 'Dutch suspect evaded sanctions by exporting microchips to Russia through third countries', *NL Times*, 13 February 2023, https://nltimes.nl/2023/02/13/dutch-suspect-evaded-sanctions-exporting-microchips-russia-third-countries.

producer on customs documents, the Lithuanian authorities conducted raids of companies presumed to be involved in this scheme and seized thousands of tonnes of Belarusian fertiliser.[43]

Belgium

Three companies and two managers have been condemned by the criminal court of Antwerp for shipping 168 tonnes of a substance potentially used in the making of chemical weapons (isopropanol) to Syria between 2014 and 2016 without the required licences, in violation of EU sanctions against Syria. The companies were ordered to pay fines of up to €500,000, despite there being no evidence that this substance had been used to make chemical weapons.

Denmark

On 14 December 2021, the Court of Odense fined fuel supplier Dan-Bunkering and its parent company Bunker Holding for having sold 172,000 tonnes of jet fuel in Syria between 2015 and 2017, in breach of EU sanctions against Syria. Dan-Bunkering was fined 30 million Danish kroner and Bunker Holding was fined 4 million kroner. The CEO of Bunker Holding was also given a suspended sentence of four months' imprisonment.

The future of EU sanctions enforcement

In recent years, particularly in recent months, EU sanctions have developed vigorously, and sanctions regimes have become increasingly complex. However, the challenge remains for these sanctions to be properly enforced in an environment of surprisingly ingenious methods of evasion and circumvention.

In this context, the Union is looking into avenues to tackle all types of circumvention. For instance, while it appears that, when prohibited under EU sanctions, the trade of certain goods with targeted countries finds ways to continue by transiting through certain third countries, the Union is considering sanctioning the export of these goods with the third countries in question.[44]

---

43 Šarūnas Černiauskas, 'Lithuania Cracks Down on Sanction Evasion Schemes after OCCRP Investigation', OCCRP, 2 March 2023, www.occrp.org/en/daily/17377-lithuania-cracks-down-on-sanction-evasion-schemes-after-occrp-investigation.

44 See 'Press statement by President von der Leyen with Ukrainian President Zelenskyy', 9 May 2023, https://ec.europa.eu/commission/presscorner/detail/en/statement_23_2661 and Article 12f of Regulation (EU) 833/2014, as amended by Council Regulation (EU) 2023/1214 of 23 June 2023.

Following the criminalisation of the violation of EU restrictive measures under Council Decision (EU) 2022/2332 of 28 November 2022 – and based on the proposal adopted by the European Commission – the Council and the Parliament are expected to adopt a directive on the definition of criminal offences and penalties for the violation of Union restrictive measures that would contribute to the harmonisation of the sanctioning of breaches by Member States.[45]

In addition, the role that the European Public Prosecutor Office (EPPO) could play in the investigation and prosecution of violations of sanctions is under discussion. The extension of the EPPO's powers would be adopted pursuant to Article 86(4) of the TFEU.[46]

In his statement during the first Sanctions Coordinators Forum, the EU Sanctions Envoy, David O'Sullivan, stressed the key responsibility of the EU and its international allies to fully and unconditionally implement restrictive measures and to tackle circumvention from all angles.[47]

In the past year, in the context of the development of sanctions against Russia, there has been increasing interest in enforcing sanctions and combatting circumvention. Several initiatives have already been undertaken by the Union to that end, including the creation of both the Freeze and Seize Task Force, to enhance inter-EU information sharing on frozen assets, and the EU Sanctions Envoy position, to coordinate with international allies. Other initiatives are currently being discussed at EU level and could be implemented in the short to medium term.

Conclusion

In its pursuit of the development of a tighter enforcement framework, the EU is looking into more efficient ways to tackle loopholes and to penalise violations of EU sanctions. However, the Union's institutions remain bound by the limits of their competences, and the legal avenues available for strengthening the enforcement of sanctions at the EU level may appear rather narrow. In this context, the extension of the EPPO's powers could create a path for extending the role of the Union in the enforcement of EU sanctions.

45 See footnote 11.

46 See Parliamentary question E-003966/2022, 'Answer given by Mr Reynders on behalf of the European Commission', 23 January 2023, www.europarl.europa.eu/doceo/document/E-9-2022-003966-ASW_EN.html.

47 See footnote 17.

CHAPTER 3

UK Sanctions

Paul Feldberg, Robert Dalling, Karam Jardaneh and Anna Gaudoin[1]

Introduction

Following the end of the Brexit transition period on 31 December 2020, EU sanctions legislation is no longer directly applicable in the UK. While the UK and the EU continue to cooperate on sanctions policy, along with other countries such as the US, there are now significant differences in terms of both legislation and lists of designated persons. In practice, this means that there is now an additional sanctions regime for multinational companies to comply with, a fact underscored by increasing variations between the EU and the UK with regard to sanctions introduced in response to the Russian invasion of Ukraine. While the approach of the UK and EU has been similar in policy terms, there have been pronounced differences between the two sanctions regimes.

Although EU sanctions legislation is no longer directly applicable in the UK, the United Nations (UN) sanctions regime continues to apply in the UK.

The legislative framework for the UK's sanctions regime is found in the Sanctions and Anti-Money Laundering Act 2018 (SAMLA). SAMLA is a substantial piece of legislation that has transformed the way in which sanctions in the UK are created, enforced and challenged. In this chapter we look at the shape of the UK's regime under SAMLA.

---

1 Paul Feldberg and Robert Dalling are partners, and Karam Jardaneh and Anna Gaudoin are senior associates, at Jenner & Block London LLP.

UK sanctions bodies and authorities

A number of different entities share responsibility for formulating sanctions policy and implementing, administering and enforcing sanctions legislation in the UK. The Foreign, Commonwealth and Development Office (FCDO) is responsible for overall UK government policy on international sanctions.

Financial sanctions are administered and implemented by His Majesty's Treasury (HM Treasury), and specifically by the Office of Financial Sanctions Implementation (OFSI), which was established in 2016 to 'provide a high-quality service to the private sector, working closely with law enforcement to help ensure that financial sanctions are properly understood, implemented and enforced'.[2] OFSI deals with applications for financial sanctions licences and any necessary notifications and authorisations, and has the power to impose monetary penalties for breaches of financial sanctions.[3] Law enforcement agencies, such as the National Crime Agency, the Serious Fraud Office, the Crown Prosecution Service and HM Revenue and Customs (HMRC), may also investigate and bring enforcement action in respect of sanctions breaches. For further information about the enforcement of UK sanctions, see Chapter 4 of this Guide. Immigration sanctions prohibiting entry into the UK (commonly known as 'travel bans') are administered by the Home Office.[4]

Trade sanctions are administered and implemented by the Department for Business and Trade (DBT). The Export Control Joint Unit (ECJU), which is part of the DBT, administers the UK's system of export controls and licensing for military and dual-use items, as well as licences issued under the UK's various trade sanctions regimes. See Chapter 8 for further information about the UK export control regime.

---

2 HM Treasury, 'New body to support financial sanctions implementation launched', www.gov.uk/government/news/new-body-to-support-financial-sanctions-implementation-launched.

3 See the Office of Financial Sanctions Implementation (OFSI) guidance 'UK Financial Sanctions – General Guidance for financial sanctions under the Sanctions and Anti-Money Laundering Act 2018' (OFSI General Guidance), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1144366/General_Guidance_-_UK_Financial_Sanctions__Aug_2022_.pdf.

4 Foreign, Commonwealth and Development Office, UK Sanctions Guidance, www.gov.uk/guidance/uk-sanctions.

Sources of UK sanctions

Until recently, the UK largely followed the EU and the UN in terms of substantive sanctions measures, with the UK's autonomous sanctions powers exercised sparingly. While SAMLA facilitates the continued application of UN sanctions in the UK, it also significantly expands the scope of the UK's autonomous sanctions powers.

SAMLA gives powers to the 'appropriate minister' in the UK, defined as the relevant Secretary of State or HM Treasury,[5] to make regulations imposing sanctions. The appropriate minister can make regulations when the minister considers it is 'appropriate', for the following purposes:[6]

- to comply with an obligation that arises as a result of a UN Security Council Resolution;
- to comply with any other international obligation (which could include obligations arising from UK membership of other international organisations (for example, the Organization for Security and Co-operation in Europe) as well as other international treaties or agreements); or
- for other purposes specified in Section 1(2) of SAMLA, including the prevention of terrorism (in the UK or elsewhere); furthering the interests of national security or the interests of international peace and security; furthering a foreign policy objective of the UK; promoting the resolution of armed conflicts or the protection of civilians in conflict zones; deterring gross violations of human rights; promoting compliance with human rights law; preventing the spread and use of weapons and materials of mass destruction; and promoting respect for democracy, the rule of law and good governance.[7]

In line with the discretionary purposes linked to human rights (as listed above), the UK government adopted a Global Human Rights Sanctions regime on 6 July 2020, followed by the Global Anti-Corruption Sanctions regime on 26 April 2021. In addition, in the run up to the end of the Brexit transition period, the UK government laid down secondary legislation under SAMLA

5 Sanctions and Anti-Money Laundering Act 2018 (SAMLA), Section 1(9).

6 id., at Section 1, Paragraphs (1) and (2).

7 The Economic Crime (Transparency and Enforcement) Act 2022 removed certain additional requirements relating to the making of regulations for any of the discretionary purposes under Section 1(2); namely the requirement that a purpose could only be considered to be 'appropriate' if the minister was satisfied that there were good reasons to pursue the purpose and that the imposition of sanctions was a reasonable course of action for that purpose.

for over 30 sanctions regimes. Through these regulations, which came fully into force on 31 December 2020,[8] the UK government intended to deliver substantially the same policy effects as existing regimes that were implemented by the EU, although the legislation is not identical. Since December 2020, the UK has amended certain regimes extensively (for example, the Russia regime), while other regimes remain unchanged.

Types of sanctions

SAMLA provides for a wide range of sanctions to be imposed by regulations, including financial sanctions, trade sanctions, immigration sanctions, and aircraft and shipping sanctions.

Financial sanctions made pursuant to SAMLA may contain prohibitions and requirements that are similar but not identical to those found in EU sanctions (covered in Chapter 2 of this Guide). Under Section 3 of SAMLA, regulations may:

- require the freezing of funds or economic resources owned, held or controlled by designated persons;
- restrict the provision of financial services to, or for the benefit of, designated persons (or persons 'connected with a prescribed country');
- prevent the making available of funds or economic resources to designated persons (as well as the receipt of funds or economic resources from them);
- prevent certain financial services being offered where they concern financial products issued by designated persons; and
- prevent the ownership or control of designated entities.

A breach of any of these prohibitions may be a criminal offence if the person or entity in question knows or has reasonable cause to suspect that the other person is designated under sanctions legislation and that person engages in prohibited conduct with the designated person, such as making funds available to them without a licence. A breach could also result in monetary penalties even where a person did not know or suspect they were breaching the prohibitions. Most prohibitions imposed by UK sanctions law are supported by prohibitions on circumventing the main prohibitions and on enabling or facilitating the

8 For a full list of regimes under SAMLA that came into force on 31 December 2020, see OFSI's consolidated List Change Notice dated 28 February 2022, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1057742/280222_Consolidated_List_Change_Notice.pdf.

contravention of the main prohibitions.[9] Taken together, these prohibitions in effect prevent any individual or company subject to UK sanctions law from having any dealings of an economic nature with a designated person, if that individual or company knows or has reasonable cause to suspect that it is dealing with a designated person, even where those dealings would otherwise be perfectly lawful. The various prohibitions apply to dealing 'directly' as well as 'indirectly' with a designated person.

The OFSI guidance 'UK Financial Sanctions – General Guidance for financial sanctions under the Sanctions and Anti-Money Laundering Act 2018' (the OFSI General Guidance), most recently issued in August 2022,[10] warns that the prohibitions relating to 'financial services' under UK sanctions regulations will be interpreted more broadly than the prohibitions relating to 'financial assistance' under existing EU sanctions regimes. In particular, the prohibitions relating to financial services cover 'any service of a financial nature, including (but not limited to) payment and money transmission services, charge and debit cards, travellers' cheques and bankers' drafts'. Businesses and practitioners should therefore be alive to this difference between the two regimes, to ensure that conduct permissible under one regime does not result in an inadvertent breach of the other. The OFSI General Guidance is not legally binding as it does not form part of UK legislation or judge-made case law. However, it is valuable as an indicator of how the UK government interprets UK sanctions legislation. In the absence of judicial authority on a point of interpretation, it is sensible to follow the OFSI General Guidance. The OFSI General Guidance consolidates definitions already included in SAMLA and regime-specific regulations and provides further guidance and information in relation to its interpretation of these definitions.

- 'Funds' mean 'financial assets and benefits of every kind', including (but not limited to) cash, cheques, deposits with financial institutions, debts, all types of security (including stocks, shares, bonds, notes, warrants, derivatives contracts), interest, dividends, guarantees, letters of credit, bills of lading and bills of sale.[11]

9 See, for example, the Russia (Sanctions) (EU Exit) Regulations 2019 (the Russia Regulations), at Regulation 19.

10 See OFSI General Guidance, at Section 3.2.

11 id., at p. 15; SAMLA, at Regulation 60.

- 'Economic resources' mean 'assets of every kind – tangible or intangible, movable or immovable – which are not funds, but may be used to obtain funds, goods or services'. The phrase includes (but is not limited to) precious metals or stones, antiques, vehicles and property.[12]
- The Guidance indicates that cryptoassets will, in OFSI's view, fall within the definitions of 'funds' and 'economic resources'.[13]
- 'Dealing with funds', in the OFSI General Guidance, means 'moving, transferring, altering, using, accessing, or otherwise dealing with them in any way which would result in any change to their volume, amount, location, ownership, possession, character, destination or other change that would enable the funds to be used'.[14]
- 'Dealing with economic resources' means exchanging them 'for funds, goods or services', or using them 'in exchange for funds, goods or services (whether by pledging them as security or otherwise)'.[15] The OFSI General Guidance indicates that the phrase covers the use of 'economic resources to obtain funds, goods, or services in any way, including, but not limited to, by selling, hiring or mortgaging them'. It should be noted that the 'everyday use by a designated person of their own economic resources for personal consumption is not prohibited'.[16]
- 'Making available funds or economic resources for the benefit of a [designated person]' extends only to situations where the designated person obtains, or is able to obtain, a significant financial benefit as a result.[17] A financial benefit includes the discharge of a debt for which the designated person is wholly or partly responsible.[18]

As regards trade sanctions, which are covered in Section 5 and Schedule 1, SAMLA provides a raft of powers, including powers to restrict imports and exports to and from prescribed countries, as well as the power to restrict imports or exports when

12 ibid.

13 ibid.

14 ibid. This is consistent with interpretative provisions found in sanctions legislation, such as Regulation 11(4) of the Russia Regulations.

15 See, for example, Regulation 11(5) of the Russia Regulations.

16 See OFSI General Guidance, at p. 16.

17 See, for example, Regulation 13(4)(a) of the Russia Regulations.

18 See, for example, id., at Regulation 13(4)(b). In *Celestial Aviation Services Ltd v. UniCredit Bank AG (London Branch)* [2023] EWHC 663 (Comm), the court found (on an *obiter* basis) that payment by a confirming bank to a beneficiary under a letter of credit issued by a designated bank would not amount to a financial benefit for the designated bank.

they are for the benefit of a designated person, and to prevent the transfer of technologies to a designated person, as well as the sale of land to or by a designated person. Services relating to these imports, exports, transfers, sales and acquisitions may also be prevented by powers conferred by SAMLA.[19] See Chapter 8 of this Guide for further information about the UK export control regime.

Immigration sanctions are covered at Section 4 of SAMLA, which confers powers to refuse leave to enter or to remain in the UK.[20] Aircraft and shipping sanctions (covered in Sections 6 and 7, respectively) provide powers in relation to aircraft and ships connected to designated persons or prescribed countries, such as detaining them, preventing them from entering or leaving UK airspace or waters, and preventing their registration in prescribed countries.

The UK government has made extensive use of its powers under SAMLA in introducing sanctions in response to the Russian invasion of Ukraine; for example, the UK:

- expanded the grounds on which it can designate individuals and entities under the Russia (Sanctions) (EU Exit) Regulations 2019 (the Russia Regulations),[21] and, as at 27 March 2023, the UK has made 180 entities and 1,549 individuals subject to asset freezes under the Russia Regulations (see below for further information on designation);

19 The Export Control Joint Unit will remain responsible for controlling and licensing the export of controlled goods. See www.gov.uk/guidance/exporting-controlled-goods-after-eu-exit.

20 The UK government has published regulations relating to the exercise of these powers (the Immigration (Persons Designated under Sanctions Regulations) (EU Exit) Regulations 2020).

21 The Russia Regulations originally only provided for the designation of persons who are or have been involved in 'destabilising Ukraine or undermining or threatening the territorial integrity, sovereignty or independence of Ukraine'. Under Regulation 6 of the Russia Regulations, the UK can now designate persons who are or have been 'involved in . . . obtaining a benefit from or supporting the Government of Russia'. This includes persons: (1) carrying on business as a government of Russia-affiliated entity; (2) carrying on a business of economic significance to the government of Russia; (3) carrying on business in a sector of strategic significance to the government of Russia; (4) owning or controlling directly or indirectly, or working as a director, trustee, manager or equivalent of any of (1) to (3); and (5) holding the right, directly or indirectly, to nominate at least one director (whether executive or non-executive), trustee or equivalent of (1) to (3).

- prohibited certain credit or financial institutions from establishing or continuing a correspondent banking relationship with a designated person; or processing a sterling payment to, from or via a designated person, or a credit or financial institution (domiciled anywhere, including the UK) owned or controlled by a designated person;[22]
- enhanced existing capital markets and loan restrictions and prohibited dealings with transferable securities and money market instruments issued on behalf of, and the provision of certain loans or credit to, a wide range of persons, including persons connected with Russia (this includes companies incorporated or constituted under the law of Russia);[23]
- prohibited the provision of financial services for the purposes of foreign exchange reserve and asset management to: (1) the Central Bank of the Russian Federation; (2) the National Wealth Fund of the Russian Federation; (3) the Ministry of Finance of the Russian Federation; and (4) a person owned or controlled directly or indirectly by, or a person acting on behalf of or at the direction of, a person mentioned in (1) to (3);[24]
- introduced wide prohibitions on investments in Russia (including direct acquisition of any ownership interest in Russian land and persons connected with Russia);[25]
- introduced prohibitions on the provision of trusts services to or for the benefit of designated persons or those connected with Russia;
- expanded trade-related restrictions under the Russia Regulations; for example, this includes restrictions on:
    - the export and supply of aviation and space goods and luxury goods to Russia;[26]
    - the import, acquisition and supply of iron and steel products from Russia;[27]
    - the import, acquisition, supply and delivery of Russian oil and oil products into the UK;[28] and

22 Regulation 17A of the Russia Regulations.

23 Regulations 16 and 17 of the Russia Regulations.

24 id., at Regulation 18A.

25 id., at Regulation 18B.

26 id., at Regulation 46B.

27 id., at Regulations 46C–46F.

28 id., at Regulations 46Z3–46Z6. See also Guidance, 'UK ban on Russian oil and oil products', www.gov.uk/government/publications/uk-ban-on-russian-oil-and-oil-products/uk-ban-on-russian-oil-and-oil-products.

    - maritime transportation of oil and oil products from a place in Russia to a third country;[29] and
- prohibited the direct or indirect provision of professional and business services (accounting, advertising, architectural, auditing, business and management consulting, engineering, IT consultancy and design, and public relations services) to persons connected with Russia.[30]

Territorial extent and application

The provisions of SAMLA and regulations made under it are enforceable against persons within the UK, including the UK's territorial waters.[31] The regulations made under SAMLA may extend to:

- 'British ships in foreign waters or international waters';[32]
- 'ships without nationality in international waters';[33] and
- 'foreign ships in international waters'.[34]

The provisions of SAMLA also apply to all UK persons, wherever they are in the world. A UK person is a UK national or a body incorporated or constituted under the law of any part of the UK.[35] This means that UK entities and their non-UK

29 id., at Regulation 46Z9B. However, the UK also introduced a coordinated price cap exception to the maritime transportation and associated services ban. This deprives Russia of access to excess oil revenues by constraining its ability to sell at global market prices, while still enabling Russian oil to flow to the third countries that need it. See also 'UK Maritime Services Ban and Oil Price Cap – Industry Guidance', https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1140563/OFSI_Industry_Guidance_-_Maritime_Services_Prohibition_and_Oil_Price_Cap_-_March_2023__1_.pdf.

30 id., at Regulation 54C. See also Guidance, 'Supplying professional and business services to a person connected with Russia', www.gov.uk/government/publications/professional-and-business-services-to-a-person-connected-with-russia/professional-and-business-services-to-a-person-connected-with-russia.

31 SAMLA, at Sections 21(1)(a) and 6(1).

32 id., at Section 19(1)(a) and (11). When exercising this power in relation to a foreign ship, the Secretary of State must approve the action. In this instance, the Secretary of State's approval is contingent on either that ship's home state requesting the assistance of the UK or there being a basis for the action under international law. These powers are not extended to aircraft.

33 id., at Section 19(1)(b).

34 id., at Section 19(1)(c).

35 id., at Section 21(1)(b).

branches must comply with UK sanctions law even when their activities take place abroad.[36]

OFSI has published guidance on civil monetary penalties for financial sanctions breaches (the OFSI Monetary Penalties Guidance), most recently issued in March 2023. This sets out OFSI's approach to jurisdictional issues, confirming that it will only seek to enforce breaches of UK financial sanctions where there is a link to the UK.

OFSI considers that:

> *a UK nexus might be created by such things as a UK company working overseas, transactions using clearing services in the UK, actions by a local subsidiary of a UK company (depending on the governance), action taking place overseas but directed from within the UK, or financial products or insurance bought on UK markets but held or used overseas.*[37]

The OFSI Monetary Penalties Guidance states that this list is not intended to be exhaustive or definitive. We should note that, although this Guidance relates to civil monetary penalties, we would expect OFSI to adopt a similar approach when considering jurisdictional issues in relation to potential criminal sanctions violations. For further information about the enforcement of UK sanctions, see Chapter 4 of this Guide.

Liability in the event of a UK sanctions law breach

As with breaches of other provisions of UK criminal law, liability under UK sanctions law may attach to both individuals and entities.[38] For further information about the enforcement action that may be taken in response to a breach of UK sanctions law, see Chapter 4.

---

36 id., at Section 21(2)(b).

37 OFSI Monetary Penalties Guidance, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1143219/March_2023_Monetary_Penalty_and_Enforcement_Guidance.pdf, at Section 3.8.

38 Although the substantive sanctions laws discussed in this chapter have effect throughout the UK (and in some cases have extraterritorial effect), issues of criminal liability are determined by reference to the law of the constituent parts of the UK (i.e., England and Wales, Scotland and Northern Ireland, depending on where criminal proceedings are brought). In this chapter, we deal with liability under the laws of England and Wales (i.e., how issues of liability would be determined in the courts of England and Wales).

There are a number of ways in which criminal liability may arise in respect of UK sanctions laws. First, a person may be prosecuted in any part of the UK for a breach of UK sanctions law where that person is directly involved in the commission of the offence, regardless of where they are in the world when they breach the law.

Second, a person may be liable under ordinary principles of criminal law on the basis of less direct forms of involvement. These alternative routes to liability include:

- encouraging or assisting another person to commit an offence;[39]
- (in relation to many sanctions laws), enabling or facilitating the contravention of a prohibition;[40] and
- conspiring (agreeing) with another person to commit an offence.[41]

Third, certain individuals may be liable as a result of a finding of liability on the part of a company or entity (corporate liability is discussed below). Sanctions laws typically provide that a director, manager, secretary or other similar officer of a body corporate will be liable where the entity commits an offence as a result of the consent, connivance (agreement) or neglect of that individual.[42] These provisions are intended to capture any individual occupying a managerial position within an entity.

A corporate entity may only be prosecuted for a crime in limited circumstances. The law of England and Wales is more restrictive than that of the US, for example, or other jurisdictions that have adopted a broad system of vicarious liability in which a company may be criminally liable for the acts of an employee provided that the employee was acting in the course of their employment.

In the case of a company, criminal liability for breach of sanctions legislation would arise only if:

- a person at a senior level within the organisation, typically at director level, was involved in the commission of an offence in the course of their employment;[43] or

39 Under Part 2 of the Serious Crime Act 2007.

40 See, for example, Regulation 19 of the Russia Regulations.

41 Under Part 1 of the Criminal Law Act 1977.

42 See, for example, Regulation 81 of the Russia Regulations.

43 See *Tesco Supermarkets Ltd. v. Nattrass* [1971] UKHL 1.

- the company's board delegated full authority for a particular activity or category of activities to one or more individuals, and those individuals committed an offence in the course of their employment[44] (again by reference to one of the first two scenarios outlined above).

OFSI also has powers to impose monetary penalties if it is satisfied that on the balance of probabilities a person breached a prohibition or failed to comply with an obligation under UK sanctions law.[45] The UK government introduced the Economic Crime (Transparency and Enforcement) Act 2022 very soon after the Russian invasion of Ukraine. The Act removed the requirement for OFSI to prove that a person must have known or suspected they were breaching UK sanctions law, when considering imposing a financial penalty. All that OFSI is now required to prove on the balance of probabilities, to levy a financial penalty, is that the entity or person breached the prohibition.[46] This effectively makes breaching sanctions a strict liability civil offence.

Designation process

Designation lists

The UK currently maintains three lists of designations made under sanctions legislation. OFSI continues to maintain two lists of those subject to financial sanctions, one listing asset freeze designations (the Consolidated List) and the other listing entities subject to capital market restrictions under the Russian sanctions regime (the Investment Ban Targets List).

Post-Brexit, the UK also maintains a third list, the UK Sanctions List, maintained by the FCDO. This is a more extensive list, which consists of all designations made under UK sanctions (financial or otherwise).

Designation by name

SAMLA empowers relevant ministers to designate individuals and entities where the minister has reasonable grounds to suspect[47] that the person is involved in, or connected to, an activity set out in the regulations for a particular sanctions

44 See *The Serious Fraud Office v. Barclays PLC & ANR* [2018] EWHC 3055 (QB), www.judiciary.uk/wp-content/uploads/2020/02/sfo-v-barclays-judgment-12-11-18.pdf.

45 Section 146 of the Policing and Crime Act 2017.

46 Section 54 of the Economic Crime (Transparency and Enforcement) Act 2022.

47 In *LLC Synesis v. Secretary of State for Foreign, Commonwealth and Development Affairs* [2023] EWHC 541 (Admin), the High Court found that the statutory threshold for 'reasonable grounds to suspect' is distinct from the standard of review applied by courts when

regime (an involved person[48]).[49] The UK government removed the stipulation that the minister must also consider that it is appropriate to designate that person (this was in response to criticism that its process for designating individuals and entities took too long).[50] It is important to note that an entity can be designated on the basis that it is owned or controlled by another designated person, and the OFSI General Guidance indicates that the UK 'will look to designate owned or controlled entities/individuals in their own right where possible'.[51] However, as set out in more detail below, even if an entity is not explicitly designated, financial sanctions will also apply to that entity in its entirety if it is owned or controlled by a designated person, meaning that it is effectively designated as well.

In addition, SAMLA empowers relevant ministers to designate individuals and entities:

- that have been designated by the UN;[52] and
- on an expedited basis if that individual or entity has been designated by the US, EU, Australia or Canada (or other jurisdiction as specified by relevant regulations) and it is in the public interest to make a designation under the expedited procedure.[53]

Where an individual or entity is designated on an expedited basis, the relevant designation shall only last for 56 days, unless the relevant minister either certifies that the individual or entity continues to be sanctioned by an applicable jurisdiction and it is in the public interest for the designation to continue for a further 56 days, or that the minister has reasonable grounds to suspect that the individual or entity is an involved person.[54]

---

considering a designation: the former requires a state of mind rather than a state of affairs. In addition, the information and material open to consideration by the minister in making a decision is not limited to what would be admitted in a court of law but could include hearsay allegations and intelligence.

48 An 'involved person' could include an individual, group or organisation involved in an activity, or a person controlled by them, someone acting on their behalf or an associated person.

49 SAMLA, at Section 11.

50 See id., at the now repealed Section 11(2)(b) (repealed by the Economic Crime (Transparency and Enforcement) Act 2022).

51 See OFSI General Guidance, at Section 4.1.

52 SAMLA, at Section 1.

53 id., at Section 11, as amended by the Economic Crime (Transparency and Enforcement) Act 2022.

54 ibid.

When a person has been designated by name, the notification usually required by sanctions regimes created under SAMLA must include a brief statement of reasons. However, the minister does not have to disclose anything that might damage national security or international relations, the prevention or detection of serious crime, or the interests of justice.[55]

Designation by description

SAMLA also permits a minister to designate persons by description rather than by name. According to the Explanatory Notes to SAMLA, '[t]his power can only be exercised when it is not practicable for the Minister to identify by name all the persons falling within the description, and the description is sufficiently precise that a reasonable person would know whether any person falls within it.'[56]

Ownership and control

Section 62 of SAMLA permits specific definitions to be inserted into each sanctions regulation on ownership and control. SAMLA itself does not provide a definition for ownership and control. The regulations adopted to date generally contain identical provisions setting out the meaning and thresholds for ownership and control of an entity by a designated person. A company is owned or controlled directly or indirectly by another person if either or both of the following two conditions is met:

- the person holds directly or indirectly more than 50 per cent of the shares or voting rights in the company, or the right, directly or indirectly, to appoint or remove a majority of the board of its directors; or
- it is reasonable to expect that the person would '(if [the person] chose to) be able, in most cases or in significant respects, by whatever means and, whether directly or indirectly, to achieve the result that affairs of [the company] are conducted in accordance with [the person's] wishes'.[57]

The OFSI Monetary Penalties Guidance provides further useful context when assessing the ownership and control of entities. It states that where OFSI determines that an incorrect assessment of ownership and control of an entity is relevant to a breach of sanctions, it will consider the degree and quality of research and due

55 ibid. Section 10(4) of the Act provides that regulations made under SAMLA may make provision as to notification and publicity.

56 Explanatory Notes to SAMLA, Paragraph 58.

57 See, e.g., Regulation 7 of the Russia Regulations.

diligence conducted on the ownership and control of that entity.[58] Appropriate due diligence will be considered a mitigating factor where the ownership and control determination was reached in good faith and was a reasonable conclusion, while failure to carry out appropriate due diligence, or carrying out the due diligence in bad faith, will be considered an aggravating factor.[59] OFSI will also consider whether the level of due diligence conducted was appropriate to the degree of sanctions risk and the nature of the transaction.[60] The guidance includes examples of areas of enquiry that OFSI may expect to be undertaken in establishing whether an entity is owned or controlled by a designated person. This includes the percentage of shares or voting power (or both) of the shareholders; whether the ownership or shareholding has recently been altered or divested; whether there are indications of continued influence by a designated person; or the presence or involvement of proxies, including parties holding assets on behalf of a designated person.[61]

Further provisions on ownership and control are set out in schedules to each of the regulations adopted under SAMLA.

In addition, the definitions of ownership and control for the purposes of asset freezes may not be applicable for the purposes of other provisions of SAMLA and, therefore, they should always be carefully checked. For example, the UK's Russian sanctions regime imposes a slightly more limited test (without the control element) in the context of certain financial restrictions concerning loans and credit arrangements. In that context, an entity is owned by another person if the person holds directly or indirectly more than 50 per cent of the shares or voting rights in the company.[62]

As noted above, an entity owned or controlled by a designated person is liable to be designated expressly by the UK government. The OFSI General Guidance confirms that the 'UK Government will look to designate owned or controlled entities/individuals in their own right where possible'.[63] Further, after the original designation of an entity, it is likely that there will be additional designations under the ownership and control criteria as the Secretary of State becomes aware of individuals or entities linked to the already designated individuals and organisations.

---

58 See Section 3.22 of the OFSI Monetary Penalties Guidance.

59 id., at Section 3.24.

60 id., at Section 3.25.

61 id., at Section 3.29.

62 Regulation 16(7) of the Russia Regulations.

63 See Section 4.1 of the OFSI General Guidance. Note that this is only guidance: the actual interpretation of sanctions legislation is a matter for the courts.

However, the prohibitions on making funds or economic resources available directly or indirectly to a designated person also prohibit making them available to an entity that is owned or controlled, directly or indirectly, by the designated person even if that person is not explicitly recorded on the designation list. The OFSI General Guidance makes clear that if the relevant ownership and control criteria are met, 'and the person who owns or controls the entity is also a designated person, then financial sanctions will also apply to that entity in its entirety (meaning these assets should also be frozen)'. This means even if an entity is not explicitly named in a designation, financial sanctions will also apply to it if it is owned or controlled by a designated person. Therefore, companies will need to conduct significant due diligence when dealing with entities that may be linked to designated individuals and organisations.

Each regime-specific set of sanctions regulations will also need to be read alongside the OFSI General Guidance on ownership and control.[64] The OFSI General Guidance provides guidance on when an entity may become subject to an asset freeze if a designated person owns a minority interest in that entity. There is also guidance on how to deal with funds that are jointly owned by a designated person.

Unlike the EU guidance on ownership and control, the definitions adopted for the purposes of the SAMLA regulations are not presented as examples of circumstances in which ownership and control can be presumed unless rebutted, but instead as conclusive indicia of ownership and control for the purposes of the UK autonomous sanctions.

The OFSI General Guidance has been revised to clarify that the ownership of separately designated individuals will not be aggregated, unless (for example) the shares or rights of the designated persons are subject to a joint arrangement.[65] By contrast, the EU's approach, as clarified in a recent set of frequently asked questions, is to 'take into account the aggregated ownership' of an entity.[66] In practice, the level of due diligence conducted by a company with a view to questions of ownership and control is likely to vary depending on its sector and geographic exposure. Companies that are subject to due diligence requirements under anti-money laundering and counterterrorist financing regulations, or that have operated in high-risk sanctions countries such as Russia, are likely to have

64 See ibid.

65 id., at Section 4.1.4.

66 See EU FAQs, 'Assets freeze and prohibition to make funds and economic resources available', https://finance.ec.europa.eu/system/files/2023-05/faqs-sanctions-russia-consolidated_en_0.pdf.

in place procedures designed to identify the presence of a designated person in a company's ownership structure. Companies that fall outside the scope of anti-money laundering and counterterrorist financing regulations may well not have these types of procedures in place, although they are still subject to sanctions legislation, and will commit an offence if they deal with a designated person when they know, or have reasonable cause to suspect, that they are dealing with such a person.

Challenging designations and delisting under SAMLA

One of the key differences between the pre- and post-Brexit UK sanctions regimes is the way in which those subject to financial sanctions can challenge their designation. Under the pre-Brexit regime, persons designated under EU sanctions, by virtue of either a UN listing or an EU listing, were only able to challenge their designations at EU level and, to a more limited extent, UN level. SAMLA permits individuals and entities to challenge their listings in the UK or to request the UK's assistance to secure their removal from a UN list.

Although SAMLA provides a mechanism for those listed under UK and UN sanctions regimes to challenge their listing, many persons would also likely be designated under corresponding EU sanctions. As under the pre-Brexit regime, there is no mechanism to challenge EU designations in the UK. However, designation transposed into UK law pursuant to secondary legislation under SAMLA can be challenged in the UK. There are also likely to be complexities in seeking to challenge a designation under the expedited designation process where the UK government is in effect relying on the evidential basis put forward by another jurisdiction as justification for a designation.

Right to request variation or revocation of designation

SAMLA provides a designated person the right to ask the government to revoke or vary their designation;[67] for example, if a person believes they have been misidentified or considers the designation does not meet the required evidentiary threshold.[68]

67 SAMLA, at Section 23(1).

68 Explanatory Notes to SAMLA, at Paragraph 89.

The evidentiary threshold for designation by name and by description using the standard procedure is set out in Sections 11(2A) and 12(5) of SAMLA, respectively. These requirements are that the appropriate minister has 'reasonable grounds to suspect' that the person, organisation or the person falling within that description is an involved person[69] (see above for the meaning of this phrase).

The UK government's response to the public consultation on the future UK sanctions regime states that the 'reasonable grounds to suspect' test is the appropriate evidentiary threshold.[70] This threshold would only be met if there is sufficient information or evidence to enable the government to form a reasonable suspicion.[71] Section 23 of SAMLA allows designated persons access to quick redress, and is labelled as an administrative challenge.[72] In practice, the FCDO is understood to have taken over six months to decide on applications under Section 23 of SAMLA. It is clear from SAMLA that the decision on this kind of request must be made as soon as 'reasonably practicable',[73] and the person who makes the request must be informed of the decision and the reasons 'as soon as reasonably practicable after the decision was made'.[74]

However, this route is not available to persons subject to a UN designation. UN-designated persons must request that the appropriate minister 'use their best endeavours' to persuade the UN to remove them from the relevant UN instrument.[75]

---

69 See SAMLA, at Section 11(2A) for designation by name, and see Section 12(5)(a) for designation by description.

70 See HM Government response to public consultation on the UK's future legal framework for imposing and implementing sanctions, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/635101/consultation-uk-future-legal-framework-sanctions-government-response.pdf, at pp.. 9–12.

71 ibid.

72 Explanatory Notes to SAMLA, at Paragraph 89.

73 SAMLA, at Section 33(2)(a).

74 id., at Section 33(2)(b). The Sanctions Review Procedure (EU Exit) Regulations 2018, which came into force in January 2019, make provision for the procedure applicable to these requests.

75 id., at Section 25.

Once a request has been made, an appropriate minister must decide whether to comply with the request.[76] The same designated persons cannot submit another request upon assessment by the appropriate minister, unless that person can show that there is a significant matter of which the government was not aware.[77]

The appropriate minister who made a designation has the discretion to revoke or vary that designation.[78] Revoking a designation means that the designated person would no longer be subject to the restrictions set out in the relevant regulation.[79] Varying a designation allows the minister to add any changes to the designation, such as updating information used to identify an individual.[80]

However, a minister is obliged to revoke a designation when the required conditions of the relevant designation power are not met.[81] This may be as a result of the government's own review of designations, or if a designated persons seeks reassessment of their designation.

Designated persons seeking reassessment of their designation

SAMLA also provides designated persons a route to challenge government decisions in the High Court, or in Scotland, the Court of Session.[82]

When considering an application brought under Section 38 of SAMLA, the courts will apply the legal principles of judicial review.[83] If a designated person seeks a revocation or variation of their listing, they must apply for this through the administrative process listed in SAMLA before being able to access the redress through a legal challenge.

The following decisions can be challenged in the relevant courts:

- a decision by the appropriate minister on whether to vary or revoke a designation or to take no action with respect to it (following a request for revocation or variation);[84] or

76 For UK designations, see SAMLA, at Section 23 and Explanatory Notes to SAMLA, at Paragraph 90. For UN sanctions, see SAMLA, at Section 25 and Explanatory Notes to SAMLA, at Paragraph 93.
77 Explanatory Notes to SAMLA, at Paragraphs 91 and 93.
78 SAMLA, at Section 22(2).
79 Explanatory Notes to SAMLA, at Paragraph 87.
80 ibid.
81 SAMLA, at Section 22, Paragraphs (3) and (4).
82 id., at Section 38(2).
83 Explanatory Notes to SAMLA, at Paragraph 111.
84 SAMLA, at Section 38(1), Paragraphs (a) and (b).

- if the appropriate minister did not comply with the request to use best endeavours to persuade the UN to remove them from the relevant UN instrument.[85]

Under proceedings on an application under Section 38 of SAMLA, the courts may not award damages unless the court is satisfied that the decision concerned was made in bad faith.[86] In addition, any damages awarded are limited to a cap in regulations that are yet to be published.[87] This approach is comparable with the current law on awards of damages in sanctions cases within the EU.[88] This Section also confirms that legal challenges are to be dealt with under the provisions in Section 38.[89]

In March 2023, in *LLC Synesis v. Secretary of State for Foreign, Commonwealth and Development Affairs*,[90] the High Court issued a judgment in respect of the first designation challenge under Section 38 of SAMLA. In rejecting the designated person's challenge, the High Court confirmed that it 'cannot stand in the shoes of the [minister] when conducting this review exercise under section 38 of SAMLA. Instead, the Court's role is to examine whether the [minister's] decision was either based on no evidence or was irrational.' In light of the significant number of designations under the Russia Regulations, we expect to see more challenges under Section 38 of SAMLA in the future. However, it took the *Synesis* case over two years from the claimant's designation to reach the High Court in March 2023 and so it may take some time before these cases reach the High Court.

Periodic government review

The requirement for the government to conduct periodic reviews of sanctions was repealed by the Economic Crime (Transparency and Enforcement) Act in 2022.[91]

Licensing

Sanctions legislation typically provides for certain exceptions from the prohibitions and restrictions imposed by the legislation. These exceptions may take the form of exempt activities (i.e., conduct that is expressly permitted by the

85 id., at Section 38(1)(c) and Explanatory Notes to SAMLA, at Paragraph 110.
86 SAMLA, at Section 39(2) and Explanatory Notes to SAMLA, at Paragraph 113.
87 SAMLA, at Section 39(2A).
88 Explanatory Notes to SAMLA, at Paragraph 113.
89 SAMLA, at Section 39(1).
90 *LLC Synesis v. Secretary of State for Foreign, Commonwealth and Development Affairs* [2023] EWHC 541 (Admin).
91 Economic Crime (Transparency and Enforcement) Act, at Section 62.

sanctions legislation in question without the need for any licence or authorisation). Sanctions legislation may also provide for licences and authorisations to be granted to permit conduct that would otherwise be in breach of a prohibition.

OFSI and the ECJU are responsible for issuing licences in connection with UK financial sanctions and trade sanctions, respectively. Those subject to immigration sanctions can request to travel in exceptional circumstances using the visa application process.

The OFSI General Guidance confirms that specific licences issued while the UK was bound by EU sanctions 'will be treated as if they had been issued under the relevant [SAMLA] Regulations' and can be relied upon until they expire.[92]

The OFSI General Guidance contains a useful explanation of the approach taken by OFSI in relation to licensing grounds that are relevant to UK sanctions.[93] These include the following.

- Satisfying the basic needs of designated persons: OFSI considers the following: 'Expenditure to meet basic needs of an individual should be expenses which are necessary to ensure that designated persons or financially dependent family members are not imperilled.' For entities, this includes the payment of insurance premiums, reasonable fees for property management services, remuneration of employees, tax payments, rent or mortgage payments and utility charges. OFSI does not consider that this ground should be used to enable designated persons to continue the lifestyle or business activities they had before they were designated.
- Fees for the provision of legal services: OFSI states that these fees must be reasonable. In addition, OFSI considers that the Supreme Court Cost Guides, or the sums that could be expected to be recouped if costs were awarded in litigation, 'provide a useful starting point for assessing the reasonableness of legal fees and disbursements'. This is separate to the general licence under the Russia and Belarus sanctions regimes, which permits the payment of legal fees owed by designated individuals and entities (see further detail below).

92 OFSI General Guidance, at Section 6.16.

93 id., at Section 6.5. The regulations relevant to specific sanctions regimes include the licensing grounds relevant to the specific sanctions regime. For example, the Russia Regulations, at Schedule 5, include the relevant licensing grounds. However, the OFSI General Guidance refers to the definitions used in the Russia Regulations but also provides further information on OFSI's interpretation of the grounds; for example, the 'basic needs' grounds are expanded on in the OFSI General Guidance.

- Routine maintenance of frozen funds and economic resources: these are fees or service charges that must be reasonable and 'result in the routine holding or maintenance of frozen funds or economic resources'.
- Extraordinary expenses: OFSI states that these must be extraordinary in nature (unexpected or unavoidable and so not recurring or easily anticipated). This ground cannot be used where other grounds are more suitable or as a way of avoiding the clear limitations of those other grounds.
- Satisfaction of pre-existing judicial decisions: OFSI's position is that the judgment or decision must have been given before the date of designation and be enforceable in the UK, and cannot be for the benefit of a designated person.
- Satisfaction of prior contractual obligations of the designated person: again, OFSI contends that the contract or obligation must have arisen prior to the date of designation and cannot result in funds or economic resources being made available to the designated person.
- Humanitarian assistance activities: OFSI states that this ground 'enables payments to facilitate any humanitarian activity; or where applicable, any activity where its purposes are consistent with the objectives of UN Security Council Resolutions'. OFSI considers humanitarian assistance to include the work of non-governmental organisations carrying out relief activities for the benefit of civilians. Importantly, OFSI notes that a licence may still be required despite an activity using government funds.
- Diplomatic missions: OFSI sets out that a licence may be granted to ensure the 'proper functions of a diplomatic mission or consular post'. A pre-requisite for this licence is compliance with international law.
- Extraordinary situations: this licensing ground applies to non-UN-designated persons, and is intended to enable 'anything to be done to deal with an extraordinary situation'. The OFSI General Guidance makes it clear that this is intended to cover 'disaster relief or provide aid' and for situations that 'must be extraordinary in nature (unexpected, unavoidable and not recurring)'. This licensing ground cannot be used 'where other grounds are more suitable' or in an attempt to circumvent a limitation present in respect of another ground.

The OFSI General Guidance also notes a number of exceptions (i.e., areas where prohibitions do not apply), which include:

- crediting frozen accounts, which allows for a firm to:
    - credit a frozen account with interest, so long as the funds are frozen immediately;
    - transfer funds to credit a frozen account to discharge obligations that were concluded or arose prior to designation; or

    - credit a frozen account with third-party payments, so long as the incoming funds are frozen immediately and OFSI is informed;[94]
- transfers in the interest of independent persons: allowing an independent person to transfer an interest in frozen funds or resources to another person where:
    - the independent person is not a designated individual;
    - they do not hold the interest jointly with a designated individual;
    - they are not controlled by a designated individual; and
    - the independent person holds the interest in the funds or resources;[95] and
- ring-fencing funds: the OFSI General Guidance also confirms that UK autonomous sanctions will contain an exception to allow large financial institutions to transfer funds held or controlled by a designated individual to comply with the ring-fencing requirements imposed under the Financial Services (Banking Reform) Act 2013.[96]

The OFSI General Guidance also provides further details about legal advice, court fees and investments.[97]

- OFSI notes that generally there is no prohibition on providing legal advice when an asset freeze is in place, but 'the payment for legal services and the provision of legal services on credit do require an OFSI licence'. The OFSI General Guidance also notes that in certain circumstances, such as where sanctions prohibit specific actions, a lawyer should carefully consider whether the advice being provided is to help the client comply with the sanctions regime or to facilitate a breach.
- OFSI states that court fees and payments into courts for security for costs 'can be licensed under the reasonable legal fees licensing grounds'. Separate licensing grounds are required for the payment of security for damages into court and, in the event a court fee will be invoiced to a designated individual as a disbursement, this can be paid 'without a licence only if the payment is "not significant"'. Whether a court fee is 'significant' is a factual matter.[98]

---

94 id., at Section 6.1.

95 id., at Section 6.2.

96 id., at Section 6.3.

97 id., at Section 6.6.

98 *PJSC National Bank Trust & anor v. Mints & ors* [2023] EWHC 118 (Comm) confirms that a court can enter judgment in favour of a designated person. However, other activities involved in the conduct of litigation (for example, payment of an adverse costs order,

- OFSI confirms that generally frozen funds, and any profits from frozen funds, cannot be invested. The OFSI General Guidance states that exceptions or licensing grounds are unlikely to allow for this activity. However, the OFSI General Guidance does note that in certain circumstances 'some asset management may be permitted, under the "basic needs" licensing ground, to ensure that the existence of the business or the frozen assets is not imperilled'. This type of application will be considered by OFSI on a case-by-case basis.

In addition to the supplemental licensing grounds above, the OFSI General Guidance and recent OFSI activity illustrates a divergence of approach between the UK and EU as regards licensing in two further aspects.

First, autonomous UK sanctions, in contrast with EU sanctions, include a power to issue general licences, as opposed to specific licences (authorisations granted to an individual or entity that has applied in writing).[99] The OFSI General Guidance indicates that the UK government will make use of these licences in unforeseen circumstances to support policy priorities. As set out in the OFSI General Guidance, each general licence will include requirements for prior notification of use, record-keeping and reporting. Any party using a general licence must check the terms of that licence and comply with its conditions. Following the Russian invasion of Ukraine, OFSI dramatically increased the number of general licences issued. Between 1 January 2021 and 24 February 2022, OFSI issued two general licences. Between 23 February 2022 and 28 March 2023, OFSI issued around 50 licences to cover a range of issues.[100] A number of the licences provided a wind-down period for transactions with designated persons. For example, upon the designation of a number of banks, OFSI issued a licence that allowed for a 30-day wind-down period of transactions with the designated banks.[101] In addition, OFSI has issued general licences to deal with the position of UK subsidiaries owned by designated persons. For example, OFSI issued a licence allowing any subsidiary of VTB to make payment for: its basic needs or reasonable fees or service charges arising from routine holding and maintenance of its frozen funds and economic resources; or reasonable professional fees for

payment of security for costs and payment of a cross-undertaking in damages) require a licence. This judgment has been appealed but the appeal remains outstanding.

99 OFSI General Guidance, at Section 6.8.

100 www.gov.uk/government/collections/ofsi-general-licences.

101 General licence – INT/2022/1295476, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1058766/04.03.22_banks_asset_freeze_Publication_Notice_INT-2022-1295476.pdf.

the provision of legal services. The licence also allowed these entities to make, receive or process any payments, or take any other action, in connection with any insolvency proceedings.[102] Finally, in October 2022, as a result of the significant increase of new designations under the Russia Regulations, and the correlating increase in the number of those seeking a licence from OFSI for the payment of legal fees, OFSI issued a general licence to permit the payment of legal fees owed by individuals and entities designated under the Russia Regulations.[103]

Second, SAMLA introduced the concept of directions. A direction may be issued under SAMLA in respect of a statutory requirement and can provide an exception to a requirement.[104] These directions are only available for certain sanctions regimes and are applied for using a form available through OFSI's website.[105] Directions may be conditional and can be varied by OFSI at any time.

Licences relating to trade sanctions are dealt with through a separate process. It should be remembered that some transactions may require licences in respect of applicable financial sanctions as well as applicable trade sanctions. The Department for International Trade maintains a web page containing links to a substantial body of guidance relating to the licensing regime for trade sanctions. Export control licence applications are processed through an online system called SPIRE. See Chapter 8 of this Guide for further information about the UK export control regime.

---

102 General licence – INT/2022/1280876, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1070783/INT.2022.1280876publication_notice.pdf.

103 General licence – INT/2022/2252300, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1114563/General_Licence_INT20222252300.pdf. This licence also applies to designations under the Republic of Belarus (Sanctions) (EU Exit) Regulations 2019.

104 SAMLA, at Section 15(2)(c).

105 See OFSI General Guidance, at Section 6.18.

CHAPTER 4

UK Sanctions Enforcement

Rachel Barnes KC, Ben Summers, Patrick Hill and Ciju Puthuppally[1]

Introduction

Sanctions enforcement is now regarded as an essential element in the United Kingdom's broader economic crime regime.[2] The Office of Financial Sanctions Implementation (OFSI) in HM Treasury was established in 2016. At its outset it aimed to 'develop as a world leader in financial sanctions implementation and enforcement'[3] and signalled an intention robustly to enforce sanctions compliance and to impose significant financial penalties in appropriate cases.

---

1 Rachel Barnes KC, Ben Summers, Patrick Hill and Ciju Puthuppally are barristers at Three Raymond Buildings. The authors are extremely grateful to their colleagues and previous co-authors of this chapter, Saba Naqshbandi and Genevieve Woods, who are also barristers at Three Raymond Buildings.

2 HM Treasury (HMT) and HM Home Office 'Economic Crime Plan 2, 2023 to 2026', at www.gov.uk/government/publications/economic-crime-plan-2023-to-2026. This chapter focuses primarily on financial sanctions enforcement. In 2020, the role of the Director of the Office of Financial Sanctions Implementation (OFSI) was expanded to include economic crime policy at HMT. In his first blog, the new Director stated of his twin roles: 'This brings HMT's sanctions policy and operational implementation roles together . . . and integrates them into the government's broader economic crime agenda. . . . I hope to use my expanded role to build stronger links between sanctions and broader economic crime work, exploiting the large overlap in threats, issues and stakeholders.' OFSI, 'An Introduction from new OFSI director Giles Thomson', 4 February 2021, at https://ofsi.blog.gov.uk/2021/02/04/an-introduction-from-new-ofsi-director-giles-thomson/.

3 OFSI, Annual Review April 2018 to March 2019 (October 2019) p. 1, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/838178/Annual_Review_2018-19_FINAL.pdf.

At the time of the publication of OFSI's Annual Review April 2021 to August 2022, reporting on the UK government's response to the Russian invasion of Ukraine, the Director of OFSI commented that the:

> *unprecedented size, scale and complexity of these new sanctions highlight the central role sanctions play in UK foreign, security and economic policy . . . Sanctions continue to be integral to the UK's ability to respond to geo-political issues and, now more than ever, the work of OFSI sits at the forefront of the UK's national security, prosperity and foreign policy goals.*[4]

In 2017, the maximum term of imprisonment for financial sanctions breaches was increased from two years to seven years.[5] Under the Sanctions and Anti-Money Laundering Act 2018 (SAMLA), it is further increased to 10 years, bringing it in line with the maximum sentence for trade sanctions and export control breaches.[6] Following the expansion of the UK's autonomous sanctions regime in response to Russia's invasion of Ukraine in February 2022, it is anticipated that there will be further expansion in its scope together with some increase in the number and severity of enforcement actions.

---

4 OFSI, Annual Review April 2021 to August 2022 (November 2022), p. 1, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1116689/OFSI_Annual_Review_2021-22_10.11.22.pdf.

5 Policing and Crime Act 2017, Section 144(3)(a), giving government the power to provide for a maximum term of imprisonment in the case of conviction on indictment of seven years in sanctions regulations made under the European Communities Act 1972. The maximum term of imprisonment provided in regulations made under that Act had been two years; see European Communities Act 1972, Schedule 2, Paragraph 1(1)(d) (unamended).

6 Sanctions and Anti-Money Laundering Act (SAMLA), Section 17(5)(a). In the Public Bill Committee for the Sanctions and Anti-Money Laundering Bill, the responsible Minister (John Glenn, Economic Secretary to the Treasury) stated that the government's intention was to maintain the practice that sanctions regulations did not provide for maximum sentences greater than seven years' imprisonment for offences other than breaches of trade sanctions (Hansard, 27 February 2018, column 22). To date, that remains the practice.

Offences established under sanctions legislation

Regulations for each sanctions regime prohibit certain conduct (see Chapter 4), creating offences that arise when the prohibited activity is conducted with the requisite mental element (principal offences). In each sanctions regime there is also a set of related offences that can be committed in connection with (1) licences applied for or issued to permit otherwise prohibited conduct, and (2) requirements to report or requests to provide information or documents to OFSI.

Principal offences

Examples of principal offences include when a person deals with the funds of a designated person without a licence, knowing or having reasonable cause to suspect that the relevant transaction is prohibited.[7] A person may be guilty of a circumvention offence when they intentionally participate in activities, knowing that the object or effect is (directly or indirectly) to circumvent any sanctions prohibition or to enable or facilitate the contravention of any prohibition.[8]

Related offences

- Licensing offences: (1) failing to comply with any condition of a licence; and (2) knowingly or recklessly providing false information or documentation for the purpose of obtaining a licence.

---

7 Exceptions and defences are set out in the regulations for each regime. See, e.g., Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019, Regulation 81. Note that the amendment to the power of HMT to impose a civil monetary penalty under Section 146 of the Policing and Crime Act 2017, brought into effect on 15 June 2022 by Section 54 of the Economic Crime (Transparency and Enforcement) Act 2022, which has removed a required mental element in any breach or failure to comply with an obligation imposed by or under financial sanctions legislation, does not apply to the criminal offences set out in each of the sanctions regimes. In other words, HMT can impose civil penalties for sanctions breaches on a strict liability basis whereas the mental element (mens rea) of the offence for which criminal liability may arise remains.

8 For a discussion of the limitations of circumventing offences, see *R v. R* [2015] EWCA Civ 796 (decided under the pre-SAMLA legislation). There has recently been some debate about whether the transfer of assets by a person in anticipation of being designated for the purposes of financial (asset freezing etc) sanctions, who is later so designated, could constitute the offence of conspiracy to circumvent sanctions contrary to, for example, Regulation 19 of the Russia (Sanctions) (EU Exit) Regulations 2019. This issue has not been judicially determined.

- Reporting offences: failing to inform HM Treasury as soon as practicable if a relevant firm knows or has reasonable cause to suspect that a person is a designated person or has breached financial sanctions regulations and the information on which the knowledge or suspicion is based came to them in the course of carrying on their business.
- Information offences: (1) failing to comply with a request by OFSI for information or the production of documents without a reasonable excuse; (2) knowingly or recklessly providing materially false information or documentation in response to a request for information;[9] (3) destroying, mutilating, defacing, concealing or removing any document with intent to evade requirements under a request for information or documents; or (4) otherwise intentionally obstructing HM Treasury in respect of its powers to make the request.[10]
- Confidentiality offences: a person who is provided with specified confidential information or who obtains it commits an offence by disclosing it without lawful authority if that person knows or has reasonable cause to suspect that the information is to be treated as confidential.[11]

---

9 As described below, both the Crown Prosecution Service (CPS) and the Serious Fraud Office (SFO) also have powers to compel the provision of information and documents that may be applicable in investigations of suspected offences under sanctions legislation (see section titled 'Investigative powers' below). Along with those powers, the relevant legislation also establishes secondary offences of failing to comply with disclosure or production notices issued by the CPS or SFO and knowingly or recklessly providing materially false or misleading information or documents in response to these notices – see Serious Organised Crime and Police Act 2005 (SOCPA), Section 67; Criminal Justice Act (CJA) 1987, Section 2(13), (14).

10 This conduct would amount to a common law offence of perverting the course of justice in the context of an anticipated criminal investigation or when one is known to have commenced. *Vreones* [1891] 1 QB 360; *Government of the USA v. Dempsey* [2018] 4 WLR 110. For the comparable offence in respect of SFO investigations, see CJA 1987, Section 2(16).

11 See, e.g., Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019, Regulation 9.

The reporting offences can only be committed by the classes of persons specified in the legislation. The definition of 'relevant firms' subject to specific reporting obligations is broad and includes currency exchange or funds transmission businesses, auditors, accountants, trust service providers, cryptoasset exchange providers, casinos and estate agents.[12]

The reporting offences can only be committed if relevant firms fail to disclose information they are obliged to report.[13] For example, if the suspicion of a sanctions breach arose solely from information obtained other than in the course of business, such as through media reporting, then neither the reporting requirement nor the offence would arise. The reporting requirement does not require the disclosure of information that is subject to legal professional privilege (LPP), or information that would be prohibited under data protection legislation or the Investigatory Powers Act 2016.[14] Regulations also provide for exceptions from liability for conduct that would otherwise constitute an offence for breach of the financial restrictions, confidentiality, information or reporting provisions, where a Crown officer acting as such has determined that the conduct would be in the interests of national security or the prevention or detection of serious crime in the UK or elsewhere.[15]

12 A 'relevant firm' is defined in each set of sanctions regulations (see, e.g., Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019, Regulation 100; Russia (Sanctions) (EU Exit) Regulations 2019, Regulation 71).

13 OFSI's General Guidance on Financial Sanctions, August 2022 (Financial Sanctions Guidance) contains a list of examples of the kinds of information that must be reported to OFSI: see pp. 25–26. The precise requirements are set out in each set of financial sanctions regulations.

14 For further discussion of legal professional privilege (LPP), see 'Duties of counsel and privilege' below. See also, e.g., Democratic People's Republic of Korea (EU Exit) Regulations 2019, Regulation 109.

15 SAMLA, Section 15(2)(a), (6); see, e.g., Global Anti-Corruption Sanctions Regulations 2021/488, Regulation 20; Global Human Rights Sanctions Regulations 2020/680, Regulation 19.

Liability for secondary parties, inchoate offences, corporates and company officers

The ordinary criminal law principles of accessorial liability, inchoate offences and corporate liability (the identification principle)[16] apply.

Under the law of England and Wales, secondary parties that 'aid or abet' or intentionally and wilfully encourage others to commit offences (including the commission of the offences summarised above) are guilty of the offences they aid, abet or encourage, as well as the principal offender. Additionally, Part 2 of the Serious Crime Act 2007 creates a number of offences of encouraging or assisting crime: intentionally encouraging or assisting an offence (Section 44), encouraging or assisting an offence believing it will be committed (Section 45), and encouraging or assisting offences believing one or more will be committed (Section 46). Each offence is subject to a defence that the accused person knew (or reasonably believed) that 'certain circumstances existed' and it was reasonable for them to act as they did in those circumstances. The resulting position is that the carrying out of acts that intentionally assist or encourage another person to commit a sanctions offence will result in liability for the same offence or a separate offence (or both) under the Serious Crime Act 2007.

When an offence is committed with the consent or connivance of, or is attributable to the neglect of, any director, manager, secretary or other similar officer of the corporation or a person acting in that capacity, that person is guilty of the offence in addition to the corporation and is liable to prosecution.[17]

16 Also known as the attribution theory of corporate liability. The primary rules of identification may be subject to a more purposive interpretation in respect of regulatory offences, such as sanctions offences, in which the conduct and *mens rea* of a corporate officer other than the directing will and mind of the company as a whole may be attributed to the company to establish liability; see *Meridian Global Funds Management Asia Ltd v. Securities Commission* [1995] 2 AC 500 (PC); *Bilta (UK) Ltd (In Liquidation) v. Nazir* [2016] AC 1; *Serious Fraud Office v. Barclays plc* [2020] 1 Cr App R 28.

17 See, e.g., Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019, Regulation 111. Similarly, where HMT determines a monetary penalty is payable by a legal entity under Section 146 of the Policing and Crime Act 2017, it may also impose a monetary penalty on an officer of that body if satisfied, on the balance of probabilities, that the breach or failure in respect of which the monetary penalty is payable by the body took place with the consent or connivance of the officer or is attributable to her neglect, pursuant to Section 148 of the 2017 Act.

Jurisdiction

Jurisdiction is established on the basis of both territory and nationality (active personality). The sanctions regulations impose prohibitions and requirements and establish related offences in relation to conduct in the United Kingdom or its territorial sea by any person and conduct elsewhere by a 'United Kingdom person',[18] defined as a 'United Kingdom national' (which includes British citizens, British subjects and British protected persons)[19] or body incorporated or constituted under the law of any part of the United Kingdom.[20] A conspiracy to commit a sanctions offence between a person in England or Wales and a person or persons outside the jurisdiction, is capable of prosecution provided the agreement would necessarily involve some 'substantial measure' of the activities constituting the crime taking place within the jurisdiction.[21] Similarly, a conspiracy formed outside the jurisdiction to commit a crime within the jurisdiction is capable of prosecution even though no act in furtherance of the agreement is committed in England and Wales.[22] A company may be convicted of an offence of conspiracy.[23]

Investigations into sanctions offences

Commencement

Investigations may commence following, inter alia: voluntary self-disclosure by a natural or legal person; a report to OFSI or a UK law enforcement agency by a third party such as a whistle-blower; disclosure by a person's professional regulator; the filing of a suspicious activity report (SAR) to the National Crime Agency (NCA) under money laundering or counterterrorism laws; a UK law enforcement agency receiving information from an overseas counterpart or international organisation that violations have or are suspected to have occurred; or a financial sanctions breach report made in compliance with the reporting obligation discussed above.

---

18 SAMLA, Section 21.

19 id., Section 21(3).

20 id., Section 21(2). Jurisdiction may be specifically extended to include bodies incorporated or constituted under the laws of any of the Channel Islands, the Isle of Man or any of the British overseas territories (id., Section 21(4)).

21 *Hammersley* (1958) 42 Cr. App. R. 207 and *Smith (Wallace Duncan) (No. 4)* [2004] EWCA Crim 631.

22 *Somchai Liangsiripraset v. Government of the United States of America* [1991] 1 A.C. 225 (PC).

23 *ICR Haulage Co. Ltd* [1944] KB 551.

Notification

There is no general requirement to notify a suspect of an investigation. In a criminal investigation conducted by criminal law enforcement authorities, a suspect may not be made aware of the investigation until some overt action is taken, such as:

- arrests of individuals or requests to attend interviews either under compulsion[24] or as volunteers;
- service of production orders or information provision notices;
- execution of search warrants;
- if a third party that holds or controls the assets, such as a bank or a trustee, freezes the assets unilaterally by refusing to execute their directions; or
- service of a subsequent court order, such as a restraint order issued in the Crown Court or a bank account freezing order by a magistrates' court.

In an OFSI investigation, if a person has self-reported or disclosed a suspected sanctions breach to OFSI (or some other enforcement authority), the investigation will typically come to the attention of the person following the authority's response to that disclosure confirming that an investigation has commenced.

Only when OFSI has formed an intention to impose a civil monetary penalty upon a person is it required to inform the person of its intention to do so and provide the person with the opportunity to make representations.[25] In practice, however, OFSI investigations will come to the attention of suspects and witnesses at a much earlier stage, as a result of OFSI requesting information or material.

Enforcement authorities

Although OFSI is the primary organisation responsible for financial sanctions implementation, other relevant agencies include the NCA, the Crown Prosecution Service (CPS), the Serious Fraud Office (SFO), His Majesty's Revenue and Customs (HMRC),[26] the Export Control Joint Unit (ECJU) of the Department for International Trade,[27] and also professional regulators and overseas enforcement agencies.[28]

---

24 For example, the exercise by the Serious Fraud Office of its powers under section 2 of the Criminal Justice Act 1987.

25 This procedure is described below in the section titled 'Civil monetary penalties'.

26 His Majesty's Revenue and Customs (HMRC) is primarily responsible for the investigation and enforcement of trade sanctions.

27 See Chapter 9. Like OFSI, the Export Control Joint Unit of the Department for International Trade does not exercise criminal investigation powers.

28 See section titled 'Self-reporting to others', below.

OFSI works closely with the NCA, whose sanctions investigations are conducted by its Combatting Kleptocracy Cell.[29] Typically, the NCA, like HMRC, refers cases for prosecution to the CPS.[30] The SFO may investigate and prosecute cases in which sanctions offences – typically those intersecting with international bribery or serious or complex fraud – satisfy their take-on criteria.[31]

In 2009, the SFO prosecuted Mabey & Johnson Ltd and three executives for breaches of UN Iraq sanctions that were linked to the payment of bribes in exchange for oil contracts.

Investigative powers

In a financial sanctions investigation, OFSI may use its powers to require persons to provide information to detect evasion and to investigate offences. Requests will be made in writing and will specify the period within which the information must be provided.[32] Many NCA officers have the operational powers of police constables and immigration and customs officers, for example, to gain entry to property, conduct searches, seize goods or detain and arrest suspects with or without a warrant.[33]

Criminal prosecutors have powers to require the provision of information. The Director of Public Prosecutions in England and Wales, the Lord Advocate in Scotland and the Director of Public Prosecutions for Northern Ireland (collectively, the Prosecutors) may authorise a specified officer to issue disclosure notices

29 See https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/bribery-corruption-and-sanctions-evasion.

30 The CPS Specialist Fraud Division has experience in prosecuting trade sanctions and export control cases following HMRC investigations.

31 The power of the Director of the SFO to accept cases for investigation and prosecution is limited to those of serious or complex fraud, or bribery and corruption (CJA 1987, Sections 1(3) and 2A(5)). See also 'SFO case acceptance: Statement of Principle' at www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-statement-of-principle/ and footnotes 130, 171 and 179, below, for details of the *Mabey & Johnson* case.

32 OFSI Financial Sanctions Guidance, § 5.6. If no period is specified, compliance must take place 'within a reasonable time'. (See, e.g., Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019, Regulation 104(1)(a).) As set out above (in the section titled 'Related offences'), failure to comply with a request for information without a reasonable excuse is a criminal offence, as is providing false information, destroying documentation or otherwise intentionally obstructing OFSI.

33 Crime and Courts Act 2013, Section 10, Schedule 5.

in investigations into offences established in sanctions regulations promulgated under SAMLA.[34] These may require the addressee to answer questions, provide information or produce documents relevant to the investigation.[35] The Director of the SFO can issue 'Section 2 notices', requiring persons under investigation and any other person that the Director has reason to believe has relevant information to answer questions or provide documents 'in any case in which it appears to [the Director] that there is a good reason to do so for the purpose of investigating'.[36] In both cases, the Prosecutors or the Director of the SFO may apply to a court for a warrant to enter and search premises to seize documents in cases where, for example, giving notice for the production of documents might seriously prejudice the investigation.[37]

Civil or criminal investigations

In many financial sanctions cases, OFSI will investigate using its own powers first. A decision will then be taken on whether OFSI will use its civil enforcement powers (whether by monetary penalty or some other action) or will refer the case, usually to the CPS, for criminal prosecution.[38] Because OFSI does not have the power to instigate criminal proceedings of its own accord, if it does refer a case for criminal prosecution, it is a matter for the prosecuting authority to determine whether the case should proceed in accordance with its policy.[39] Where the prosecuting authority decides not to proceed to prosecution, the case may revert to OFSI.

---

34 SAMLA, Section 17(8), amending SOCPA, Section 61. The Prosecutors' powers are contained within SOCPA, Section 60. The specified officers are a constable, a designated National Crime Agency (NCA) officer or an HMRC officer.

35 SOCPA, Section 62(3). They may only be issued when, among other things, the relevant prosecutor has reasonable grounds for (1) suspecting a specified offence has been committed, (2) suspecting that the target has information that relates to a matter relevant to the investigation of that suspected offence, and (3) believing that the information sought is likely to be of substantial value to that investigation.

36 CJA 1987, Section 2. The jurisdictional limits of the Director's powers to issue Section 2 notices were considered by the Supreme Court in *R (oao KBR Inc) v. Director of the Serious Fraud Office* [2021] UKSC 2.

37 SOCPA, Section 66(2); CJA 1987, Section 2(4).

38 The distinction between a civil and criminal investigation may only be relevant when the enforcement authority forms an early view that criminal proceedings against any person are unlikely.

39 Note that: 'OFSI will work closely with law enforcement agencies to ensure that breaches of financial sanctions are dealt with in the most appropriate way. We will seek to reach agreement with them where possible, but recognise that sometimes an independent

Investigations into trade sanctions breaches are conducted by the HMRC. The ECJU conducts compliance audits of exporters of controlled goods and technology and will report to HMRC any irregularities it identifies in the course of an inspection that indicate a breach of trade sanctions or export controls.[40] HMRC may deal with breaches by way of civil monetary penalties (known as compound penalties) or referring cases to the CPS for prosecution.

Best practice for corporates in an investigation

Once a company becomes aware of a suspected sanctions breach, it should quickly decide on its response strategy. Enforcement authorities place considerable emphasis on timely voluntary disclosure, the extent of a company's cooperation during an investigation and the remedial actions it puts in place to prevent future sanctions violations when deciding the nature and scope of any enforcement action.[41] Companies may also be subject to industry regulatory regimes and shareholder or other disclosure requirements. Companies with operations overseas will need to consider whether regulators in those jurisdictions would expect to be informed.

Actions and issues to be considered after the discovery of suspected breaches or during a sanctions investigation include:

- notifying the board of directors;
- the board of directors' role going forward and protocol for board communications;
- the role of in-house lawyers and the compliance function;
- appointing external counsel (and other consultants and experts);
- preserving all relevant material (e.g., documents, emails, telephone recordings) concerning both the suspected breaches and the response to their discovery;
- an internal investigation into the suspected breaches;
- reviewing other business and transactions for additional breaches;
- identifying remedial compliance measures;

---

prosecutor may choose not to take forward a prosecution. The 2017 Act also provides additional options for prosecutors when dealing with financial sanctions breaches.' OFSI Consultation Response on the Process for Imposing Monetary Penalties for Breaches of Financial Sanctions, April 2017, § 1.13.

40 Export Control Joint Unit Guidance: Export controls, at www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources.

41 OFSI Financial Sanctions Guidance (March 2023) at § 7.1; Director of Public Prosecutions and SFO Joint Guidance on Corporate Prosecutions at p. 8.

- early engagement with relevant law enforcement authorities;[42]
- disclosure to other parties (e.g., regulators, shareholders, lenders, insurers, auditors, overseas authorities);
- public relations strategy;
- accounting provision for any anticipated financial penalties and associated costs; and
- disciplinary action against specific employees.

Self-reporting

Overview

In its first financial year (2017–2018), OFSI received 122 reports of suspected breaches of financial sanctions with a reported value of around £1.35 billion.[43] In its second financial year (2018–2019), OFSI received 99 reports of suspected breaches with a reported value of £262 million.[44] In its third financial year (2019–2020), OFSI received 140 reports of suspected breaches with an estimated value of £982.34 million.[45] In its fourth financial year (2020–2021), OFSI received 132 reports of potential financial sanctions breaches.[46] In its latest reporting period (April 2021 to August 2022), OFSI considered 147 reports, noting that 'the number of cases considered remains on an upwards trajectory. Since the invasion of Ukraine in February 2022 the number of breaches reported to OFSI has significantly increased.'[47]

---

42 For example, the Deferred Prosecution Agreements Code of Conduct identifies as a factor that a prosecutor may take into account when deciding whether to enter into a deferred prosecution agreement (DPA), the extent to which the company involves the prosecutor in the early stages of an internal investigation thereby giving the prosecutor the opportunity to give direction as to its scope and the manner in which it is conducted. CPS/SFO Deferred Prosecution Agreements Code of Practice (11 February 2014) (the DPA Code), § 2.9.2.

43 See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746207/OFSI_Annual_Review_2017-18.pdf.

44 See https://ofsi.blog.gov.uk/2019/10/15/ofsi-releases-2018-to-2019-annual-review/.

45 See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/925548/OFSI_Annual_Review_2019_to_2020.pdf.

46 See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025562/OFSI_Annual_Review_2021.pdf.

47 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1116689/OFSI_Annual_Review_2021-22_10.11.22.pdf.

The ability of sanctions authorities to perform their monitoring and enforcement roles depends, in large part, on the provision of information about potential sanctions violations by those within the private sector. Therefore, the UK sanctions framework both imposes reporting requirements on certain persons and rewards voluntary disclosure of suspected sanctions breaches.

Self-reporting should be considered by all putative defendants. It is a significant mitigating factor when enforcement authorities decide what action, if any, to take in relation to a sanctions breach and the extent of any penalties.[48] OFSI expects a breach to be disclosed as soon as 'reasonably practicable' after its discovery,[49] and for it to be reported on the designated form.[50] To qualify as 'self-reporting', individuals or entities cannot rely on self-reporting by another party involved in the suspected breach. If multiple parties are involved, OFSI expects voluntary disclosure from each.[51]

OFSI requires disclosures to include 'all evidence relating to all the facts of the breach'.[52]

Considerations before self-reporting[53]

Whether to self-report

If a person has a legal duty to report to OFSI, failure to self-report is a criminal offence. OFSI, the CPS and the SFO identify in their respective guidance the potential weight they will attach to a genuine self-report as a mitigating factor in all their case disposal decisions.[54]

---

48 OFSI enforcement and monetary penalties for breaches of financial sanctions: guidance (June 2022) (OFSI Monetary Penalties Guidance), § 3.39: 'OFSI values voluntary disclosure. Voluntary disclosure of a breach of financial sanctions by a person who has committed a breach may be a mitigating factor when we assess the case. It may also have an impact on any subsequent decision to apply a penalty.' For further discussion, see section titled 'Civil monetary penalties', below.

49 id., at § 3.43.

50 id., at § 3.42; the designated form is available at www.gov.uk/guidance/suspected-breach-of-financial-sanctions-what-to-do.

51 id., at § 3.40.

52 id., at § 3.44.

53 In addition to the actions and issues listed above, in section titled 'Best practice for corporates in an investigation'.

54 The privilege against self-incrimination would be expected to operate, however, in the event of a prosecution of any person for failing to report their own offence.

When to self-report

OFSI expects suspected sanctions breaches to be reported reasonably promptly.[55] It recognises that it may be reasonable for a person to take 'some time' to assess the nature and extent of the breach or to seek legal advice but emphasises that this should not delay an effective response.[56] In the *Standard Chartered Bank* case, OFSI accepted that it was reasonable for the company to initially report the existence of a potential breach and then to provide further information in stages during its internal investigation.[57] This position is reflected in the March 2023 edition of the OFSI Monetary Penalties Guidance.[58]

Delaying a self-report risks the law enforcement authority (1) receiving prior notification of the breach from a third party, or (2) concluding that the delay has been unreasonably lengthy, with the result that it will not be a factor weighing against prosecution, in favour of entering into a deferred prosecution agreement (DPA) or justifying a civil penalty discount. If a breach was only discovered as a result of a separate regulatory or law enforcement investigation, the enforcement authority could, potentially, be persuaded that the reporting party should retain the mitigation benefit of voluntary disclosure if it can demonstrate that it quickly instigated a wide-ranging and thorough review of sanctions compliance, cooperated with any external investigation and implemented meaningful remedial actions.[59]

---

55 OFSI Monetary Penalties Guidance, § 3.43: disclosure should occur 'as soon as reasonably practicable after discovery of the breach' and 'what this means will differ in each case'. See also CPS/SFO Corporate Prosecutions: 'Failure to report wrongdoing within reasonable time of the offending coming to light' is an additional public interest factor in favour of prosecution, and self-reporting is an additional public interest factor against prosecution; and DPA Code, §§ 2.8.1(v), 2.9.2 and 2.9.3.

56 OFSI Monetary Penalties Guidance, § 3.43.

57 If there is good reason for delaying the reporting of a breach or for providing partial disclosure, OFSI is able to receive and consider representations (OFSI Monetary Penalties Guidance, § 3.47). For a description of the *Standard Chartered Bank* case, see footnote 166.

58 id., at 3.43.

59 See, e.g., although it was not a sanctions case, *SFO v. Rolls-Royce Plc, Rolls-Royce Energy Systems Inc* [2017] 1 WLUK 189, [19]–[22]; see also www.sfo.gov.uk/cases/rolls-royce-plc/.

How to self-report

OFSI, ECJU/HMRC[60] and the SFO provide information about how to make a report on their respective websites. In both cases, there is a form to be completed and electronically submitted. In practice, an accompanying letter may set out greater detail than is contained within the standard form. The consequences of making an inaccurate disclosure or a disclosure that omits important information can be severe.[61]

Self-reporting to others

Companies should consider whether disclosure should also be made to other domestic regulators or to sanctions authorities in other jurisdictions. This latter point is particularly important if an entity operates in multiple jurisdictions or the breaches took place outside the United Kingdom, because enforcement action in the UK may trigger corresponding investigations overseas and vice versa.[62]

Where the suspected conduct would be in breach only of a non-UK sanctions regime, companies and relevant individuals should still consider whether there are relevant UK regulators to whom a report should be made.[63] These violations can

60 See www.gov.uk/government/organisations/export-control-joint-unit.

61 'OFSI takes very seriously any evidence that a disclosure did not include relevant information, unless this was a mistake or new facts emerge.' (OFSI Monetary Penalties Guidance, § 3.34).

62 Pre-SAMLA, UK sanctions regulations typically included provisions empowering HMT to disclose any information obtained under sanctions regulations to any person for the purpose of facilitating or ensuring compliance with corresponding EU sanctions regulations. This power is extended under SAMLA-promulgated regulations to allow disclosure of information to, among other parties, the government of any country. See, e.g., Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019/411, Regulation 108(3)(i). In his introductory remarks following his appointment as Director of OFSI in February 2021, Giles Thomson expressed an intention for OFSI to work with partners in other jurisdictions: 'The UK will continue to work on sanctions with key partners such as the US and the EU, but also with a wider range of partners . . . Sanctions are generally most effective when implemented multilaterally by as many countries as possible.' See footnote 2, above.

63 Although it is outside the scope of this chapter, it is important to note that overseas investigations and prosecutions may give rise to mutual legal assistance and extradition proceedings in the UK. For example, the US has successfully requested the extradition of individuals wanted for prosecution under US sanctions laws, see *Diri v. Government of the United States of America* [2015] EWCA 2130 (Admin); *Tappin v. Government of the United States of America* [2012] EWHC 22 (Admin).

be indicative of wider institutional control failures even though there has been no breach of applicable UK sanctions. UK anti-money laundering supervisors would expect to be informed of these situations by those they regulate.[64]

Those regulated persons are obliged to make a SAR to the NCA under the UK's anti-money laundering (AML) legislation if they have reasonable grounds to suspect assets are the proceeds of crime. This obligation may be engaged when they suspect sanctions breaches have occurred.[65] Breaches of financial sanctions may also amount to or be linked to other criminal offending, such as the funding of terrorism or bribery and corruption. In these cases, individuals and corporations may have obligations to report information to the police under Section 19 of the Terrorism Act 2000, or reporting obligations under the Counter-Terrorism (Sanctions) (EU Exit) Regulations 2019 or the Anti-Terrorism, Crime and Security Act 2001.[66] In cases of international bribery and corruption, companies may consider it is in their best interests also to self-report to the SFO.

Other notification requirements

Companies may have contractual obligations to notify counterparties of their involvement in sanctions offences, or in suspected criminal conduct or criminal investigations more generally. These types of clauses are often included in insurance policies, loan and other facility agreements, bank covenants and contracts for international trade. When a company is considering notifying third parties, whether voluntarily or as a requirement, it should also consider informing OFSI and any other relevant law enforcement or regulatory agency of its intention to do so. This is to avoid an allegation of breaching the confidentiality of, or even unlawfully prejudicing, a sanctions investigation.

---

64 See section titled 'Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017', below.

65 See section titled 'Suspicious activity reports', below.

66 Under Regulation 21 of the Regulations, a relevant firm (as defined in Regulation 22) must inform the Treasury as soon as practicable if it knows or has reasonable cause to suspect that a person is a designated person or has committed an offence under Part 3 or Regulation 20 of the Regulations based on information that came to them in the course of their business. Failure to comply is a criminal offence. Prior to 31 December 2019, the relevant reporting obligations were contained in the Terrorist Asset Freezing Act 2010. Section 19 of the 2010 Act applied when a person believes or suspects that someone has committed an offence under the Act (such as money laundering, the possession or use of funds for terrorism or fundraising for the purposes of terrorism) based on information they obtain in the course of their employment, trade, profession or business. When Section 19 applied, the person was required to disclose the information to a constable as soon as is reasonably practicable.

Anti-money laundering

Introduction

In a suspected sanctions breach,[67] two AML questions arise: (1) has a money laundering offence also been committed? and (2) is the suspected sanctions breach evidence of failings in mandatory AML compliance standards? As noted above, shortly after taking up his post in 2021, the new Director of OFSI emphasised the 'large overlap in threats, issues and stakeholders' in financial sanctions and broader economic crime,[68] and it is anticipated that this understanding will inform both sanctions enforcement policy and OFSI's approach to compliance standards.

The UK's AML legislative regime:[69]

- creates three principal money laundering offences, criminalising:
  - 'concealing, disguising, converting, transferring or removing criminal property from the jurisdiction';[70]
  - 'entering into or becoming concerned in an arrangement known or suspected to facilitate by whatever means the acquisition, retention, use or control of criminal property by or on behalf of another person';[71] and
  - 'acquiring, using or possessing criminal property';[72]

67 A sanctions breach may also lead to criminal confiscation or civil recovery proceedings in respect of assets obtained through the predicate conduct or any subsequent money laundering offence. See section titled 'Asset recovery', below.

68 See footnote 2.

69 The principal money laundering legislation is the Proceeds of Crime Act 2002 (POCA) and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI 2017/692) (MLR), as amended.

70 POCA, Section 327. Criminal property is defined, widely, in POCA, Section 340 as property that constitutes or represents a person's benefit from criminal conduct when the alleged offender knows or suspects that it constitutes a benefit. 'Property' includes all forms of property wherever situated and in whatever form, including money, real or personal property, things in action, and other tangible or incorporeal property. An individual will have 'obtained' property if they acquire an interest in it, including an equitable interest or power in relation to land in England and Wales, or a right (including a right to possession) in relation to property other than land.

71 POCA, Section 328.

72 id., Section 329. A conviction for any of the principal offences in POCA Sections 327, 328 and 329 carries the following maximum penalties: on summary conviction, six months' imprisonment or a fine (or both) and, on indictment, 14 years' imprisonment or a fine (or both).

- creates 'supplementary'[73] money laundering offences for failing to disclose suspicious transactions,[74] prejudicing an investigation[75] and tipping off;[76] and
- obliges specified private sector entities (e.g., banks and other financial institutions) to establish and maintain appropriate AML policies and procedures.[77]

Money laundering offences

There are three questions that will determine whether a money laundering offence has been committed in connection with a known or suspected sanctions breach:

- What predicate sanctions offence has been committed?
- Has 'criminal property' been generated as a result of, or in connection with, the sanctions offence?
- Has there been any prohibited dealing with the 'criminal property', such that an offence under Sections 327 to 329 of the Proceeds of Crime Act 2002 (POCA) would be found to have been committed if the relevant *mens rea* is established?[78]

Fees received as payment for the unauthorised provision of goods or services to a designated person or otherwise in circumstances that constitute a sanctions offence will be criminal property.[79] The subsequent use, transfer to a third party, or disposal of those fees with the requisite mens rea would constitute a money laundering offence under the appropriate provision of Sections 327 to 329 of POCA.[80]

---

73 As described in *R v. GH* [2015] 2 Cr App R 12 (SC) at [14].

74 POCA, Sections 330 and 331. The sentences on summary conviction are six months' imprisonment or a fine (or both), and on indictment, five years' imprisonment or a fine (or both).

75 id., Section 332.

76 id., Section 333A–333E.

77 MLR, Regulation 19.

78 Those three questions must be addressed separately because the conduct that amounts to a predicate sanctions offence cannot at the same time amount to an offence under POCA Sections 327–329; *R v. GH* [2015] 2 Cr App R 12 (SC) at [20], per Lord Toulson: '[I]t is a prerequisite of the offences created by sections 327, 328 and 329 that the property alleged to be criminal property should have that quality or status at the time of the alleged [money laundering] offence . . . Criminal property . . . means property obtained as a result of or in connection with criminal activity separate from that which is the subject of the [money laundering] charge itself.'

79 *R v. McDowell* [2015] 2 Cr App R (S) 14 (CA). Separately, having been obtained through criminal conduct, those fees will be liable to confiscation or civil recovery under POCA.

80 In *R (Golfrate Property Management Ltd) v. Southwark Crown Court* [2014] 2 Cr App R 12 at [104] and [105], the Court of Appeal analysed two factual situations in which a designated person outside the UK transfers funds to a person in the UK. In the first, although the

Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017[81]

UK sanctions law does not, directly, require the establishment of sanctions policies and procedures.[82] Nevertheless, a sanctions breach may demonstrate a failure

---

transfer may not, without more, constitute a breach of the asset freezing provisions of the relevant sanctions regime, if the designated person retained a property interest in the funds after the transfer, any subsequent unauthorised movement of the funds may constitute a sanctions offence. In this first situation, any further use, transfer, etc. of the funds could amount to a money laundering offence. In the second situation, the funds are transferred to a person in the UK with the intent of circumventing the relevant sanctions regulations and a sanctions offence would have been committed at that stage. In this second situation, any subsequent possession, use, transfer, etc. of the funds with the requisite *mens rea* would constitute a money laundering offence. *R (NCA) v. Aven* [2022] EWHC 2631 (Admin) concerned bank account freezing orders obtained by the NCA pursuant to Part V, Chapter 3B (Section 303Z ff) of POCA in respect of monies connected to a person designated under the Russia sanctions regulations (the designated person or DP). Among other things, the NCA successfully advanced the position that the transfer of monies to the bank accounts of the third party shortly before the designation of the DP could be evidence that the monies were intended to be used in unlawful conduct (i.e., payments that would be prohibited if financial sanctions were imposed against the DP, and therefore, fell within the scope of the POCA bank account freezing and forfeiture provisions).

81 The MLR remain in force in the UK in amended form, following Brexit. See, e.g., Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020/991.

82 Following the 2018 Financial Action Task Force Mutual Evaluation Report for the UK, HMT undertook to consider whether new powers or guidance are necessary to enable all anti-money laundering (AML) supervisors to take enforcement action when there are deficiencies in their regulated populations' financial sanctions systems and controls. HMT, Home Office Economic Crime Plan, 2019–2022, Action 17, Paragraph 4.13. The Economic Crime Plan: Statement of Progress July 2019–February 2021 records: 'HMT is reviewing the systems and controls in place under the UK's AML supervisory regime to monitor financial sanctions compliance. HMT has worked with the [professional body supervisors] to better understand the compliance practices within their regulated populations and will continue to engage them throughout this year to improve sanctions systems and controls.' The Economic Crime Plan 2 (2023–2026) states, first, that the Financial Conduct Authority (FCA) has strengthened its supervisory approach in assessing financial services firms' sanctions controls and that the Office for Professional Body Anti-Money Laundering Supervision has been similarly working with professional body supervisors (paragraph 3.4) and second, that 'Government commits to continue to provide all relevant sectors with the proper guidance, support, and collaboration around these various sanctions regimes' (paragraph 3.8). The MLR contain scant reference to economic sanctions, although Regulation 33 specifies that when assessing whether there is a high risk of money laundering or terrorist financing for the purpose of applying enhanced due diligence measures and enhanced ongoing monitoring, one of the risk factors relevant firms must take into account is whether the customer is resident in a country 'subject to sanctions, embargos [sic] or similar measures issued by, for example, the European Union or the United Nations' (Regulation 33(6)(a)(ii), (c)(iii)).

to comply with more general AML and counterterrorist financing compliance obligations under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR), such as the obligation to conduct ordinary or enhanced customer due diligence or transaction monitoring.[83] Failing to operate adequate compliance systems to address AML and to combat the financing of terrorism is a breach of Regulation 19 of the MLR; that is to say, the requirement under the MLR to adopt 'proportionate' systems and controls.[84] This, in turn, constitutes an offence under Regulation 86 of contravening a relevant requirement, which is punishable by an unlimited fine or imprisonment for two years (or both) following conviction on indictment and three months on summary conviction.

In 2021, the Financial Conduct Authority (FCA) brought its first criminal prosecution for breaches of the MLR. This resulted in NatWest bank pleading guilty and being fined £264,772,619.95.[85] As an alternative to bringing criminal proceedings, the designated supervisory authorities under the MLR, such as the

---

83 The MLR's compliance obligations relating to AML and countering the financing of terrorism apply to 'relevant firms' (i.e., persons acting in the course of business carried on by them in the United Kingdom who are credit institutions, financial institutions, auditors, insolvency practitioners, external accountants, tax advisers, independent legal professionals, trust or company service providers, estate agents, letting agents, high-value dealers, casinos, art market participants, cryptoasset exchange providers, custodian wallet providers or auction platforms) (Regulation 8).

84 In considering what is appropriate or proportionate with regard to the size and nature of its business, a relevant firm may take into account any guidance that has been issued by the FCA or issued by any other supervisory authority or appropriate body and approved by HMT. Reference should be made, inter alia, to the guidance published by the FCA, the Joint Money Laundering Steering Group (JMLSG), the Office for Professional Body Anti-Money Laundering Supervision, the Law Society and other sources. In addition to a breach of the MLR, a regulated person may be in breach of general compliance obligations established under its particular regulatory scheme. For example, FCA-regulated entities that fail to adopt appropriate policies and procedures for screening and reporting sanctions breaches may be in breach of general FCA compliance obligations and, in particular: 'Principle 3 of the FCA's Principles for Businesses, which requires regulated firms to take reasonable care to organise their affairs responsibly and effectively, with adequate risk management systems; and SYSC 3.2.6 and related provisions contained in the FCA's Senior Management, Arrangements, Systems and Controls Sourcebook (SYSC) that require firms to establish and maintain effective systems and controls to counter the risk that the firm might be used to further financial crime'. See also, FCA, 'Financial Crime Guide: A firm's guide to countering financial crime risks (FCG)' (February 2023), Chapter 7.

85 See www.fca.org.uk/news/press-releases/natwest-fined-264.8million-anti-money-laundering-failures.

FCA, HMRC or various professional bodies,[86] may elect to use their powers to impose civil penalties of fines and issue public statements of censure, prohibit individuals from having a management role in 'a named relevant firm or payment service provider', suspend or remove a person's permission to carry on a regulated activity, deny applications for authorisation or registration, or impose other limitations or restrictions on these persons.[87] In March 2021, the FCA had 42 investigations ongoing into firms and individuals.[88] In 2010, the FCA had used its civil powers to fine the Royal Bank of Scotland Group (of which NatWest is a part) £5.6 million for breaches of the MLR 2007 for failing to have adequate systems and controls in place to prevent breaches of UK sanctions.[89]

86 The UK has 25 AML/counterterrorist financing supervisors appointed by HMT under the MLR. There are three statutory supervisors (the FCA, HMRC and the Gambling Commission) and 22 professional body accountancy and legal supervisors. For a complete list, see MLR, Regulation 7(1)(b), (2) and Schedule 1.

87 MLR, Regulations 76–78. See also HMRC Guidance, 'Civil Measures for money laundering supervision' (updated 9 December 2020), www.gov.uk/government/publications/money-laundering-supervision-enforcement-measures/money-laundering-supervision-civil-measures (accessed 10 April 2023).

88 'The importance of purposeful anti-money laundering controls': speech by Mark Steward, Executive Director of Enforcement and Market Oversight, delivered at the AML & ABC Forum 2021, www.fca.org.uk/news/speeches/importance-purposeful-anti-money-laundering-controls (accessed 15 May 2023).

89 FCA Decision Notice dated 2 August 2010, available at www.fca.org.uk/publication/final-notices/rbs_group.pdf (accessed 17 April 2023).

The civil fines can be sizeable.[90]

In 2020, the FCA fined Commerzbank AG £37.8 million for failing to put adequate AML systems and controls in place between October 2012 and 2017. Although these failings were not specific to sanctions controls, the FCA did note that they occurred 'against a background of heightened awareness within Commerzbank . . . following action taken by US regulators in 2015' in relation to sanctions and AML failings, which the bank settled for a total of US$1.452 million.

In 2010, the Royal Bank of Scotland Group was fined £5.6 million for failing to have adequate systems and controls in place to prevent breaches of UK financial sanctions, as required under the Money Laundering Regulations 2007.

90 In 2017, the FCA imposed its largest penalty to date, of £163 million, on Deutsche Bank AG for failing to maintain adequate AML controls, finding that the breaches of the MLR obligations also amounted to a breach of Principle 3 and SYSC Rules 6.1.1 R and 6.3.1 R (Press Release, FCA, 31 January 2017, at www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure); FCA Final Notice, 30 January 2017, at www.fca.org.uk/publication/final-notices/deutsche-bank-2017.pdf. For details of the FCA's action against Commerzbank, see FCA Final Notice 2020, § 2.7, at www.fca.org.uk/publication/final-notices/commerzbank-ag-2020.pdf; Press Release, Commerzbank AG, 12 March 2015, at www.commerzbank.com/en/hauptnavigation/aktionaere/service/archive/ir-nachrichten_1/2015_2/ir_nachrichten_detail_15_49802.html. For details of the Financial Services Authority (FSA) action against the Royal Bank of Scotland Group, see Press Release, FSA, 3 August 2010, at www.fca.org.uk/news/press-releases/fsa-fines-royal-bank-scotland-group-%C2%A356m-uk-sanctions-controls-failings; FSA Final Decision Notice (2 August 2010), at https://webarchive.nationalarchives.gov.uk/20130202120729/http://www.fsa.gov.uk/static/pubs/other/rbs_group.pdf (accessed 3 April 2023). In October 2020, the FCA and the Prudential Regulation Authority (PRA) fined Goldman Sachs £96.6 million for risk management failures connected to 1Malaysia Development Berhad (1MDB) and its role in three fundraising transactions for 1MDB, see www.fca.org.uk/news/press-releases/fca-pra-fine-goldman-sachs-international-risk-management-failures-1mdb and the FCA Final Notice, 21 October 2020, at www.fca.org.uk/publication/final-notices/gsi-2020.pdf (accessed 3 April 2023). In 2021, the FCA imposed a penalty of £63,946,800 on HSBC in relation to breaches of the Money Laundering Regulations 2007 regarding financial crime in the retail sector, at www.fca.org.uk/publication/decision-notices/hsbc-bank-plc.pdf (accessed 3 April 2023) and a penalty of £147,190,200 on Credit Suisse for breaches of Principles 2 and 3 regarding anti-bribery and corruption failings in the investment banking sector, at www.fca.org.uk/publication/final-notices/credit-suisse-2021.pdf (accessed 3 April 2023). In 2022, the FCA imposed a fine of £107,793,300 on Santander UK plc for breaches related to related to the risk of financial crime in the retail banking sector, see Final Notice dated 8 December 2022, at www.fca.org.uk/publication/final-notices/santander-uk-plc-2022.pdf (accessed 17 April 2023).

Enforcement actions for breach of AML compliance requirements have extended to cases in which the sanctions issues have been breaches of US sanctions law.[91]

In 2019, Standard Chartered Bank was fined £102 million by the FCA for breaches of the Money Laundering Regulations 2007, which was part of US$1.1 billion total financial penalties arising from breaches of US sanctions.

Financial services regulators will expect their regulated populations to notify them of known or suspected sanctions breaches.[92]

In 2017, the Prudential Regulation Authority (PRA) of the Bank of England imposed a £17.85 million fine on The Bank of Tokyo-Mitsubishi UFJ Ltd (BTMU) and an associated fine of £8.925 million on MUFG Securities EMEA plc for failing to be open and cooperative with the PRA in relation to sanctions enforcement action into BTMU by the New York Department of Financial Services.

91 See www.fca.org.uk/news/press-releases/fca-fines-standard-chartered-bank-102-2-million-poor-aml-controls (accessed 3 April 2023). In its Decision Notice, the FCA noted that 'inadequate Due Diligence and ongoing monitoring not only exposed SCB to sanctions evasion but also increased the risk of SCB receiving and/or laundering the proceeds of crime': FCA Decision Notice, Paragraph 2.8, at www.fca.org.uk/publication/decision-notices/standard-chartered-bank-2019.pdf (accessed 3 April 2023). In 2012, HSBC Group received a 'requires action' notice in coordination with but separate to the US$1.92 billion financial penalties imposed by US authorities for breaches of US sanctions laws that had highlighted HSBC's AML and sanctions compliance failings (Press Release, FSA, 11 December 2012, 'FSA requires action of the HSBC Group' (FSA/PN/111/2012), at www.fca.org.uk/publications/documents/fsa-requires-action-hsbc-group; FSA Notices (and statements re: firms, individuals) 2012, p. 34 (accessed 3 April 2023)).

92 For FCA-regulated firms, this is expressed in Principle 11 of the FCA's Principles for Businesses: 'A firm must deal with its regulators in an open and cooperative way, and must disclose to the FCA appropriately anything relating to the firm of which that regulator would reasonably expect notice.'

This £26.78 million in total fines issued to UK Bank of Tokyo-Mitsubishi entities illustrates the importance UK financial regulators place on international financial institutions making them aware of overseas enforcement actions so that they may assess the implications for the systems and controls of UK affiliates.[93]

Suspicious activity reports

POCA imposes reporting obligations on private entities in the regulated sector and creates offences for non-reporting.[94] These arise when a relevant firm knows or suspects or has reasonable grounds for knowing or suspecting that another person is engaged in money laundering when that knowledge came to them in the course of business.[95] Failing to report suspicions of money laundering or

93 See www.bankofengland.co.uk/news/2017/february/pra-imposes-fine-on-the-bank-of-tokyo-mitsubishi-ufj-limited-and-fine-on-mufg-securities-emea-plc. Note: conversely, in 2019, British Arab Commercial Bank reported to and involved the PRA in its negotiations with the US Treasury's Office of Foreign Assets Control (OFAC) in respect of apparent breaches of US sanctions. This led to the immediate penalty imposed by OFAC being reduced from US$228.4 million to US$4 million with the remainder suspended because the PRA confirmed that enforcement would lead to the bank becoming insolvent.

94 The offences under POCA Sections 330 and 331 carry a maximum sentence of five years' imprisonment on indictment. Similar provisions are contained within the Terrorism Act 2000, Section 21A in relation to knowledge or suspicion of terrorist financing offences.

95 The threshold of 'suspicion' engaging the requirement to make a suspicious activity report (SAR) is low. In *Da Silva* [2006] EWCA Crim 1654, [16] and [17], 'suspecting' means the person 'must think there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice.' In an appropriate case, the suspicion 'must be of a settled nature; a case might, for example, arise in which a defendant did entertain a suspicion in the above sense but, on further thought, honestly dismissed it from his or her mind as being unworthy or as contrary to such evidence as existed or as being outweighed by other considerations'. The test expressed in *Da Silva* is widely replicated in statutory guidance. See, e.g., the Law Society guide, 'Suspicious activity reports', last updated 9 March 2023, at www.lawsociety.org.uk/en/topics/anti-money-laundering/suspicious-activity-reports. The JMLSG Guidance describes suspicion (at [6.11]) as 'more subjective [than knowledge] and falls short of proof based on firm evidence. [It is] beyond mere speculation and based on some foundation'; see JMLSG, 'Prevention of money laundering/combating terrorist financing' (2020 revised version amended July 2022), at www.jmlsg.org.uk/guidance/current-guidance/ (accessed 17 April 2023). In deciding whether a person has committed an offence under Section 330 or Section 331, the court must consider whether they followed any relevant guidance that was at the time concerned issued by a supervisory authority or any other appropriate body, approved by the Treasury and published in a manner it approved as appropriate in its opinion to bring the guidance to the attention of persons likely to be affected by it (POCA, Sections 330(8) and 331(7)). A person does not commit an offence under either of these sections if they have a reasonable excuse for not making the required disclosure or the information that otherwise

terrorist funding to a firm's nominated officer or to file a SAR as soon as practicable may also demonstrate AML compliance failings that amount to a breach of the MLR.[96] Filing a SAR does not absolve a person in the regulated sector of their obligation to report subject assets[97] of designated persons or breaches of sanctions laws to OFSI.[98] Both those in and outside the regulated sector may file SARs. Irrespective of the obligations upon those within the regulated sector to do so, which are described above, regulated and non-regulated entities may wish to file a SAR in respect of assets with which they intend to deal in order to obtain a Defence Against Money Laundering (DAML) from the NCA; in other words, authorisation to deal with the subject assets. SARs are submitted to the NCA via the NCA SAR Online System. The offences under POCA Sections 330 and 331 carry a maximum sentence of five years' imprisonment.[99]

Where a DAML request is filed, POCA prohibits the carrying out of any transaction in relation to the subject property without NCA consent, or the expiry of the prescribed time limits.[100] A person in the regulated sector may not disclose

---

is required to be disclosed came to the person in legally privileged circumstances (Sections 330(6)(a), (b)(7B) and 331(6)). A person will not commit an offence under Section 330 on the basis that they had reasonable grounds to know or suspect another person is engaged in money laundering where they have not been specified training by their employer. The scope of the 'reasonable excuse' defence is not defined in POCA; it is covered in some of the statutory guidance; see, e.g., The Law Society guide on 'Suspicious activity reports', last updated 9 March 2023, at www.lawsociety.org.uk/en/topics/anti-money-laundering/suspicious-activity-reports (accessed 3 April 2023).

96 MLR, Regulation 19(4)(d); see also Regulations 21(5), 24, 31(1)(d).

97 See POCA, Sections 335, 338.

98 OFSI, HMT, 'UK Financial Sanctions, General guidance for financial sanctions under the Sanctions and Anti-Money Laundering Act 2018' (August 2022) (5.9), see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1144366/General_Guidance_-_UK_Financial_Sanctions__Aug_2022_.pdf (accessed 3 April 2023).

99 The NCA SAR Online System at www.ukciu.gov.uk/(hsacnc55jt4f20ucgkvemfbd)/saronline.aspx. The NCA's SARs 2022 annual report records that 901,255 SARs were made in 2021–2022 (NCA, UK Financial Intelligence Unit, Suspicious Activity Reports Annual Report 2022, at https://nationalcrimeagency.gov.uk/who-we-are/publications/632-2022-sars-annual-report-1/file) (accessed 3 April 2023). This was a 21.41 per cent increase on 2020–2021.

100 See POCA, Sections 335 and 336D. In summary: after an initial period of seven working days, the NCA must either consent to transactions or expressly withhold consent, in which case a moratorium period of 31 days starts to run (Section 335). If the NCA does not respond within the initial period, consent is deemed, and dealing with the assets would not constitute an offence under Sections 330 and 331. If it withholds consent, the NCA may apply to the Crown Court to extend the first moratorium period (the 31 days) for a further (maximum) period of 186 days (Section 336A). Only in exceptional circumstances might

that a SAR has been filed or that a related investigation is being contemplated or is being carried out.[101] A disclosure that is 'likely to prejudice' an investigation amounts to a tipping-off offence.[102] Even if no SAR has been filed, if a person knows or suspects that a confiscation investigation, a civil recovery investigation or a money laundering investigation is being or about to be conducted, that person commits an offence by making a disclosure that is likely to prejudice the investigation.[103] This offence is not limited to persons in the regulated sector.[104]

Effect on investigations

The filing of a SAR may be the precursor to a range of investigative orders or civil[105] or criminal asset recovery orders on the application of law enforcement authorities such as the NCA, the police, the SFO, HMRC and the FCA. These may include:

- Crown Court production orders,[106] search warrants,[107] restraint orders[108] and, in post-conviction cases, confiscation orders;[109]

---

an account holder be able to seek interim relief requiring a reporting bank to operate an account subject to a SAR during a moratorium period. *National Crime Agency v. N* [2017] 1 WLR 3938.

101 Section 333B protects, subject to conditions, disclosure within the 'undertaking or group' (e.g., internally within the bank or internally within a law firm). Sections 333C and 333D protect disclosure in other defined circumstances.

102 POCA, Section 333A.

103 id., Section 342(2)(a).

104 These provisions do not mean that a SAR may never be disclosed to an account holder but the circumstances in which it will be lawful to do so are limited. *Lonsdale v. National Westminster Bank Plc* [2018] EWHC 1843 (QB).

105 See, e.g., *R (NCA) v. Aven* [2022] EWHC 2631 (Admin) where a series of SARS filed by banks, indicating suspicions that funds were being moved between accounts to circumvent the sanctions imposed on Mr Aven or were intended to assist with sanctions evasion, were the precursor to account freezing orders.

106 See, e.g., *Golfrate* [2014] 2 Cr App R 12 (money laundering investigation in relation to suspected breach of EU sanctions imposed against members of Zanu-PF precipitated by a bank filing a SAR).

107 In *Golfrate*, the police applied for search warrants under POCA, Sections 352(1) and 352(6)(b).

108 POCA, Section 40. A restraint order may be granted if a criminal investigation has begun, there are reasonable grounds to suspect the subject of the restraint order has benefited from their criminal conduct, and there is a real risk that the assets will be dissipated if the restraint order is not made.

109 See section titled 'Asset recovery', below.

- magistrates' courts' arrest warrants,[110] search warrants,[111] and bank and building society account freezing and forfeiture orders;[112] and
- High Court property freezing orders, civil recovery orders[113] and unexplained wealth orders.[114]

Duties of counsel and privilege

Overview

The role of lawyers in sanctions and AML regimes requires special consideration. The starting point is that LPP applies.[115] A professional legal adviser continues to be exempt from the reporting obligations under sanctions legislation and POCA if the information or other matter comes to them in legally privileged circumstances.[116]

---

110 Magistrates' Courts Act 1980, Section 1.

111 The Police and Criminal Evidence Act 1984, Section 8.

112 POCA, Sections 303Z1–303Z8 (freezing) and 303Z14–303Z17 (forfeiture).

113 See, e.g., the *Mabey & Johnson* case, described in footnotes 130, 171 and 179, below.

114 A requirement for making an unexplained wealth order is that the respondent is either a politically exposed person or there are reasonable grounds for suspecting that the respondent or a person connected with the respondent is or has been involved in serious crime (POCA, Section 362B(4)). 'Serious crime' includes an offence under UK sanctions legislation (POCA, Section 362B(9)(a), Serious Crime Act 2007, Section 2, Schedule 1, Paragraph 13B).

115 See *Bowman v. Fels* [2005] 1 WLR 3083, 3108F-H, at [78]. For recent Court of Appeal cases considering the scope of the two limbs of LPP, namely litigation privilege and legal advice privilege, see, respectively, *Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Ltd* [2019] 1 WLR 791 and *R (on the application of Jet2.com Limited) v. Civil Aviation Authority* [2020] EWCA Civ 35. The Solicitors Regulation Authority has published guidance, 'Complying with the UK Sanctions Regime' (28 November 2022), www.sra.org.uk/solicitors/guidance/financial-sanctions-regime/ (accessed 3 April 2023). The Bar Standards Board (BSB) has also published sanctions guidance for barristers, chambers and BSB entities about compliance with sanctions obligations, www.barstandardsboard.org.uk/for-barristers/compliance-with-your-obligations/sanctions.html (accessed 3 April 2023).

116 Typical wording for this exclusion in sanctions regulations is contained in, e.g., Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019, Section 109(3): 'Nothing in this Part is to be read as requiring a person who has acted or is acting as counsel or solicitor for any person to disclose any privileged information in their possession in that capacity.' In POCA, see Section 330(6) and (7B), 'Failure to disclose: regulated sector', which provides that a person does 'not commit an offence under this section if . . . (b) he is a professional legal adviser or relevant professional adviser and – (i) if he knows either of the things mentioned in subsection (5)(a) [identity of person engaged in money laundering] and (b) [whereabouts of laundered property], he knows the thing because of information or other matter that came to him in privileged circumstances, or (ii) the information or other matter mentioned in subsection (3) came to him in privileged

OFSI recognises that the duty to make reports to OFSI does not 'override or supersede' LPP and that LPP may constitute a reasonable excuse for not disclosing information or documents when otherwise required under sanctions regulations.[117] OFSI's Guidance on Financial Sanctions notes, however, that it 'expects legal professionals to carefully ascertain whether legal privilege applies, and which information it applies to' and observes that OFSI may challenge blanket assertions of privilege.[118]

English law does not distinguish between in-house and independent external counsel for the purposes of LPP.[119] LPP is subject to the 'crime/fraud exception': it does not apply to information or any other matter that is communicated or given to the professional legal adviser with the intention of furthering a criminal purpose.[120] This may have increasing relevance with the current focus among UK enforcement agencies on 'professional enablers' of sanctions breaches.[121]

---

circumstances, or (c) subsection . . . (7B) applies to him.' Subsection (7B) applies to a person if – '(a) he is employed by, or is in partnership with, a professional legal adviser or a relevant professional adviser to provide the adviser with assistance or support, (b) the information or other matter mentioned in subsection (3) comes to the person in connection with the provision of such assistance or support, and (c) the information or other matter came to the adviser in privileged circumstances.' The wording in the sanctions statutory instruments is therefore arguably narrower than in POCA. The implications (i.e., whether that is lawful or an *ultra vires* abrogation of the principle of LPP fundamental to the rule of law) are untested.

117 'Such protections may apply even where not explicitly referenced [in the Regulations]', OFSI Monetary Penalties Guidance, § 3.39.

118 OFSI, Financial Sanctions Guidance [5.4].

119 The English law approach is not reflected in EU law: Case C-550/07P, *Akzo Nobel Chemicals Ltd v. Commission of the European Communities* [2011] 2 AC 338.

120 *R v. Central Criminal Court, Ex parte Francis & Francis* [1989] AC 346, 397 (HL): 'privilege will only be excluded in so far as it relates to communications . . . made with the . . . intention of furthering a criminal purpose. No other communication will be excluded from the application of the privilege; and the client's confidence will to that extent be protected'. POCA, Section 330(11) reflects this exception.

121 See, e.g., National Economic Crime Centre and OFSI, 'Red ALERT Financial Sanctions Evasion Typologies: Russian Elites and Enablers' (July 2022), which refers to facilitation by 'professionals such as lawyers', https://nationalcrimeagency.gov.uk/who-we-are/publications/605-necc-financial-sanctions-evasion-russian-elites-and-enablers/file (accessed 3 April 2023).

Resolution

Overview

OFSI has the power to respond to breaches of financial sanctions by taking action with increasing levels of severity, ranging from low-level outcomes such as issuing a warning, naming and shaming without further penalty or referring concerns to relevant regulatory bodies, to imposing a civil financial penalty or, in the most serious cases, referring the case for criminal investigation and prosecution.[122] Criminal prosecutions can only be brought where a prosecutor has determined that the proceedings would meet the 'full code test', namely that in respect of each defendant, there is sufficient evidence to provide a realistic prospect of conviction on each charge and that prosecution would be in the public interest.[123] In contrast, OFSI applies a civil standard of proof, namely that on the 'balance of probabilities' a breach has occurred, to its enforcement actions.

This section begins with an overview of criminal proceedings relating to sanctions offences, including prosecution, DPAs and agreements that individuals may reach with prosecutors. It then describes OFSI's civil penalty regime. It concludes by identifying some of the ancillary measures that may be imposed following a sanctions violation.

Criminal prosecution

Primary sanctions offences and licensing offences are punishable upon conviction on indictment by a fine or imprisonment for up to 10 years.[124] Reporting and information offences are summary offences punishable by a fine or the maximum

122 OFSI Monetary Penalties Guidance, § 3.2. The actions are not mutually exclusive, and several can be taken in a given case. For a summary of enforcement activity in 2021–2022, see the OFSI Annual Review (April 2021 to August 2022), pp. 11–13, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1116689/OFSI_Annual_Review_2021-22_10.11.22.pdf (accessed 17 April 2023). The Economic Crime (Transparency and Enforcement) Act 2022, Section 56 amended Section 149 of the Policing and Crime Act 2017 to allow OFSI to publish reports of cases in which it has not imposed a money penalty but in which it is satisfied, on the balance of probabilities, that a person has breached a prohibition or failed to comply with an obligation.

123 The 'Full Code Test' is set out in the Code for Crown Prosecutors, available at www.cps.gov.uk/publication/code-crown-prosecutors (accessed 17 April 2023).

124 SAMLA, Section 17(5)(a).

term of imprisonment that magistrates' courts can impose (six months).[125] Confidentiality offences may be punishable following conviction on indictment by a fine or up to two years' imprisonment.[126]

To secure a conviction, the prosecution must prove beyond reasonable doubt that the person has committed the *actus reus* (conduct) with the requisite *mens rea* (mental element) of the relevant sanctions offence, whether as a principal, a secondary party or a conspirator. It is also an offence to encourage or assist a sanctions offence intending to do so or believing that this type of offence will be committed.[127] As described above, both companies and corporate officers may be liable for criminal offences.[128]

Historically, UK financial sanctions enforcement by way of criminal prosecution has been limited.[129] Two groups of prosecutions, the *Mabey & Johnson* and *Weir Group* cases, concerned bribes paid in the context of the UN Iraq Oil-For-Food programme.[130]

Following the introduction of the Economic Crime (Transparency and Enforcement) Act 2022, a new cell was established within the NCA in July 2022 to target 'kleptocracy' and sanctions evasion (the Combating Kleptocracy Cell). The increased focus on the imposition of sanctions against Russia in 2022 may lead to greater criminal enforcement of sanctions, including criminal proceedings for circumvention of sanctions. At the time of writing, there were active NCA investigations into alleged sanctions circumvention.

---

125 This may rise to a maximum term of imprisonment of 12 months for offences committed after Section 224 of the Sentencing Act 2020 comes into force. SAMLA, Section 17(5)(b)(i); see, e.g., Russia (Sanctions) (EU Exit) Regulations 2019/855, Regulations 70, 74 and 80(4), and Burma (Sanctions) (EU Exit) Regulations 2019/136, Regulation 51(4).

126 See, e.g., Russia (Sanctions) (EU Exit) Regulations 2019/855, Regulation 80(3) and Burma (Sanctions) (EU Exit) Regulations 2019/136, Regulation 51(3).

127 Serious Crime Act 2007, Sections 44–46.

128 See section titled 'Liability for secondary parties, inchoate offences, corporates and company officers', above.

129 For discussion of prosecutions for breaches of trade sanctions and export controls, see Chapters 8 and 9.

130 The case against the three senior executives of Mabey & Johnson Ltd was subject to interlocutory appellate proceedings: see *R v. Forsyth* [2011] 2 AC 69. The parent company was later subject to High Court civil recovery proceedings. (See footnote 153, below.) For details of the prosecution of Weir Group Plc, see www.copfs.gov.uk/publications/bribery-act (accessed 5 May 2021).

In 2009, Mabey & Johnson Ltd pleaded guilty to charges including 'making funds available' in violation of Article 3 of the Iraq (United Nations Sanctions) Order 2000. The company was sentenced to total financial penalties, including costs, confiscation, reparations and monitoring costs, of about £6.6 million. Two ex-directors of the company were subsequently tried and convicted for their roles and were sentenced to terms of immediate imprisonment. An ex-sales manager cooperated with the SFO, pleaded guilty and gave evidence against the directors at their trial; he was sentenced to a suspended term of imprisonment.

In 2010, Scottish company Weir Group plc pleaded guilty to breaching sanctions in relation to Iraq through the payment of kickbacks in return for contracts from Saddam Hussein's government. It was sentenced to financial penalties of £3 million and received a confiscation order for £13.9 million.

Deferred prosecution agreements

DPAs are a mechanism by which organisations (typically companies) make an agreement with either the CPS or SFO, under the supervision of a judge, that a criminal prosecution will be suspended for a defined period if the organisation meets certain conditions, which may include financial penalties, compensation, cooperation in the prosecution of individuals and the implementation of appropriate compliance programmes.[131] Since 2017, DPAs have been available in respect of sanctions offences.[132] There has been a small number of DPAs since they were introduced in 2013, most of which have related to significant corporate offending.[133]

131 Crime and Courts Act (CCA) 2013, Section 45 and Schedule 17. The Act identifies the designated prosecutors that may enter into a DPA as the Director of Public Prosecutions in England and Wales (DPP) and the Director of the SFO and any other prosecutor so designated by the Secretary of State (Schedule 17, Paragraph 3).

132 CCA 2013, Schedule 17 Paragraph 26A, introduced by the Policing and Crime Act (PCA) 2017, Section 150 and subsequently amended to include sanctions offences created by regulations promulgated under SAMLA.

133 See *R v. Airbus SE* [2020] 1 WLUK 435; *SFO v. Rolls-Royce Plc, Rolls-Royce Energy Systems Inc* [2017] 1 WLUK 189; *Tesco Stores Ltd* [2017] 4 WLUK 558; *SFO v. XYZ Limited* (unrep), 11 July 2016, Sir Brian Leveson P; *SFO v. Standard Bank Plc* [2015] 11 WLUK 802.

The financial penalty levied upon the defendant company must be broadly comparable to the fine that a court would have imposed following conviction after a guilty plea.[134] The non-prosecution, however, may enable the company to avoid significant, consequential financial effects that might flow from a conviction. Airbus, for example, assessed the loss of global revenue that might follow from debarment from public tendering as US$200 billion.[135]

The CPS and SFO DPA Code of Practice governs, among other things, the factors the prosecutor may take into account when deciding whether to enter into a DPA, the process for negotiations, terms of a DPA, including the financial penalty, applying for court approval of a DPA and overseeing a DPA after its approval.[136] Voluntary self-reporting, subsequent cooperation and restorative measures are public interest factors tending away from prosecution and towards a DPA.[137] The DPA Code will apply in sanctions breach cases, as will the Code for Crown Prosecutors, the CPS/SFO Joint Prosecution Guidance on Corporate Prosecutions and, where corruption offences may also have occurred, the Joint Prosecution Guidance on the Bribery Act 2010.

Arrangements between prosecutors and individual defendants

Frequently, there are plea arrangements between defendants and prosecutors, which may take various forms. In some, the defendant pleads guilty to part of an indictment and the prosecution offers no evidence on the remaining counts on that indictment or asks the court to allow those counts to lie on the file. In others, the defendant pleads guilty to a lesser offence or to the indicted offence but on a less serious factual basis than that originally alleged against them.[138]

134 CCA 2013, Schedule 17, Paragraph 5(4); DPA Code, §§ 7.9(iii), (iv), 8.3, 8.4; *Standard Bank Plc* [2015] 11 WLUK 804, [16].

135 *Director of the Serious Fraud Office v. Airbus SE* [2020] 1 WLUK 435 [85].

136 See www.cps.gov.uk/sites/default/files/documents/publications/dpa_cop.pdf.

137 DPA Code, § 2, in particular, § § 2.8.1(iii), (iv), (v), 2.8.2(i), 2.9.1.

138 The principles an English prosecutor should apply in these situations are contained within Section 9 of the Code for Crown Prosecutors and the Attorney General's Guidelines on the Acceptance of Pleas and the Prosecutor's Role in the Sentencing Exercise. Additionally, the Attorney General's Guidelines on Plea Discussions in Cases of Serious or Complex Fraud may apply in some sanctions cases.

When a defendant offers to provide information or to give evidence about the criminal activities of others, they may enter into a formal written arrangement with a specified prosecutor, known as a 'SOCPA agreement'.[139] In return for providing information or giving evidence in accordance with the agreement, a defendant could potentially achieve immunity from prosecution[140] but more likely would receive a reduced sentence in respect of their own criminality.[141] The level of sentence reduction will depend on the timing, nature, extent and value of the assistance offered or provided. In cases of genuine and substantial assistance, it could be a reduction of between one-half and two-thirds of the sentence that a defendant would otherwise receive.[142]

Civil monetary penalties

Following the establishment of OFSI in 2016, HM Treasury was given a power to impose monetary penalties for sanctions breaches on companies and officers of companies.[143] Prior to the introduction of the Economic Crime (Transparency and Enforcement) Act 2022 on 15 March 2022, OFSI could impose a monetary penalty if satisfied, on the balance of probabilities, that a person has breached a prohibition or failed to comply with an obligation imposed by or under financial sanctions legislation and that the person knew or had reasonable cause to suspect that they were in breach of the prohibition or had failed to comply with the obligation.[144] Following the entry into force of the Act on 15 June 2022, OFSI is now able to impose monetary penalties on a strict liability basis.[145]

---

139 SOCPA, Sections 71–75B. See also, CPS guidance 'SOCPA 2005 – Queen's evidence: Immunities, Undertakings and Agreements' and 'SOCPA Agreements: Note for those representing assisting offenders'. The DPP and the Director of the SFO are specified prosecutors: SOCPA, Section 71.

140 SOCPA, Section 71 empowers a specified prosecutor to issue a written immunity notice with the effect that no proceedings for any offence specified in the notice may be brought against that person except in circumstances specified in the notice. An immunity notice ceases to have effect if the person fails to comply with any conditions specified within it.

141 For a 'typical example' of such an agreement, see *Blackburn* [2008] 2 Cr App R (S) 5, [7].

142 *Blackburn* [2008] 2 Cr App R (S) 5, [41].

143 PCA 2017, Sections 146–149.

144 id., at Section 146(1).

145 Policing and Crime Act 2017 at Section 146, as amended by the Economic Crime (Transparency and Enforcement) Act 2022 at Section 54.

OFSI describes its approach to deciding whether to impose a monetary penalty as the application of its 'holistic' compliance and enforcement model: 'promote, enable, respond, change'.[146] This means that OFSI seeks to: 'promote' compliance by publicising financial sanctions and engaging with the private sector; 'enable' compliance by giving guidance and alerts on responsibilities; 'respond' to non-compliance by intervening to disrupt attempted breaches and tackling completed breaches; and 'change' behaviour by preventing future non-compliance.

When a monetary penalty is payable by a legal person, HM Treasury may also impose a monetary penalty on an officer of the body if satisfied, on the balance of probabilities, that the legal person's breach or failure took place with the consent or connivance of the officer or was attributable to any neglect by the officer.[147] If OFSI can estimate the value of the funds involved in the breach, the maximum penalty is the greater of £1 million or 50 per cent of the estimated value. In all other cases, the maximum penalty is £1 million.[148]

OFSI must observe various procedural steps before imposing a monetary penalty. They include providing the target with: (1) notice of OFSI's intention to impose a monetary penalty;[149] (2) an opportunity to make representations about any relevant matters, including matters of law, the facts of the case, how OFSI has followed its process and whether the penalty is fair and proportionate;[150] and, if a penalty is imposed, (3) the right to a ministerial review.[151] There is then a right of appeal to the Upper Tribunal.[152]

---

146 See OFSI, Monetary penalties for breaches of financial sanctions: guidance, Chapter 3, available at www.gov.uk/government/publications/ofsi-guidance-html-documents/monetary-penalties-for-breaches-of-financial-sanctions-guidance (accessed 17 April 2023).

147 id., at Section 148.

148 id., at Section 146(3).

149 OFSI Monetary Penalties Guidance, § 5.2.

150 id., at § 5.4.

151 id., at § 6.3. PCA 2017, at Section 174. These are reflected in OFSI's Monetary Penalties Guidance. OFSI will impose a 28-day period in which to make representations. Late representations are not normally accepted and any request for an extension must be accompanied by evidence (OFSI Monetary Penalties Guidance, § 5.10). If no representations are made within that time frame, the penalty will be finalised and the person will become liable to make payment (§ 5.11). OFSI aims to issue a response within 28 working days of the deadline for representations (§ 5.13). Section 55 of the Economic Crime (Transparency and Enforcement) Act 2022 provides that the review no longer needs to be conducted by the Minister personally.

152 PCA 2017, Section 146(6). The Upper Tribunal may quash the Minister's decision and (1) quash the decision to impose a penalty or (2) uphold the decision to impose a penalty but substitute a different amount for the amount determined by HMT(Section 146(7)).

When deciding how to dispose of a case and the size of any monetary penalty, OFSI applies a three-step process: (1) penalty threshold; (2) baseline penalty matrix; and (3) penalty recommendation.[153] The penalty threshold is met if the statutory threshold for imposing a penalty has been met and a monetary penalty would be appropriate and proportionate. The 'appropriate and proportionate' limb will most likely be met if (1) funds or economic resources were made available to or for the benefit of a designated person, (2) a person has dealt with the funds or economic resources of a designated person in breach of an asset freeze, (3) the sanctions prohibitions were circumvented, or (4) there was non-compliance with a requirement to provide information.[154] If none of these factors is present, OFSI may still conclude that a monetary penalty is appropriate and proportionate.[155]

A 'baseline penalty matrix' is used to calculate the appropriate penalty. First, OFSI will calculate the statutory maximum: the greater of £1 million or 50 per cent of the value of the breach. Second, it will identify a 'reasonable and proportionate' penalty based on its view of the seriousness of the case. This is the 'baseline penalty level'. This could be any amount between the maximum and zero. Third, it will consider whether a penalty reduction for 'prompt and complete voluntary disclosure of the breach' is warranted. In 'serious' cases, this reduction can be up to 50 per cent of the baseline penalty. In the 'most serious' cases, the potential reduction is capped at 30 per cent.[156] The 'most serious' cases may involve: a very high value; particularly poor, negligent or intentional conduct; or severe or lasting damage to the purposes of the sanctions regime.[157]

153 OFSI Monetary Penalties Guidance, § 4.1.

154 id., at § 4.3.

155 ibid.

156 id., at §§ 4.8–4.9 and 4.11.

157 id., at § 3.55.

OFSI will determine whether a penalty is proportionate based on the relationship between the proposed penalty and a 'holistic assessment' of all the other factors present in the case. Penalties need not be 'a specific percentage or multiple of the breach amount'.[158]

When assessing the seriousness of a case, deciding whether or what type of enforcement action is required and identifying aggravating or mitigating factors to determine an appropriate monetary penalty, OFSI will generally take into account[159] the following:

- the value of the breach;[160]
- harm or risk of harm to the objectives of the sanctions regime;[161]
- whether the breach is deliberate, negligent or the result of an error;[162]
- whether the breach is the result of broader systems failures;
- repeated or persistent breaches;[163]
- voluntary self-disclosure of suspected breaches;[164] and
- the public interest in responding to the breaches.[165]

158 id., at § 4.8.

159 OFSI reserves the right to take into account any factor that it considers material and relevant; id., at § 3.51.

160 id., at § 3.18. High-value breaches are generally more likely to result in enforcement action.

161 id., at § 3.19.

162 id., at § 3.32–3.34. OFSI may take into account the actual and expected level of knowledge of sanctions law within an organisation or in respect of an individual (§ 3.20). Failure by regulated professionals to meet regulatory and professional standards may be an aggravating factor (§ 3.21).

163 id., at § 3.37.

164 See section titled 'Self-reporting', above.

165 OFSI Monetary Penalties Guidance, § 3.50.

In 2017 and 2018, OFSI did not impose any civil monetary penalties. Between January 2019 and March 2020, it imposed four monetary penalties, two of which were subject to a ministerial review.[166] Two additional penalties were imposed in both 2021 and 2022.[167]

In 2020, Standard Chartered Bank received penalties of £20.47 million from OFSI for breaches of Ukraine-related sanctions by granting loans worth £97.5 million to the subsidiary of a designated Russian entity.

166 See www.gov.uk/government/collections/enforcement-of-financial-sanctions. The penalties were as follows: (1) Raphael Bank (January 2019): £5,000 penalty for dealing with funds of £200 belonging to a person designated under the Egypt (Asset-Freezing) Regulations 2011. A 50 per cent reduction for voluntary disclosure was applied; (2) Travelex (UK) Ltd (March 2019): £10,000 penalty for dealing with the same funds as Raphael Bank, despite having access to the designated person's passport, which clearly identified the individual by name, date of birth and nationality. There was no voluntary disclosure and so no penalty reduction; (3) Telia Carrier UK Limited (September 2019): £146,341 penalty, reduced from £300,000 following a ministerial review, for making economic resources available to a designated person under the Syria sanctions regime by indirectly facilitating international telephone calls to SyriaTel repeatedly and for an extended period. During the review, the value of the breaches was reassessed as approximately £234,000; there was no voluntary disclosure; (4) Standard Chartered Bank (March 2020): £20.47 million total penalties, reduced from £31.5 million following a ministerial review. A 30 per cent reduction for voluntary disclosure was applied. The Minister substituted a lower penalty figure after finding that although it was a 'most serious' case, OFSI had given insufficient weight to facts that Standard Chartered had not wilfully breached the sanctions regulations, acted in good faith, intended to comply with the restrictions, fully cooperated with OFSI and had taken remediation steps. OFSI Report, 'Imposition of Monetary Penalty – Standard Chartered Bank' [14].

167 The penalties were as follows: (1) TransferGo Ltd (June 2021): £50,000 penalty for making funds available to a designated person by issuing instructions for 16 transactions totalling £7,764.77 to accounts held at the Russian National Commercial Bank (RNCB). No discount was applied for voluntary disclosure, as transactions were only disclosed following requests by OFSI for information; (2) Clear Junction Ltd (June 2021): £36,393.45 penalty for making funds available to a designated person by making transactions totalling £7,703.68 to accounts held at the RNCB. A 26.7 per cent reduction was applied for incomplete voluntary disclosure; (3) Tracerco Ltd (May 2022): £15,000 penalty for making funds available to a designated person (Syrian Arab Airlines) by booking flights for an employee to the value of £2,956.43. A 50 per cent discount was applied for voluntary disclosure; (4) Hong Kong International Wine and Spirits Competition Ltd (September 2022): £30,000 penalty for receiving funds and economic resources from a designated person and making economic resources available to a designated person, namely by receiving payments and wine bottles from the designated person to the value of £3,919.62 and making available publicity to the designated person.

Although caution must be exercised in drawing conclusions from this limited pool of cases, the *Standard Chartered Bank* case in 2020 marks a significant step change and signals a preparedness by OFSI to issue substantial penalties. It also demonstrates the value placed by OFSI on self-reporting, cooperation and remedial action following suspected sanctions breaches. The *Raphael Bank* case suggests that even self-reported breaches of modest value may be considered sufficiently 'serious' for OFSI to determine that a civil monetary penalty is 'appropriate and proportionate'.

Overall, the size of penalties imposed by OFSI remains strikingly small compared with, for example, penalties imposed in the United States by the Office of Foreign Assets Control (OFAC).[168] OFSI is, however, looking to learn from OFAC, and OFSI's recent 'enhanced partnership agreement' with OFAC seeks to 'support OFSI's move to a larger and more proactive organisation'.[169]

As noted above, HMRC also has the power to impose civil penalties against those who breach trade sanctions under its compound penalty scheme. Whereas it regularly publicises some details of exporters against whom compound penalties have been assessed for breaches of export controls, there have been no recent published cases of compound penalties being imposed for exports or transfers of technology in breach of trade sanctions.

Ancillary orders and additional consequences of sanctions breaches

Asset recovery

Recovery of property obtained as a result of sanctions offences may be pursued through confiscation proceedings following prosecution and conviction[170] or in separate civil proceedings.[171]

---

168 See https://ofac.treasury.gov/civil-penalties-and-enforcement-information.

169 OFSI, 'OFAC-OFSI Enhanced Partnership', 17 October 2022, available at https://ofsi.blog.gov.uk/2022/10/17/ofac-ofsi-enhanced-partnership/.

170 *R v. McDowell* [2015] 2 Cr App R (S) 14 (CA). M had negotiated the sale of prohibited items from China to Ghana without a licence, in contravention of Articles 4 and 9(2) of the Trade in Goods (Control) Order 2003. In addition to a sentence of two years' suspended imprisonment, the confiscation order made against M was based on his gross receipts for the trades (approximately £2.5 million) and the commission payments he received.

171 In *Mabey & Johnson*, the offending company's parent company settled civil asset recovery proceedings instituted by the SFO in the High Court under Part 5 of POCA for £130,000 in recognition of sums it had received through share dividends derived from contracts won by Mabey & Johnson Ltd through unlawful conduct: see https://webarchive.nationalarchives.gov.uk/20120314165057/http://www.sfo.gov.uk//press-room/latest-press-releases/press-releases-2012/shareholder-agrees-civil-recovery-by-sfo-in-mabey--johnson.aspx. In 2019, monies received by a niece of Syrian president Bashar al-Assad in breach of the Syrian

There is also the possibility that property frozen under sanctions regulations (which do not themselves alter the legal rights and interests in the property) may itself be subject to an asset recovery order with a view to forfeiture. This could occur where the frozen assets are the realisable property of a convicted person or the property can be shown to have been obtained through or by unlawful conduct or with the intent to use them in circumventing or breaching sanctions[172] or where a private claimant sought to enforce a judgment debt against the assets. As an example of the latter, in *R (Certain Underwriters at Lloyds) v. HM Treasury*,[173] the claimants sought information from HM Treasury in relation to assets frozen pursuant to sanctions against the Syrian regime as a precursor to applying to HM Treasury for a licence to enforce a US judgment debt against those assets. Looking forward, we anticipate that this interplay between property frozen under sanctions regulations and law enforcement asset recovery measures may also emerge. In April 2022, OFSI issued a general licence permitting officers of non-Crown organisations such as the FCA to carry out their duties in respect of asset recovery measures in relation to assets frozen under the Global Anti-Corruption Sanctions Regulations 2021 and the Russia (Sanctions) (EU Exit) Regulations 2019 (officers of Crown organisations such as the CPS and police forces are already able to do so).[174] Further, while no proposed legislation has been published, in 2022 and 2023 there have been press reports about proposals to introduce measures allowing for confiscation of property frozen under sanctions

---

sanctions regulations were subject to a magistrates' court bank account forfeiture order; David Brown, 'Aniseh Chawkat: Police freeze Assad niece's bank account in London', *The Times*, 22 May 2019, at www.thetimes.co.uk/article/aniseh-chawkat-police-freeze-assadniece-s-bank-account-in-london-5qr07sxpl. See also *R. (on the application of NCA) v. Westminster Magistrates' Court* [2022] EWHC 2631 (Admin), where the NCA had obtained account freezing orders on the basis that there were reasonable grounds to suspect that the funds were intended for use in circumventing sanctions.

172 See, as above, *R. (on the application of NCA) v. Westminster Magistrates' Court*. Another example of the NCA obtaining bank account freezing orders in sanctions investigations is the case of Graham Bonham-Carter, alleged to have received monies linked to Oleg Deripaska, who was designated under the US sanctions regime and later, in March 2022, by the UK; see James Gregory 'UK businessman charged with "helping Russian oligarch evade sanctions"', BBC News Online (11 October 2022), at www.bbc.co.uk/news/uk-63218643 (accessed 17 April 2023).

173 [2021] 1 WLR 387.

174 OFSI General Licence – INT/2022/1679676.

regulations.[175] Canada became the first country to introduce related legislation in June 2022.[176] In the UK, however, the proposal has not yet been taken up in the 'second Economic Crime Bill' before Parliament at the time of writing, and no other concrete plans have been put forward by the government. Various parliamentarians have raised this issue since Russia's invasion of Ukraine.[177] Proponents of reform may ultimately have more success as regards the use or seizure of Russian state assets that are currently frozen in the UK to fund reconstruction in Ukraine rather than more expansive proposals for the seizure of all frozen assets, including those owned by private individuals and companies as well as state assets.[178]

Monitorships

Monitors are independent third parties, generally law firms, risk consultancies or professional service firms, appointed by the court to oversee and report on a company's internal controls and compliance functions following a criminal or regulatory investigation. A monitor may be appointed voluntarily by a company (e.g., to demonstrate cooperation during an investigation) or agreed between the company and the investigating agency as part of a negotiated settlement and

175 See, for example, www.ft.com/content/71a856af-061b-49cc-8c30-7819d2296f96; www.theguardian.com/world/2022/mar/04/property-of-russian-elites-could-be-handed-to-ukrainian-refugees-says-raab.

176 Canadian Special Economic Measures Act 1992, Sections 4(1)(b) and 5.4(1), as amended.

177 The matter was raised in Parliament on 7 March 2022 and 14 March 2023; see https://hansard.parliament.uk/commons/2022-03-07/debates/97B249F2-C666-46EF-B46A-F2FF22DE2264/EconomicCrime(TransparencyAndEnforcement)Bill#contribution-C2AE4ECC-A04E-4AB6-914F-7C01293ED0E6; https://hansard.parliament.uk/commons/2023-03-14/debates/39A33641-F699-4244-B437-C6A2447C68E2/RussianAssetsSeizure (accessed 17 April 2023).

178 A private member's bill has been introduced in Parliament, which, if passed, would require the Secretary of State to make proposals for the seizure of Russian state assets to be used, among other things, in the reconstruction of Ukraine. Its second reading has been scheduled for a date in November when Parliament is not currently scheduled to sit and it is unlikely to pass into law. See Seizure of Russian State Assets and Support for Ukraine Bill (Bill 245, 2022–23), https://bills.parliament.uk/bills/3415/news (accessed 19 May 2023).

presented for court approval.[179] A monitor may also be appointed under the terms of a DPA[180] or as part of a serious crime prevention order (SCPO)[181] or civil recovery order.[182]

Serious crime prevention orders

SCPOs are designed to prevent, restrict or disrupt involvement in serious crime. They may be made in respect of sanctions offences.[183] SCPOs can be made against natural or legal persons and may, among other things, impose restrictions or requirements in relation to financial, property or business dealings or holdings, and require a person to answer questions or provide information.[184] When an SCPO is made against a legal person (usually a company or a partnership), it can include the appointment of an authorised monitor, paid for by that legal person.[185] SCPOs may be imposed for up to five years.[186]

SCPOs can be made by the Crown Court during sentencing[187] or in separate civil proceedings in which a conviction is not a prerequisite, if the court is satisfied that a person has been involved in serious crime, whether in the United Kingdom

179 Following its conviction in 2009 for bribery and breaching United Nations sanctions against Iraq, Mabey & Johnson Ltd was required to instruct an SFO-approved monitor for up to three years, whose costs for the first year were capped at £250,000.

180 The DPA Code addresses the potential appointment of compliance monitors. It states that it is important for a prosecutor to consider whether the organisation already has a 'genuinely proactive and effective corporate compliance programme' and that the use of monitors 'should therefore be approached with care'. Ultimately, the guidance explains: 'The appointment of a monitor will depend upon the factual circumstances of each case and must always be fair, reasonable and proportionate.'

181 Serious Crime Act (SCA) 2007, Section 39.

182 For a detailed guide to monitorships, see https://globalinvestigationsreview.com/guide/the-guide-monitorships/third-edition/article/united-kingdom-ordered-monitorships (accessed 31 May 2021).

183 PCA 2017, Section 151.

184 SCA 2007, Section 5(3)–5(5).

185 id., at Section 39.

186 id., at Section 16(2). See Section 22E for the power to extend orders pending the outcome of criminal proceedings.

187 id., at Section 19.

or elsewhere, and it has reasonable grounds to believe that the order would protect the public by preventing, restricting or disrupting involvement by the person in serious crime in the relevant part of the UK.[188]

SCPO proceedings in both the Crown Court and the High Court are civil proceedings and the civil standard of proof is applied.[189] Breach of an SCPO without reasonable excuse is a criminal offence punishable with imprisonment for a term not exceeding five years or a fine, or both.[190]

Naming and shaming

Prior to 2022, OFSI only publicised the imposition of monetary penalties. Where breaches resulted in other enforcement outcomes, this was not made public. As set out above, following the introduction of the Economic Crime (Transparency and Enforcement) Act 2022, OFSI now has the power to publicly name persons who have been found to be in breach of sanctions but who have not received a civil penalty.[191]

Debarment

A breach of sanctions may result in debarment from tendering for public sector contracts in the UK and elsewhere.[192] In the UK, tendering for public sector contracts is governed by the Public Contracts Regulations 2015, which implement the EU Procurement Directive.[193] Sanctions breaches may result in discretionary debarment.[194]

---

188 id., at Section 1. They can be made by the English High Court, an appropriate court in Scotland or the High Court in Northern Ireland on an application by a specified prosecutor; namely, the DPP or the Director of the SFO in England and Wales, the Lord Advocate in Scotland and the DPP in Northern Ireland (Section 8).

189 SCA 2007, Sections 35 and 36.

190 id., at Section 25.

191 Economic Crime (Transparency and Enforcement) Act 2022, Section 56.

192 See, e.g., *Director of the Serious Fraud Office v. Airbus SE* [2020] 1 WLUK 435 [84].

193 Amendments to the Regulation will come into force following Brexit.

194 Regulation 57 of the Public Contracts Regulations 2015; see also, e.g., *Director of the Serious Fraud Office v. Airbus SE* [2020] 1 WLUK 435 [84].

Directors' disqualification and regulatory measures

Upon conviction for an offence in connection with, inter alia, the promotion or management of a company, the court may make a disqualification order for up to 15 years.[195] Breach of a disqualification order is a criminal offence.[196]

Even without a conviction, a sanctions breach will be relevant to the FCA's and HMRC's assessment of the continuing 'fitness and propriety' of approved persons and may result in withdrawal of approval.[197]

Concluding remarks

This chapter began with a quote from OFSI's director about the central importance of sanctions enforcement to the UK's broader economic crime regime and the aspirations of OFSI to be a 'world leader' in sanctions enforcement. That has not yet transpired. While the legal tools are largely in place, neither OFSI nor HMRC yet has a significant track record of civil enforcement for breaches of financial or trade sanctions, and recent UK prosecutions for sanctions breaches are notable by their absence. We anticipate some change over time and an increase in enforcement actions with a range of disposals. However, for all the rhetoric of, for example, the NCA 'surging' officers into its 'K-Cell', investigations may never result in prosecutions. These investigations may well be complex and time and resource intensive, but the investigative and enforcement agencies remain constrained by capacity, and, as tacitly accepted by the NCA, the purpose of some investigative actions may be more about 'disruption' than prosecution.[198]

---

195 Company Directors Disqualification Act 1986, Section 2.

196 id., at Sections 13 and 14.

197 See section titled 'Anti-money laundering', above. See also FCA, 'Fit and Proper test for Employees and Senior Personnel sourcebook', at www.handbook.fca.org.uk/handbook/FIT.pdf (last accessed 5 May 2021) and HMRC, 'The fit and proper test', at www.gov.uk/government/publications/money-laundering-supervision-fit-and-proper-test-and-approval/money-laundering-supervision-guidance-on-the-fit-and-proper-test-and-hmrc-approval (updated 5 April 2023) (accessed 16 May 2023).

198 Gordon Corera, 'Russian oligarchs: Inside K-Cell – the UK police unit raiding their homes', BBC News Online (27 May 2022), at www.bbc.co.uk/news/uk-61591547 ('Law enforcement normally judges success by prosecutions. But this team's measure is different. Changing behaviour is seen as success as much as an appearance in court.').

CHAPTER 5

US Sanctions

John D Buretta and Megan Y Lew[1]

This chapter surveys US economic and trade sanctions, with a particular focus on the authorities underlying US sanctions and the processes by which the US Department of the Treasury's Office of Foreign Assets Control (OFAC) regulates sanctions and exemptions thereto.

US economic and trade sanctions are long-standing US foreign policy tools directed at specific jurisdictions, such as Cuba, Iran and North Korea, and specific governments, government officials, companies or individuals determined to have acted contrary to US foreign policy and national security objectives, such as with respect to nuclear weapons proliferation or narcotics trafficking.

Authorities for US sanctions

In the ordinary course, Congress passes statutes that authorise the President to promulgate sanctions through executive orders. OFAC then issues and enforces those sanctions regulations as published in the Code of Federal Regulations (CFR). The constitutional authority for these interwoven powers stems from Article II, Section 3 (that the Executive shall 'take Care that the Laws be faithfully executed') and Article I, Section 8 (Congress' legislative power in respect of foreign commerce). The key legislative authorities underpinning US sanctions are the Trading with the Enemy Act (TWEA), the International Emergency Economic Powers Act (IEEPA) and the United Nations Participation Act (UNPA).

---

1 John D Buretta is a partner and Megan Y Lew is of counsel at Cravath, Swaine & Moore LLP. The authors would like to thank William S Janover and Andrea J Xu, previously associates at the firm, for contributing to the chapter.

TWEA

Congress passed TWEA[2] in 1917, at the time of the United States' entry into the first world war, to 'define, regulate, and punish trading with the enemy'. This statute conferred on the President wide-ranging powers to restrict trade between the United States and foreigners or countries considered enemies during wartime. Currently, TWEA remains the underlying legislation only for sanctions against Cuba.

IEEPA

The most common legislative authority the President relies on to impose sanctions today is IEEPA,[3] which Congress passed in 1977 in an effort to demarcate more clearly the President's emergency powers. With IEEPA, the focus shifted from wartime powers under TWEA to address more broadly 'any unusual and extraordinary threat' to US national security, foreign policy or economic stability.[4] Pursuant to IEEPA, the President can declare a national emergency and issue executive orders to address that national emergency by, among other things, freezing the assets of and prohibiting financial transactions with any country, entity or person determined to be a threat to the United States.[5] Typically, the prohibitions found in the executive orders become codified in Title 31, Chapter V of the CFR.

UNPA

Another source of legislative authority for the President to issue economic sanctions is the UNPA,[6] which empowers the President to impose economic sanctions when mandated by the United Nations Security Council pursuant to Article 41 of the UN Charter. Through any agency that they may designate, the President can investigate, regulate and prohibit in whole or in part economic relations between any country or national thereof, and the United States, any US person or any property interest subject to US jurisdiction. Some examples of the President's exercise of power under the UNPA include President Reagan's imposition of sanctions in response to apartheid in South Africa in 1985 and President Clinton's imposition of sanctions prohibiting specific financial transactions with Rwanda in 1994.

---

2 50 United States Code (USC) § 4301 et seq.

3 50 USC § 1701 et seq.

4 See 50 USC §§ 1701, 1702.

5 ibid.

6 22 USC § 287(c).

Other legislation

In addition to the above statutes, Congress has from time to time issued additional legislation with respect to sanctions and foreign policy that either authorises or mandates the President or the US Department of the Treasury to impose certain sanctions. Some examples are the North Korean Sanctions and Policy Enhancement Act of 2016 (NKSPEA),[7] the Countering America's Adversaries Through Sanctions Act (CAATSA),[8] the Sanctioning the Use of Civilians as Defenceless Shields Act (SUCDSA),[9] the Caesar Syria Civilian Protection Act of 2019 (the Caesar Act)[10] and the Protecting Europe's Energy Security Clarification Act (PEESCA).[11] Section 104 of the NKSPEA mandates that the President shall sanction any persons found to, among other things, knowingly directly or indirectly import, export or re-export into North Korea any goods, services or technology relating to nuclear weapons proliferation. Section 104 of CAATSA likewise mandates that the President shall sanction any persons found knowingly to engage in any activity that materially contributes to the activities of the government of Iran with respect to its ballistic missile programme, whereas Section 232 stipulates that the President may impose sanctions on certain persons found to have made specific investments in the Russian Federation. Section 3 of SUCDSA provides for both mandatory and permissive designations of persons found to use civilians to shield military targets from attack, including, but not limited to, members of Hezbollah or Hamas. The Caesar Act requires the President to impose sanctions on any persons found to have, among other things:

- engaged in a significant transaction with the government of Syria;
- provided aircraft or spare aircraft parts for military use to Syria; or
- provided significant construction or engineering services to the government of Syria.

Last, PEESCA, which was passed in January 2021 and amends the Protecting Europe's Energy Security Act of 2019 (PEESA), mandates sanctions for certain conduct that supports the Nord Stream 2 and TurkStream 2 pipeline

7 Public Law 114-122 (18 February 2016), 22 USC § 9201 et seq.
8 Public Law 115-44 (2 August 2017), 22 USC §§ 9401 et seq. and 9501 et seq.
9 Public Law 115-348 (21 December 2018), 132 Stat 5055.
10 Public Law 116-92, §§ 7401–7438 (20 December 2019), 133 Stat. 2291–2300.
11 Public Law 116-283, § 1242 (1 January 2021), 134 Stat. 3945–3947.

construction projects that were planned to transport natural gas from Russia to Europe. In February 2022, after Russia invaded Ukraine, OFAC designated Nord Stream 2 AG and its chief executive officer under PEESA.[12]

Because both Congress and the Executive Branch can issue sanctions, tensions can sometimes arise between these branches of government. It may be that the sanctions prescribed by Congress do not directly align with the Executive Branch's foreign policy goals. At other times, Congress will enact mandatory sanctions or require ongoing congressional review of certain sanctions programmes in the event it believes the Executive Branch has failed to take a sufficiently forceful stance on a particular issue. CAATSA is an example of this kind of tension as it includes mandatory sanctions and a requirement that Congress review any decision from the Executive Branch to lift certain sanctions against Russia.[13] Although President Trump signed CAATSA into law, he also issued a statement expressing his view that ongoing congressional review of the sanctions against Russia was unconstitutional, but that he expected to honour the statute's requirements.[14]

Design and implementation

The key motivation for US economic and trade sanctions is to impose economic pressure on specific governments, companies or individuals for acting in contravention of US foreign policy and national security objectives. US sanctions in effect cut off sanctioned jurisdictions and sanctioned persons from accessing US dollars and the US financial system, which can have significant repercussions.

12 See US Dep't of the Treasury's Office of Foreign Assets Control (OFAC), 'PEESA Designations' (23 February 2022), at https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220223_33; The White House, 'Statement by President Biden on Nord Stream 2' (23 February 2022) at www.whitehouse.gov/briefing-room/statements-releases/2022/02/23/statement-by-president-biden-on-nord-stream-2/; Dep't of State, 'Sanctioning NS2AG, Matthias Warnig, and NS2AG's Corporate Officers' (23 February 2022) at www.state.gov/sanctioning-ns2ag-matthias-warnig-and-ns2ags-corporate-officers/.

13 See 22 USC § 9511; Countering America's Adversaries Through Sanctions Act (CAATSA) § 231, 22 USC § 9525 (against persons found to have knowingly operated for or on behalf of the defence or intelligence sectors of the government of the Russian Federation); see also Benjamin Alter, 'Sanctions Are Congress's Path Back to Foreign Policy Relevance', *Lawfare* (27 March 2018), at www.lawfareblog.com/sanctions-are-congresss-path-back-foreign-policy-relevance; Jordan Tama, 'So Congress is challenging the president about sanctions? That has a long history', *Washington Post* (16 June 2017), at www.washingtonpost.com/news/monkey-cage/wp/2017/06/16/so-congress-is-challenging-the-president-about-sanctions-that-has-a-long-history/.

14 'Statement by President Donald J. Trump on the Signing of H.R. 3364' (2 August 2017).

Given that foreign policy and national security objectives have changed over time and financial transactions have grown in complexity, US sanctions have evolved from more broad embargoes to more targeted sanctions programmes.

There are three basic types of US sanctions: comprehensive embargoes against countries or regions, list-based asset-blocking sanctions and non-blocking sanctions. OFAC currently maintains comprehensive embargoes against Cuba, Iran, North Korea, Syria and the Crimea and so-called 'Donetsk People's Republic' and 'Luhansk People's Republic' regions of Ukraine.[15] These embargoes generally prohibit dealings by US persons with these jurisdictions, including financial transactions, exports and imports. Interestingly, Venezuela is an example of a jurisdiction in which the government, members of the government and persons acting on behalf of the government are subject to blocking sanctions but the country has not been targeted by a comprehensive embargo.[16]

OFAC's list-based sanctions consist of numerous different lists, designating as sanctioned specific governments, government entities, government officials, companies, individuals or property such as vessels, aircraft and digital currency addresses. In 2022, for the first time, OFAC designated two virtual currency mixers.[17] Designated parties and property are included on the Specially Designated Nationals (SDNs) and Blocked Persons List or the Specially Designated Global Terrorist (SDGT) List, which are collectively referred to in this chapter, for simplicity, as the SDN List. Persons or property on the SDN List are subject to asset-blocking sanctions. US persons are prohibited from directly or indirectly dealing with anyone on the SDN List or their property, and all assets and property interests subject to US jurisdiction, whether tangible or intangible, direct or indirect, are frozen.

OFAC maintains several types of 'non-blocking' sanctions that implement targeted forms of sanctions against certain persons or transactions that are less restrictive than asset-blocking sanctions. Many of OFAC's non-blocking sanctions are list based and persons subject to these sanctions programmes are

15 31 Code of Federal Regulations (CFR) Parts 510 (North Korea), 515 (Cuba), 560 (Iran), 569 (Syria), 589 (Crimea); Executive Order 14065 (21 February 2022) (so called 'Donetsk People's Republic' and 'Luhansk People's Republic' regions of Ukraine).

16 Executive Order 13884 (5 August 2019).

17 US Dep't of Treasury, 'U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats' (6 May 2022), at https://home.treasury.gov/news/press-releases/jy0768; US Dep't of Treasury, 'U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash' (8 August 2022), at https://home.treasury.gov/news/press-releases/jy0916.

identified on separate lists maintained by OFAC, where the scope of the restrictions depends upon the legal authority implementing the sanctions. OFAC has discretion to designate a person to one or more asset-blocking or non-blocking sanctions lists if the applicable designation criteria are met. In other words, the lists are not mutually exclusive, and a person may be found on more than one list.

A few examples of OFAC's non-blocking sanctions lists are given below.

- Non-SDN Chinese Military-Industrial Complex Companies List (the NS-CMIC List): in November 2020, the United States announced a ban on transactions involving publicly traded securities, or derivatives of any of these securities, and of Chinese military companies by US persons.[18] The NS-CMIC List identifies the companies that are subject to this prohibition.[19]
- Non-SDN Menu-Based Sanctions List (the NS-MBS List): the NS-MBS List includes persons who are subject to targeted, non-blocking sanctions selected from a 'menu' of options. The menu of sanctions options includes prohibitions on: obtaining assistance from the Export-Import Bank of the United States, obtaining export licences from other US government agencies, obtaining loans from US financial institutions, entering into procurement contracts with the US government and engaging in transactions with US persons involving the debt or equity of the sanctioned person.[20] The exact prohibitions applicable to each person on the NS-MBS List are described in the list. Dozens of persons were added to the NS-MBS List in February and March 2022, as a result of Russia's invasion of Ukraine.[21]

18 Executive Order 13959 (12 November 2020).

19 US Dep't of Treasury, 'Non-SDN Chinese Military–Industrial Complex Companies List (NS-CMIC List)' (last updated 16 December 2021), at https://ofac.treasury.gov/consolidated-sanctions-list/ns-cmic-list.

20 US Dep't of Treasury, 'Non-SDN Menu-Based Sanctions List (NS-MBS List)' (last updated 24 February 2023), at https://ofac.treasury.gov/consolidated-sanctions-list-non-sdn-lists/non-sdn-menu-based-sanctions-list-ns-mbs-list. The 'menu' of sanctions is derived from several statutory authorities, including Section 235 of CAATSA. Pub. L. 115-44, 131 Stat. 886, 919 (2 August 2017); 22 US Code (USC) § 9529.

21 See, e.g., Press Release, US Dep't of Treasury, 'U.S. Treasury Announces Unprecedented & Expansive Sanctions Against Russia, Imposing Swift and Severe Economic Costs' (24 February 2022), https://home.treasury.gov/news/press-releases/jy0608.

- Foreign Sanctions Evaders List (the FSE List): the FSE List identifies non-US persons who have 'violated, attempted to violate, conspired to violate, or caused a violation of' certain sanctions against Syria or Iran.[22] In addition, the FSE List includes non-US persons who have 'facilitated deceptive transactions for or on behalf of persons subject to US sanctions'.[23] Persons on the FSE List are prohibited from engaging in transactions with US persons or within the United States.[24]
- List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions (the CAPTA List): the CAPTA List identifies non-US financial institutions that face restrictions on having a correspondent account or payable-through account in the United States.[25] Non-US financial institutions that are on the CAPTA List have been designated under sanctions authorities targeting North Korea, Iran, Russia and Hezbollah.[26]
- Sectoral Sanctions Identifications List (the SSI List): sectoral sanctions have been used by OFAC to impose limited sanctions on certain sectors of a country's economy. Sectoral sanctions were first developed in response to Russia's annexation of Crimea in 2014 and those sanctions take the form of four directives, each bearing its own prohibitions. Three of the four directives prohibit designated entities operating in the 'financial services, energy, metals and mining, engineering, defence and related materiel' sectors of the Russian economy from raising equity or debt of certain tenures in the United States or involving US persons. The fourth directive prohibits designated entities from engaging in oil exploration or production for deepwater, Arctic offshore or shale projects that involve US persons.[27] Entities subject to these sanctions are designated under one or more of the four directives and can be

22 US Dep't of Treasury, 'Foreign Sanctions Evaders (FSE) List' (last updated 12 December 2022), https://ofac.treasury.gov/consolidated-sanctions-list-non-sdn-lists/foreign-sanctions-evaders-fse-list.

23 ibid.

24 ibid.

25 US Dep't of Treasury, 'List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions (CAPTA List)' (last updated 6 April 2022) at https://ofac.treasury.gov/consolidated-sanctions-list-non-sdn-lists/list-of-foreign-financial-institutions-subject-to-correspondent-account-or-payable-through-account-sanctions-capta-list.

26 ibid.

27 Executive Order 13662 (20 March 2014); see also OFAC, 'Ukraine/Russia-Related Sanctions Program' (last updated 16 June 2016), at https://ofac.treasury.gov/media/8741/download?inline.

found on OFAC's SSI List.[28] Sectoral sanctions have also been used in the Venezuela sanctions programme by prohibiting US persons from engaging in transactions involving certain debt issued by the government of Venezuela or state-owned entities.[29]

In 2022, the US government implemented stricter and more complex sanctions to address Russia's invasion of Ukraine. These include traditional forms of sanctions, such as embargoes against areas in Ukraine that Russia purportedly recognised as 'independent',[30] the addition of hundreds of Russian persons to the SDN List[31] and the imposition of export and import bans on certain types of goods.[32] Non-blocking sanctions – separate from the list-based non-blocking sanctions discussed above – have also been widely used, ranging from prohibiting certain Russian banks from processing payments using US financial institutions to restricting US persons' ability to engage in transactions with the Central Bank of Russia.[33] Other forms of non-blocking sanctions involving Russia include prohibiting new investment in Russia[34] and the provision of accounting, trust and corporate formation and management consulting services to any person in Russia.[35] In addition, in late 2022, the US, European Union and members of the G7 coordinated the implementation of non-blocking sanctions that seek to reduce Russia's oil revenues. Known colloquially as a 'price cap' on Russian oil, these sanctions prohibit the maritime transport of Russian oil that had been

28 Although OFAC's Specially Designated Nationals and Blocked Persons List and Specially Designated Global Terrorist List and Sectoral Sanctions Identifications List (the SSI List) serve different purposes, certain persons are on both lists.

29 Executive Order 13808 (24 August 2017).

30 Executive Order 14065 (21 February 2022).

31 See, e.g., Press Releases, US Dep't of Treasury, 'U.S. Treasury Announces Unprecedented & Expansive Sanctions Against Russia, Imposing Swift and Severe Economic Costs' (24 February 2022), https://home.treasury.gov/news/press-releases/jy0608; 'Treasury Sanctions Kremlin Elites, Leaders, Oligarchs, and Family for Enabling Putin's War Against Ukraine' (11 March 2022), https://home.treasury.gov/news/press-releases/jy0650; and 'U.S. Treasury Sanctions Russia's Defense-Industrial Base, the Russian Duma and Its Members, and Sberbank CEO' (24 March 2022), https://home.treasury.gov/news/press-releases/jy0677.

32 Executive Order 14068 (11 March 2022).

33 Directive 2 to Executive Order 14024 (24 February 2022); Directive 4 to Executive Order 14024 (28 February 2022).

34 Executive Order 14071 (6 April 2022).

35 Determination Pursuant to Section 1(a)(ii) of Executive Order 14071, Prohibitions Related to Certain Accounting, Trust and Corporate Formation, and Management Consulting Services (8 May 2022).

sold above a price cap set by the G7.[36] In February 2023, these sanctions were expanded to other petroleum products of Russian origin.[37] As a result of such wide ranging non-blocking sanctions, any transactions with or involving Russian parties requires careful assessment that goes beyond screening against sanctions lists maintained by OFAC.

In addition, traditional and non-traditional forms of sanctions have been used to address national security concerns arising from the potential risk that the Chinese government could use social media apps owned by Chinese companies to collect personal information about users. Relying on IEEPA and related national security authorities, President Trump issued a series of executive orders in August 2020 that prohibited US persons from transacting with ByteDance Ltd[38] (owner of TikTok Inc, a video-sharing app) and Tencent Holdings[39] (owner of WeChat, a messaging, social media and payment app) and required the sale of TikTok Inc to a US company.[40] However, the executive orders have been challenged in US federal courts, and judges presiding over those cases issued orders temporarily enjoining their implementation.[41] After initially requesting to stay those cases to re-evaluate the executive orders,[42] the Biden administration rescinded the executive orders

36 Determination Pursuant to Sections 1(a)(ii) of Executive Order 14071, Prohibitions on Certain Services as They Relate to the Maritime Transport of Crude Oil of Russian Federation Origin (5 December 2022); Determination Pursuant to Sections 1(a)(ii), 1(b), and 5 of Executive Order 14071, Price Cap on Crude Oil of Russian Federation Origin (5 December 2022).

37 Determination Pursuant to Sections 1(a)(ii) of Executive Order 14071, Prohibitions on Certain Services as They Relate to the Maritime Transport of Petroleum Products of Russian Federation Origin (5 February 2023); Determination Pursuant to Sections 1(a)(ii), 1(b), and 5 of Executive Order 14071, Price Cap on Petroleum Products of Russian Federation Origin (5 February 2023).

38 Executive Order 13942 (6 August 2020).

39 Executive Order 13943 (6 August 2020) (prohibiting transactions with Tencent Holdings that relate to WeChat).

40 Executive Order of 14 August 2020, 85 Fed Reg 51297 (19 August 2020).

41 Order, *TikTok Inc. v. Trump*, 20-cv-2658 (CJN) (DDC 27 September 2020); Order, *TikTok Inc. v. Trump*, 20-cv-2658 (CJN) (DDC 7 December 2020); Order Granting Motion for Preliminary Injunction, *U.S. WeChat Users Alliance v. Trump*, 20-cv-5910-LB (ND Cal 19 September 2020); Order, *U.S. WeChat Users Alliance v. Trump*, 20-16908 (9th Cir. 26 October 2020).

42 See Joint Status Report, *U.S. WeChat Users Alliance v. Biden*, 20-cv-5910-LB (ND Cal 12 April 2021); Joint Status Report, *TikTok Inc. v. Biden*, 20-cv-2658 (CJN) (DDC 12 April 2021).

on 9 June 2021.[43] The following month, the district court granted ByteDance's motions to voluntarily dismiss the case.[44] In October 2021, the *Tencent* case was dismissed based on a joint stipulation from the parties.[45]

Designation process

Required information

In undertaking an investigation as to whether to designate a person or entity, OFAC relies on information and intelligence compiled from US government agencies, foreign governments, UN expert panels, press and open source reporting.[46] OFAC's investigators review the totality of information available, documenting their findings and conclusions in a memorandum describing the evidence to support designation under relevant sanctions authority.[47] Before OFAC makes a final determination on designation, proposed listings are subject to inter-agency review by the US Departments of the Treasury, Justice, State 'and other US agencies as warranted'.[48] Additionally, OFAC will use the criteria in presidential executive orders or congressional statutes to impose designations.

The US Department of State may also issue sanctions designations under authorities focused on terrorism, proliferation activities, Iran and Russia. OFAC implements the sanctions restrictions associated with the Department of State's designations.[49]

---

43 Executive Order 14034 (9 June 2021) (rescinding Executive Orders 13942, 13943 and 13971).

44 Order, *Tiktok v. Trump*, 20-cv-2658 (CJN) (DDC 20 July 2021).

45 Stipulation of Dismissal, *U.S. WeChat Users Alliance v. Trump*, 20-cv-5910-LB (ND Cal 20 October 2021).

46 US Dep't of Treasury, 'Filing a Petition for Removal from an OFAC List', at https://ofac.treasury.gov/specially-designated-nationals-list-sdn-list/filing-a-petition-for-removal-from-an-ofac-list.

47 ibid.

48 ibid.

49 See, e.g., Exec. Order 13949 (21 September 2020) (authorising the US Department of State to identify sanctions targets who engaged in arms transactions with Iran); Executive Order 13382 (28 June 2005) (authorising the US Department of State to identify sanctions targets who engaged in activities relating to proliferation of weapons of mass destruction).

Challenging designations or delisting

A designated entity or individual can petition for removal from any OFAC sanctions list by sending either hard copy or electronic applications to OFAC.[50] Per OFAC's guidance, petitions for removal should include the listed person's name and the contact person's name and mailing address, the date of the relevant listing action and a request for reconsideration of OFAC's determination, accompanied by a detailed description of why the listing should be removed.[51]

Petitioners may submit additional information to OFAC, including evidence that an insufficient basis exists for designation or that there has been a change in circumstances rendering the designation moot. Specifically, 31 CFR Section 501.807 codifies procedures for delisting persons, and OFAC has included the following as examples of sufficient grounds for removal:

- a positive change in behaviour;
- the death of an SDN;
- the basis for designation no longer exists; or
- the designation was based on mistaken identity.

Section 501.807 provides the opportunity for a designated entity or individual to affirmatively propose remedial actions – such as corporate reorganisation – to negate the designation. For example, this was successfully done in the case of En+ Group plc, UC Rusal plc and JSC EuroSibEnergo, three corporate entities that were designated in April 2018 because they were indirectly owned by Oleg Deripaska, who was designated for operating in the energy sector of the Russian economy and acting on behalf of senior officials in the Russian government.[52] After lengthy negotiations with OFAC, these three entities were delisted in January 2019 as a result of Deripaska's agreement to sell his majority stake in those entities and relinquish control over them.[53] Deripaska remained on the SDN

50 Petitions can be made out to: Office of Foreign Assets Control, Office of the Director, US Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220; or to OFAC.Reconsideration@treasury.gov.

51 US Dep't of Treasury, 'Filing a Petition for Removal from an OFAC List' (footnote 46).

52 Press Release, US Dep't of Treasury, 'Treasury Designates Russian Oligarchs, Officials, and Entities in Response to Worldwide Malign Activity' (6 April 2018), at https://home.treasury.gov/news/press-releases/sm0338.

53 Press Release, US Dep't of Treasury, 'OFAC Delists En+, Rusal, and EuroSibEnergo' (27 January 2019), at https://home.treasury.gov/news/press-releases/sm592.

List, but the three entities were removed because there was no longer a basis for their designations given the corporate restructuring and dilution of Deripaska's shareholding stake in each.[54]

There is no set amount of time established for the delisting process to be concluded. Typically, the process takes months, if not years, and requires designated parties to complete multiple questionnaires and provide extensive documentary evidence.

In the event that a petition for removal fails, judicial review of OFAC's determination is available under the Administrative Procedure Act (APA). Although a US district court's review would be highly deferential to OFAC, reversal is possible if the court finds that a designation was arbitrary, capricious, an abuse of discretion or otherwise not in accordance with the law. For example, grounds for removal of a designation can include a failure by OFAC to provide timely or sufficient notice of its rationale or evidence. In *Al Haramain Islamic Foundation, Inc v. US Department of the Treasury*,[55] the US Court of Appeals for the Ninth Circuit found that the petitioner's due process rights had been violated when OFAC had failed to mitigate the petitioner's inability to review classified information underlying the designation at issue. However, the Court ultimately ruled that the due process violations were harmless in light of the whole record, and the petitioner remained designated.[56] It is rare for designated persons to file lawsuits against OFAC challenging their designation. In recent years, however, several Russian individuals on the SDN List have done so. For instance, Deripaska, who was designated for operating in the energy sector of the Russian economy and acting on behalf of senior officials of the Russian government, filed suit against the US Department of the Treasury and OFAC after his designation in April 2018. In June 2021, the US District Court for the District of Columbia dismissed Deripaska's suit, concluding that OFAC's decision to designate him, and its decision not to delist him, did not violate the APA.[57] Deripaska appealed the District Court's ruling to the US Court of Appeals for the District of Columbia, which upheld the dismissal on 29 March 2022.[58]

54 ibid.

55 686 F.3d 965, 984 (9th Cir. 2011).

56 id., at 990.

57 *Deripaska v. Yellen*, No. 1:19-cv-00727-APM, 2021 WL 2417425 (DDC 13 June 2021).

58 *Deripaska v. Yellen*, No. 21-5157, 2022 WL 986220 (DC Cir. 29 March 2022), cert denied, 143 S. Ct. 117 (3 October 2022).

Application of sanctions

Entities subject to sanctions measures

OFAC issued guidance on 14 February 2008 that any property or interests in property of an entity[59] are blocked if the entity is 50 per cent or more owned, directly or indirectly, by a designated person. This is known as the 50 Percent Rule.

On 13 August 2014, OFAC issued further detailed guidance about the 50 Percent Rule. Designated persons are considered to have an interest in all property and interests in property of an entity in which the designated person owns, whether individually or in the aggregate, directly or indirectly, a 50 per cent or greater interest. The significance of this is that any entity directly or indirectly owned individually or in the aggregate 50 per cent or more by one or more designated persons is itself considered designated. This is the case whether or not the designated entity is actually placed on the SDN List.

Because OFAC applies the 50 Percent Rule to entities owned indirectly by a designated person, the Rule has a cascading effect of designation and may reach entities several levels removed from the designated person. For instance, if designated Person A owns in aggregate 50 per cent or more of Company X, Company X owns in aggregate 50 per cent or more of Company Y and Company Y owns in aggregate 50 per cent or more of Company Z, companies X, Y and Z are each considered designated by virtue of Person A's indirect ownership of each.[60]

As for entities that are controlled but not 50 per cent owned by an SDN, the analysis is more complicated; if an SDN controls another entity, that entity is not presumptively an SDN according to the 50 Percent Rule.[61] Rather, OFAC cautions that it may designate these types of entities pursuant to statutes or executive orders that empower OFAC to do so for entities over which a blocked person exercises control.[62] OFAC further cautions that SDN-controlled entities may be the subject of future OFAC enforcement actions, and advises that persons exercise caution when dealing with non-blocked persons who are controlled by blocked persons. In addition, OFAC prohibits dealings with blocked persons who

---

59 This was subsequently broadly defined to include any direct or indirect property or interest in property, tangible or intangible, including present, future or contingent interests. See US Dep't of Treasury, 'Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property are Blocked' (13 August 2014), at https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20140813.

60 For additional ownership examples, see OFAC FAQ 401 (last updated 13 August 2014), at https://ofac.treasury.gov/faqs/401.

61 OFAC FAQ 398 (last updated 11 August 2020), at https://ofac.treasury.gov/faqs/398.

62 ibid.

conduct business on behalf of non-blocked entities. For example, because OFAC sanctions generally prohibit direct or indirect dealings with blocked persons, a US person may not enter into a contract signed by a blocked person – even on behalf of a non-blocked entity.[63]

The 50 Percent Rule applies to persons on the SSI List,[64] but generally does not apply to other persons who are subject to non-blocking sanctions, such as those persons identified on the NS-MBS List or the NS-CMIC List.[65] OFAC may also carve out certain sanctions programmes from the 50 Percent Rule, which it did in the context of certain sanctions authorised in September 2021 in relation to the humanitarian and human rights crisis in Ethiopia[66] and sanctions against Alisher Usmanov, a Russian oligarch, in March 2022.[67] The licence related to entities owned by Usmanov was rescinded on 12 April 2023.[68]

Application to non-US persons

Under the sanctions regulations, US persons must comply with sanctions that prohibit transactions with sanctioned countries or sanctioned persons. Known as 'primary sanctions', these apply to US persons, defined to include all US citizens and permanent resident aliens wherever located, all persons and entities within the United States, and all US-incorporated entities and their foreign branches.[69] Foreign subsidiaries owned or controlled by US companies are not required to

63 ibid.

64 When applying the 50 Percent Rule to persons on the SSI List, ownership interests are aggregated for each directive to determine whether an entity is subject to a particular directive. However, ownership interests are not aggregated across directives.

65 OFAC FAQ 869 (last updated 5 January 2021), at https://ofac.treasury.gov/faqs/869; OFAC FAQ 857 (last updated 3 June 2021), at https://ofac.treasury.gov/faqs/857; see also OFAC FAQ 943 (last updated 2 December 2021) at https://ofac.treasury.gov/faqs/943 (explaining that the 50 Percent Rule does not apply to certain non-blocking sanctions against certain government entities in Belarus).

66 OFAC FAQ 923 (last updated 17 September 2021), at https://ofac.treasury.gov/faqs/923.

67 See US Dep't of Treasury, 'Treasury Sanctions Russians Bankrolling Putin and Russia-Backed Influence Actors' (3 March 2022), at https://home.treasury.gov/news/press-releases/jy0628.

68 US Dep't of Treasury, 'Treasury Targets Russian Financial Facilitators and Sanctions Evaders Around the World' (12 April 2023), at https://home.treasury.gov/news/press-releases/jy1402.

69 See, e.g., 31 CFR §§ 536.201, 536.316. See also OFAC FAQ 11 (last updated 15 January 2015), at https://ofac.treasury.gov/faqs/11. For indicia of control, OFAC looks to whether a US person holds an equity interest of 50 per cent or more by vote or value in the entity, holds a majority of seats on the board of directors of the entity or otherwise controls the actions or policies or the entity.

comply with primary sanctions, except in relation to the sanctions programmes for Cuba and Iran, and those applicable to financial institutions in relation to North Korea sanctions.[70]

IEEPA and the sanctions regulations also prohibit activities that 'cause' a violation of sanctions.[71] While both US and non-US persons may face liability under a causing theory, most enforcement actions relying on this theory have been brought against non-US persons. Thus, even if a non-US person is not directly prohibited from engaging in sanctioned conduct, that person could be exposed to primary sanctions liability for engaging in transactions with a sanctioned country or a sanctioned person that causes a US person to violate primary sanctions. This theory has been used frequently to prosecute non-US financial institutions that processed US-dollar-denominated transactions through US banks for the benefit of a sanctioned person, thereby causing the US banks (i.e., US persons) to violate sanctions by exporting financial services from the United States to a sanctioned person or jurisdiction.[72] Non-US financial institutions have faced OFAC enforcement actions under these circumstances even when they were not aware that the US-dollar-denominated transactions were transiting through the US financial system.[73]

By contrast, secondary sanctions directly apply to non-US persons and allow the US Department of the Treasury to designate non-US persons for certain types of behaviour depending on the sanctions programme, even in the absence of a US nexus to the activity. Non-US entities should be aware of the secondary sanctions that might apply to their business activities. If any do apply and OFAC

---

70 31 CFR §§ 560.204, 560.215, 560.314 (Iran); 31 CFR § 515.329 (Cuba); 31 CFR § 510.214 (North Korea).

71 See, e.g., 50 USC § 1705(a) (under the International Emergency Economic Powers Act, '[i]t shall be unlawful for a person to . . . cause a violation of any . . . prohibition issued under this chapter'); 31 CFR § 510.212.

72 For example, in 2019, Standard Chartered Bank and UniCredit Bank AG, both non-US banks, resolved civil and criminal charges that were brought under a theory of causing liability. See Press Release, US Dep't of Justice, 'UniCredit Bank AG Agrees to Plead Guilty for Illegally Processing Transactions in Violation of Iranian Sanctions' (15 April 2019), at www.justice.gov/opa/pr/unicredit-bank-ag-agrees-plead-guilty-illegally-processing-transactions-violation-iranian; Press Release, US Dep't of Justice, 'Standard Chartered Bank Admits to Illegally Processing Transactions in Violation of Iranian Sanctions and Agrees to Pay More than $1 Billion' (9 April 2019), at www.justice.gov/opa/pr/standard-chartered-bank-admits-illegally-processing-transactions-violation-iranian-sanctions.

73 See US Dep't of Treasury, 'Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and British Arab Commercial Bank plc' (17 September 2019), at https://ofac.treasury.gov/recent-actions/20190917_33.

imposes sanctions, the designated non-US entity would effectively be cut off from the US financial system, with a deleterious economic and reputational impact for that entity. Last, even if a designated entity does not want to access the US financial system, many non-US banks maintain their own sanctions policies barring dealings with SDNs.

Exemptions

The statutory framework that gives rise to US sanctions includes a number of exempted activities, which, by definition, fall outside the scope of the regulations. For example, IEEPA contains exceptions for humanitarian activities such as donating food, clothing and medicine to relieve human suffering; the import and export of informational materials and communications; and postal, telegraphic, telephonic or other personal communication that does not involve a transfer of anything of value.[74] These statutory exceptions are typically reflected in exemptions implemented by OFAC in its sanctions regulations. The Iranian Transactions and Sanctions Regulations, for instance, contain specific exemptions for all the activities exempted under IEEPA.[75]

OFAC has provided further guidance regarding authorised humanitarian activities in connection to the covid-19 pandemic, specifically in relation to its Iran, Venezuela, North Korea, Syria, Cuba and Ukraine/Russia sanctions programmes.[76] While most medicine and medical devices (including certain personal protective equipment) used for covid-19-related treatment are already exempted under IEEPA's humanitarian aid exception, other items (such as oxygen generators and certain decontamination equipment) require a specific licence for individuals and entities to provide to sanctioned countries. To help combat the spread of covid-19, OFAC issued three general licences in June 2021, which were amended in June 2022, 'to provide authorizations for certain covid-19-related transactions and activities' involving Iran, Syria and Venezuela.[77] Generally, these licences authorise the exportation or sale of goods 'related to the prevention, diagnosis, or treatment of covid-19 (including research or clinical studies relating to covid-19)' to Iran, Syria or the government of Venezuela, as well as any related

74 50 USC § 1702(b).

75 See, e.g., 31 CFR § 560.210.

76 OFAC, 'Fact Sheet: Provision of Humanitarian Assistance and Trade to Combat COVID-19' (16 April 2020, updated 16 June 2022), at https://ofac.treasury.gov/media/35851/download?inline.

77 ibid.

financial transactions.[78] OFAC has also sought to ensure that sanctions do not impede the provision of humanitarian assistance in the wake of earthquakes and other natural disasters impacting sanctioned countries. For example, after the earthquake in Turkey and Syria in February 2023, OFAC issued a general licence authorising 'all transactions related to earthquake relief efforts in Syria'.[79]

Despite many commonalities of the exemptions discussed above, there are some differences across the sanctions programmes that stem from the policy objectives that the sanctions are intended to advance, as opposed to any differences in the authority granted by legislation or regulations underlying the sanctions programmes. For example, the goal of the Syria sanctions is to 'disrupt the Assad regime's ability to finance its campaign of violence against the Syrian people'.[80] With this goal in mind, OFAC has prohibited transactions that have the potential to fund the Assad regime, while still permitting personal remittances and donations of humanitarian goods.

In contrast, the animating concerns behind SDGT-based sanctions dictate exemptions that are more narrowly drawn. For example, Executive Order 13224, issued in the wake of the September 11 terror attacks and which identified persons who posed a threat to US national security, does not permit as expansive humanitarian activities, and prohibits donations of the kind otherwise permitted by IEEPA, on the grounds that the donations would seriously impair the President's 'ability to deal with the national emergency declared in this order, and would endanger Armed Forces'.[81]

Licensing

Types of licences

Apart from statutory exceptions and regulatory exemptions, other activities may be authorised by OFAC, which has the authority to issue general and specific licences.

78 See General License No. 21A (10 June 2022), at https://ofac.treasury.gov/media/923686/download?inline; General License No. 39A (10 June 2022), at https://ofac.treasury.gov/media/923691/download?inline; General License N-1 (10 June 2022) at https://ofac.treasury.gov/media/923681/download?inline.

79 General License No. 23 (9 February 2023), at https://ofac.treasury.gov/media/931106/download?inline.

80 OFAC FAQ 225, at https://ofac.treasury.gov/faqs/225.

81 Executive Order 13224 (23 September 2001).

General licences authorise a class of persons subject to OFAC's jurisdiction to engage in categories of activities that would otherwise be prohibited by the applicable sanctions programme.[82] Under general licensing programmes, there is no need to apply for an authorisation case by case.[83] General licences for different sanctions programmes can be found in the CFR[84] or as separate guidance documents on OFAC's website. Common examples of general licences include the provision of legal services, financial institutions debiting blocked accounts for normal service charges owed by the account owner and, in certain cases, companies winding down their businesses with sanctioned persons after newly imposed or expanded sanctions. Persons who rely on general licences may be required to file reports and statements with OFAC in accordance with the instructions specified in those licences, and failure to do so may nullify the authorisation and result in an enforcement action by OFAC.[85]

Specific licences are issued case by case, normally by OFAC, but on occasion by the Secretary of Treasury directly.[86] They authorise a specific person to conduct a certain transaction or set of transactions that would otherwise be prohibited by a sanctions programme.[87] Examples include the release of blocked funds, receipt of payment for legal services using blocked funds, or exportation of medical devices or agricultural commodities that are not otherwise exempted or covered by a general licence. A specific licence is typically granted for a set period; however, an applicant may seek a licence renewal. Last, similar to certain general licences, specific licence grantees may be required to send reports and statements to OFAC.[88]

The application process

A person or entity seeking to obtain a specific licence may file an application via OFAC's website. Applicants should provide as much detail as possible about the transaction for which a licence is being sought, including the names and addresses of all parties involved or interested in the transaction, the applicant's taxpayer identification number and any other information deemed necessary by OFAC per

82 OFAC FAQ 74 (last updated 16 June 2016), at https://ofac.treasury.gov/faqs/74.
83 Prosecutions for Violations of U.S. Export Controls and Trade Sanctions, § 16:2.1[E], White Collar Issues Deskbook (November 2019).
84 31 CFR Chapter V.
85 31 CFR § 501.801(a).
86 31 CFR § 501.801(b)(3).
87 31 CFR § 501.801(b).
88 31 CFR § 501.801(b)(4).

the specific sanctions programme.[89] Upon review of the application and possible inter-agency consultation,[90] OFAC may request additional information or documentation and the process may take several weeks to more than a year, depending on the volume of applications and the complexity of the transaction involved.

Refusal to grant a licence

A denial by OFAC of a licence application constitutes final agency action and there is no formal process of administrative appeal.[91] OFAC's regulations, however, do not preclude the reconsideration of an application or the filing of a further application, should there be new facts or changed circumstances that warrant a review.[92]

Nonetheless, parties can rely on the APA and seek judicial review of OFAC's licensing determination where, for instance, the determination is claimed to be arbitrary, capricious or contrary to law. However, in conducting their review, US courts typically defer to the agency's decision,[93] provided that there is a rational basis for it.[94] When it comes to decisions based on foreign policy, courts exercise an even higher degree of deference.[95] To date, courts have, at most, remanded cases to OFAC and directed it to consider certain legal and regulatory aspects, but have not made a determination on whether to require OFAC to grant a specific licence.[96]

Legal services licensing

OFAC has long noted its 'willingness to remove persons from the SDN List consistent with the law' and its goal to 'bring about a positive change in behaviour'.[97] To achieve these goals, OFAC has issued general licences allowing

89 OFAC FAQ 75 (last updated 8 October 2013), at https://ofac.treasury.gov/faqs/75.

90 OFAC FAQ 58 (last updated 10 September 2002), at https://ofac.treasury.gov/faqs/58.

91 OFAC FAQ 76 (last updated 10 September 2002), at https://ofac.treasury.gov/faqs/76.

92 31 CFR § 501.801(b)(5).

93 See *Citizens to Preserve Overton Park v. Volpe*, 401 U.S. 416 (1971).

94 See *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 42–43 (1983).

95 See *Regan v. Wald*, 468 U.S. 222, 242 (1984) ('Matters relating "to the conduct of foreign relations . . . are so exclusively entrusted to the political branches of government as to be largely immune from judicial inquiry or inference"') (citation omitted); see also *Walsh v. Brady*, 729 F.Supp. 118, 120 (DDC 1989) ('However, it is obviously not this Court's function to usurp the authority of the Secretary in this area [granting a licence or not]').

96 See *Pac. Solar Energy, S.A. de C.V. v. U.S. Dep't of the Treasury*, Civil Action No. 18-48 (RDM) (DDC 26 March 2019); see also *World Fuel Corp. v. Geithner*, 568 F.3d 1345 (11th Cir. 2009).

97 US Dep't of Treasury, Filing a Petition for Removal from an OFAC List (footnote 46).

SDNs to obtain legal services that would enable them to navigate the idiosyncrasies of each sanctions programme and obtain, for instance, legal representation related to the challenging of a designation.[98] The licences for the provision of legal services, however, do not automatically entail an authorisation for the payment of those services with blocked funds. Payment for legal services with blocked funds is highly dependent on the rules of each sanctions programme and the nationality of the SDN seeking counsel, but must rely on either a general or a specific licence.

OFAC's general licences allowing the provision of legal services often contain an authorisation for the SDNs to pay for legal services using funds located outside the United States. This authorisation is accompanied by certain reporting requirements to OFAC by the US person providing the services and receiving payment.[99] The funds used for payment must not originate from the United States or from any entity, wherever located, that is controlled by a US person. In addition to these requirements, OFAC's general licences also typically allow a third party to make the payment on behalf of the SDN seeking legal services, provided that the funds used are not blocked by any sanctions.[100] In the absence of a general licence authorising payment of legal services, or if the general licence is inapplicable in a given set of circumstances, the US counsel providing legal services must obtain a specific licence to receive payment.[101]

With regard to providing legal representation for blocked US persons, OFAC has issued a legal fee guide containing the requirements and documentation necessary to release limited amounts of blocked funds for payment of legal fees and costs incurred in challenging their blocking in administrative or civil

98 The CFR contains numerous licences for legal services under different US sanctions programmes. See, e.g., 31 CFR §§ 510.507, 515.512, 560.525, 576.507 and 589.506 for licences for legal services relating to the country-specific sanctions programmes targeting North Korea, Cuba, Iran, Iraq and Ukraine, respectively; see also 31 CFR §§ 594.506, 544.507, 590.506 and 530.506 for licences for legal services relating to sanctions programmes targeting terrorism, proliferators of weapons of mass destruction (WMD), transnational criminal organisations and narcotics trafficking.

99 See, e.g., 31 CFR §§ 560.553, 579.507 and 589.507, detailing the requirements US persons must fulfil to receive payment for legal services from funds originating outside the United States in the Iran, Foreign Interference in the US Elections and Ukraine sanctions programmes, respectively.

100 US Dep't of Treasury, Filing a Petition for Removal from an OFAC List (footnote 46).

101 See, e.g., 31 CFR § 544.507(a) of the WMD proliferators sanctions programme, which does not contain a general licence and requires all legal services providers to obtain a specific licence for payment; see also US Dep't of Treasury, Filing a Petition for Removal from an OFAC List (footnote 46).

proceedings.[102] This route is only available if there are no other funding options for the blocked US person[103] and it does not ensure payment of legal fees in their entirety.[104]

Incidental transactions

Most sanctions programmes provide that transactions ordinarily incident to and necessary to a licensed transaction are permitted, provided that the transaction does not involve a blocked person or blocked property.[105] Although OFAC has not issued a comprehensive list of the types of activities that are considered ordinarily incident to or necessary to a licensed transaction, certain general licences and guidance from OFAC provide insight into this authorisation, the scope of which is dependent on the underlying permitted activity. Described below are a few examples from OFAC's country-wide sanctions programmes.

Travel

US sanctions against Cuba impose restrictions on travel by US persons to Cuba; the purpose of the travel must fall within one of OFAC's authorised categories.[106] Activities that are ordinarily incident to and necessary to the travel are also authorised and include activities such as the exportation of accompanied baggage for personal use,[107] payment of living expenses, purchase of goods for personal consumption, and the purchase of health insurance, life insurance and travel insurance, including paying for any emergency medical services.[108]

---

102 US Dep't of Treasury, 'Guidance on the release of limited amounts of blocked funds for payment of legal fees and costs incurred in challenging the blocking of U.S. persons in administrative or civil proceedings' (23 July 2010), at https://ofac.treasury.gov/media/6191/download?inline.

103 id., at Introduction.

104 id., at Part III, explaining that the Guidance follows fee rates and caps established by the Criminal Justice Act and the Equal Access to Justice Act.

105 See, e.g., 31 CFR § 510.404 (North Korea); 31 CFR § 515.421 (Cuba); 31 CFR § 560.405 (Iran); 31 CFR § 589.404 (Ukraine). Most commonly, any ordinarily incident, or necessary, transaction with a blocked person is not permitted under these provisions, among other exceptions.

106 31 CFR § 515.560.

107 OFAC FAQ 730 (last updated 14 October 2016), at https://ofac.treasury.gov/faqs/730.

108 31 CFR § 515.560(c)(2) and Note 2.

Import/export

When licences permit exports or imports of certain goods to or from a sanctioned country, OFAC has provided examples of ordinarily incident transactions that are permitted. For example, in the context of a general licence permitting imports of certain goods from Cuban entrepreneurs, ordinarily incident transactions include payments for those goods made using online payment platforms.[109]

Publishing

Under numerous sanctions programmes, transactions that are necessary and ordinarily incident to 'the publishing and marketing of manuscripts, books, journals, and newspapers in paper or electronic format' are authorised.[110] These types of authorised transactions include commissioning and making advance payment for future written publications, collaboration to create and enhance these works, substantive editing, payment of royalties, implementing a marketing campaign for promotional purposes, and any other 'transactions necessary and ordinarily incident to the publishing and marketing of written publications'.[111] The publishing authorisations are also supported by the 'informational materials' exception that permits the exportation and importation of publications and other types of media to or from sanctioned countries.[112] The publishing authorisations, however, do not confer general permission to engage in business activities that are 'delivered through the use of information and informational materials', such as accounting, legal, design and consulting services, that do not involve publishing activities.[113] Likewise, these provisions do not generally authorise activities such as marketing products other than written publications, importing and exporting goods other than certain software used to support written publications in electronic format, engaging in transactions relating to travel to and from the sanctioned country, or operating a publishing house or sales outlet within the sanctioned country.[114]

---

109 80 Fed Reg 56918 (21 September 2015).

110 See, e.g., 31 CFR §§ 515.577, 542.532, 560.538, detailing the various transactions that qualify as necessary and incidental to publishing written publications under the Cuba, Syria and Iran sanctions programmes, respectively.

111 31 CFR § 515.577(a); see also 31 CFR §§ 542.532(a), 560.538(a).

112 31 CFR §§ 515.206(a), 515.332(a); see also 31 CFR §§ 510.213(c), 560.210(c).

113 31 CFR § 515.577(b)(1); see also 31 CFR §§ 542.532(b)(1), 560.538(b)(1). However, as discussed above, the provision of legal services may be authorised under a separate general licence.

114 31 CFR §§ 515.577(b)(2) to (b)(5); see also 31 CFR §§ 542.532(b)(2) to (b)(4), 560.538(b)(2) to (b)(4).

Export administration regulations

In addition to the sanctions imposed by OFAC, the US Department of Commerce's Bureau of Industry and Security (BIS) enforces the Export Administration Regulations (EAR) codified at 15 CFR Part 730 et seq. in respect of exports, re-exports and in-country transfers of goods of US origin, and technology and software to destinations outside the United States and to non-US citizens. The EAR impose limitations on the unlicensed export, re-export or transfers of goods, technology or software of US origin, including transit through or to sanctioned jurisdictions such as Cuba, North Korea, Crimea, Iran and Syria. The EAR generally apply to commodities with a minimum of 10 per cent US-origin content for exportation to sanctioned jurisdictions, and 25 per cent US-origin content for exportation to all other countries, so it is important for businesses to properly screen exports in compliance with the EAR.

BIS maintains its own lists of prohibited or restricted individuals, separate from OFAC's sanctions lists. It can therefore be important for companies with components or products of US origin to consult both OFAC and BIS designations to understand applicable restrictions.[115]

Termination of US sanctions

Considering that the underlying goal of US economic and trade sanctions is to advance the United States' foreign policy and national security objectives, it is natural that these objectives may change or be accomplished, leading to the termination of sanctions programmes.

For example, the only remaining sanctions programme based on the authority of TWEA is the Cuban Asset Control Regulations.[116] Previous sanctions programmes supported by TWEA have been rescinded.

In many cases, the President may lift sanctions by issuing an executive order. For example, in 2016, President Obama terminated comprehensive sanctions against Myanmar by an executive order in light of advances in the promotion of democracy, the release of political prisoners and greater enjoyment of human

115 As regards defence articles, the State Department's Bureau of Political-Military Affairs Directorate of Defense Trade Controls likewise maintains its own designation lists and restrictions, in connection with its enforcement of the International Traffic in Arms Regulations.

116 'The US Economic Sanctions Regime at II.B(2)' in *Sanctions Enforcement and Compliance: A Practitioner's Guide to OFAC*, Bloomberg BNA Banking Practice Portfolio Series (2019). See also 85 Fed. Reg. 67988 (27 October 2020) (noting that US sanctions against Cuba are promulgated pursuant to the Trading with the Enemy Act).

rights and fundamental freedoms.[117] However, in 2021, President Biden issued an executive order imposing targeted, non-comprehensive sanctions against Myanmar in response to the February 2021 coup that overthrew the democratically elected civilian government.[118] Throughout 2021, President Biden imposed asset-blocking sanctions against persons involved in repressing the pro-democracy movement in Myanmar. In 2017, President Obama terminated sanctions against Sudan through an executive order because of the country's reduction in offensive military activity, improved humanitarian access and cooperation with the United States on addressing regional conflicts and the threat of terrorism.[119]

Under certain statutes authorising sanctions, the President may not unilaterally lift sanctions without approval from Congress. For example, CAATSA prohibits the President from lifting sanctions against a person designated under certain Russia-related sanctions authorities if Congress issues a joint resolution of disapproval.[120] With respect to Cuba, the US embargo is mandated by statute and likely would require congressional action to be repealed; however, the President has the authority to issue executive orders or OFAC policies to loosen certain aspects of the sanctions programme against Cuba, as President Obama did during his presidency.[121]

117 Executive Order 13742 (7 October 2016).

118 Executive Order 14014 (10 February 2021).

119 Executive Order 13761 (13 January 2017).

120 CAATSA § 216(b)(6); Pub. L. 115-4, 131 Stat. 886, 902 (2 August 2017); 22 USC § 9511(b)(6).

121 See, e.g., The White House, 'Presidential Policy Directive – United States–Cuba Normalization' (14 October 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/10/14/presidential-policy-directive-united-states-cuba-normalization.

CHAPTER 6

US Sanctions Enforcement by OFAC and the DOJ

David Mortlock, Britt Mosman, Nikki Cronin and Ahmad El-Gamal[1]

Introduction

The US Department of the Treasury's Office of Foreign Assets Control (OFAC) administers and enforces most economic and trade sanctions. Specifically, OFAC is responsible for civil enforcement of US sanctions laws, and its regulations are enforced on a strict liability basis, meaning that OFAC does not need to prove fault or intent to enter an enforcement action and issue a civil penalty. In addition to OFAC, the US Department of Justice (DOJ) and the US Attorney may pursue criminal investigations and enforcement actions for wilful violations of US sanctions laws. Federal criminal prosecutions of sanctions violations are generally conducted on referral by OFAC, although the DOJ may choose to pursue some cases on its own initiative.[2] Other regulators, such as the Financial Crimes Enforcement Network (FinCEN) and the New York State Department of Financial Services, may impose additional penalties for failure to maintain specific controls to help ensure compliance with OFAC-administered regulations.

Companies should also account for any complementary export control restrictions implemented by the Department of Commerce and enforced by the Bureau of Industry and Security (BIS), or the Department of State and the Directorate of Defense Trade Controls (DDTC) in the case of defence articles and defence services, which may be imposed with respect to exports involving sanctioned countries and regions or sanctioned persons. As evidenced by the significant

1 David Mortlock and Britt Mosman are partners, and Nikki Cronin and Ahmad El-Gamal are associates, at Willkie Farr & Gallagher LLP.

2 31 C.F.R. Part 501 Appendix A (II)(F).

export restrictions placed on Russia and Belarus following Russia's invasion of Ukraine,[3] the publication of significant new OFAC sanctions programmes or updates to existing programmes are often followed by a corresponding restriction on exports to the affected countries, regions or persons. Notably, OFAC, BIS and the DDTC may have different licence requirements to engage in certain activities. A failure to understand each respective set of licensing requirements and acquire all the necessary licences to engage in an otherwise prohibited activity could leave a company facing an enforcement action and potential penalties from one or more regulators.

Both federal and state regulators may pursue enforcement actions for the same conduct simultaneously, which could lead to multiple investigations by multiple entities. In 2019, OFAC Director Andrea Gacki made it clear that OFAC would no longer give credit for all types of fines paid to other agencies in global, multi-agency settlements.[4] This change in how OFAC calculates fines could lead to increased penalties in global settlement agreements where OFAC would have taken into account the amount of fines and penalties being levied by other agencies when determining the final penalty amount. Currently, for a non-egregious violation, ignoring any adjustment of the penalty based on aggravating or mitigating factors, the base penalty amount would be approximately the value of the transaction, determined specifically by a schedule provided in OFAC's enforcement guidelines, capped at US$356,579 per transaction.[5] If a company voluntarily discloses an apparent violation to OFAC, the base amount of the proposed civil penalty is one-half of the transaction value capped at a maximum base amount of US$178,290 per violation.[6]

---

3 The Department of Commerce's Bureau of Industry and Security (BIS) has imposed sweeping export control restrictions on Russia and Belarus. These restrictions have been updated, modified and added to on a near continuous basis since they were first imposed on 24 February 2022. The continually changing regulatory landscape means that parties should ensure they are up to date on the latest additions or modifications to the export controls targeting Russia and Belarus. The Department of Commerce maintains and updates a list of the press releases and federal register links related to the export controls on Russia and Belarus at www.bis.doc.gov/index.php/policy-guidance/country-guidance/russia-belarus.

4 Dylan Tokar, 'Treasury Department Changes Approach to Fines in Sanctions Cases', *Wall Street Journal* (14 June 2019), at www.wsj.com/articles/treasury-department-changes-approach-to-fines-in-sanctions-cases-11560552590.

5 31 C.F.R. Part 501, Appendix A(V)(B)(2)(a)(ii).

6 id., Appendix A(V)(B)(2)(a)(i).

The overall number of enforcement actions closed and published by OFAC remains down from the 2019 high of 26 enforcement actions totalling US$1.2 billion in settlements and penalties, which was largely attributable to two significant OFAC settlements (UniCredit Bank for US$611 million and Standard Chartered Bank for US$657 million).[7] In 2022, OFAC published 16 enforcement actions representing a total of US$43.6 million in settlements and penalties. While the number of published enforcement actions has remained relatively consistent since 2020, the total settlement and penalty amounts for 2022 doubled those reported for 2021 and for 2020. This is largely due to the enforcement action against Bittrex, Inc,[8] the largest cryptocurrency-related enforcement action to date.

OFAC has continued to pursue novel and more aggressive enforcement theories, including showing a willingness to pierce the corporate veil and pursue enforcement cases for even indirect contact with US financial institutions and expanding its jurisdiction in the wake of technological advancement. OFAC has also strengthened its commitment to pursue enforcement actions in the cryptocurrency sector after publishing its first two enforcement actions related to cryptocurrency transactions on 30 December 2020 and 18 February 2021, nearly two years after the publication of FAQs 559 to 563.[9] The 11 October 2022 enforcement action against Bittrex, Inc, a Seattle-based entity providing online cryptocurrency exchanges and wallet services, was settled for US$24.3 million, making it the largest cryptocurrency-related settlement to date.[10] Bittrex's settlement with OFAC was part of a global settlement that included FinCEN, which determined a civil money penalty of over US$29 million for Bittrex's failure to implement an effective anti-money laundering programme, making it the first joint

7 See US Department of the Treasury's Office of Foreign Assets Control (OFAC), 'Enforcement Information for April 15, 2019', at https://ofac.treasury.gov/media/16521/download?inline; OFAC, 'Enforcement Information for April 9, 2019', at https://ofac.treasury.gov/media/26286/download?inline.

8 See Financial Crimes Enforcement Network (FinCEN), 'In The Matter Of: Bittrex, Inc.', Consent Order Imposing Civil Money Penalty, No. 2022-03, at www.fincen.gov/sites/default/files/enforcement_action/2023-04-04/Bittrex_Consent_Order_10.11.2022.pdf.

9 Published in March 2018, FAQs 559–563 detail the compliance responsibilities of entities involved in the cryptocurrency industry or using cryptocurrency as a means of conducting transactions as well as providing key definitions and information on how OFAC will use existing authorities to bring enforcement actions with respect to apparent violations involving the use or transfer of cryptocurrency. See OFAC FAQs 'Questions on Virtual Currency', at https://ofac.treasury.gov/faqs/topic/1626.

10 See OFAC, 'Enforcement Information for October 11, 2022', at https://ofac.treasury.gov/media/928746/download?inline.

rollout of an enforcement action with FinCEN. The enforcement action against Bittrex followed OFAC's publication of its Sanctions Compliance Guidance for the Virtual Currency Industry in October 2021, which is intended to be used as a resource to help members of the virtual currency industry understand and comply with their sanctions obligations.[11]

Notably, there has been little judicial review or oversight of OFAC's enforcement theories. Almost all cases that are not resolved by no-action or cautionary letters are settled, and very few are challenged in court. However, there are exceptions to this general trend, including Exxon Mobil Corporation's challenge of a US$2 million civil penalty imposed by OFAC, which resulted in the penalty being vacated by a district court in the Northern District of Texas on the grounds that OFAC failed to provide fair notice regarding the agency's interpretation of the relevant sanctions regulations.[12] Additionally, in enforcement actions concluded after the May 2019 release of OFAC's 'A Framework for OFAC Compliance Commitments' (the Framework),[13] OFAC has assessed parties' compliance with the Framework as an aggravating or mitigating circumstance, tracking the parties' violations against the Framework. The trends in enforcement, highlighted by recent OFAC cases, show that a strong compliance programme in line with the Framework is a key factor for parties seeking to avoid OFAC enforcement actions going forward.

Criminal enforcement

The DOJ enforces criminal sanctions violations. Criminal liability may be imposed against a person who wilfully commits, attempts to commit or conspires to commit, or aids or abets in the commission of, an unlawful act pursuant to the International Emergency Economic Powers Act (IEEPA), the Act pursuant to which most sanctions regulations are issued. Criminal liability pursuant to the IEEPA may include a fine of not more than US$1 million or, if a natural person, a prison term of not more than 20 years, or both.[14]

---

11 US Department of the Treasury, 'Sanctions Compliance Guidance for the Virtual Currency Industry', October 2021, at https://ofac.treasury.gov/media/913571/download?inline.

12 See *Exxon Mobil Corporation v. Steven Mnuchin*, Civil Action No. 3:17-CV-1930-B (N.D. Tex. 2019).

13 US Department of the Treasury, 'A Framework for OFAC Compliance Commitments', at https://ofac.treasury.gov/media/16331/download?inline.

14 50 U.S.C. 1705(c).

Recent DOJ actions in the wake of the sanctions placed on Russia have pushed the DOJ to the forefront of sanctions enforcement along with OFAC. These include the creation of Task Force KleptoCapture on 2 March 2022, an inter-agency law enforcement task force led by the DOJ and aimed at enforcing the sanctions, export restrictions and economic countermeasures placed on Russia.[15] Since its creation, the Task Force has been involved in the seizure of assets and funds from Russian kleptocrats, including the seizure of a US$90 million yacht belonging to Viktor Vekselberg, a sanctioned Russian oligarch.[16] In the year since its inception, in addition to seizing over US$500 million in assets, the Task Force has indicted over 30 individuals and two corporate entities accused of sanctions evasion, export control violations, money laundering and other crimes.[17]

The DOJ has also continued to prosecute individuals that have violated US sanctions, including bringing cases against one US citizen and two European citizens for conspiring to assist North Korea in evading sanctions and the first criminal indictment for violations of US sanctions against Russia for its 2014 incursion into Ukraine. On 25 April 2022, the Southern District of New York unsealed an indictment against two European citizens who were charged with conspiring to violate US sanctions on North Korea by working with a US citizen to illegally provide cryptocurrency and blockchain technology services to North Korea. On 12 April 2022, the DOJ announced that the US citizen was sentenced to 62 months in prison after pleading guilty to conspiracy to violate the IEEPA by providing technical advice and instructions to North Korea on using block-chain and cryptocurrency technology to launder money and evade US sanctions and for pursuing plans to facilitate North Korea's dealings in cryptocurrency.[18]

---

15 See US Department of Justice (DOJ), 'Attorney General Merrick B. Garland Announces Launch of Task Force KleptoCapture', 2 March 2022, at www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-launch-task-force-kleptocapture.

16 See DOJ, '$90 Million Yacht of Sanctioned Russian Oligarch Viktor Vekselberg Seized by Spain at Request of United States', 4 April 2022, at www.justice.gov/opa/pr/90-million-yacht-sanctioned-russian-oligarch-viktor-vekselberg-seized-spain-request-united.

17 See DOJ, 'Fact Sheet: Justice Department Efforts in Response to Russia's February 2022 Invasion of Ukraine', at www.justice.gov/opa/press-release/file/1569781/download.

18 See DOJ, 'U.S. Citizen Who Conspired to Assist North Korea in Evading Sanctions Sentenced to Over Five Years and Fined $100,000', 12 April 2022, at www.justice.gov/opa/pr/us-citizen-who-conspired-assist-north-korea-evading-sanctions-sentenced-over-five-years-and; and DOJ, 'Two European Citizens Charged for Conspiring with a U.S. Citizen to Assist North Korea in Evading U.S. Sanctions,' 25 April 2022, at www.justice.gov/opa/pr/two-european-citizens-charged-conspiring-us-citizen-assist-north-korea-evading-us-sanctions#:~:text=Both%20Cao%20De%20Benos%20and,Kevin%20Castel.

In the actions targeting a Russian oligarch and his US associate, the DOJ charged a US citizen with violations of US sanctions for his dealings with Russian national Konstantin Malofeyev, who is also designated on OFAC's List of Specially Designated Nationals and Blocked Persons. Malofeyev was also charged with conspiracy to violate US sanctions and violations of US sanctions for hiring a US citizen to work with him and conspiring to transfer US dollars from a US bank for the benefit of Malofeyev, a blocked person.[19] The DOJ highlighted in its press release that OFAC designated Malofeyev in 2014 pursuant to Executive Order 13660 when OFAC determined that Malofeyev was one of the main sources of financing for Russians promoting separatism in Crimea, and materially assisted, sponsored and provided financial, material or technological support for, or goods and services to or in support of, the so-called 'Donetsk People's Republic'.[20] The DOJ noted that this was the first ever criminal indictment for violations of the sanctions on Russia for its 2014 activity in Crimea.[21]

The DOJ has also cracked down on the use of shell companies and transshipment points in third-party countries to evade the sanctions and export control restrictions on Russia. In October 2022, the DOJ unsealed an indictment, dated 26 September 2022, charging five Russian nationals, a Spanish national and a seventh co-conspirator with sanctions evasion and money laundering in connection with a global scheme to obtain US military technology and sanctioned Venezuelan oil using a network of shell companies and cryptocurrency transactions.[22]

---

19 See DOJ, 'TV Producer for Russian Oligarch Charged with Violating Crimea-Related Sanctions', 3 March 2022, at www.justice.gov/opa/pr/tv-producer-russian-oligarch-charged-violating-crimea-related-sanctions; and DOJ, 'Russian Oligarch Charged with Violating U.S. Sanctions', 6 April 2022, at www.justice.gov/opa/pr/russian-oligarch-charged-violating-us-sanctions.

20 ibid.

21 ibid.

22 See Indictment, *United States v. Orekhov, et al.*, Case 1:22-cr-00434-EK (E.D.N.Y. 26 September 2022); see also DOJ Press Release, 'Five Russian Nationals and Two Oil Traders Charged in Global Sanctions Evasion and Money Laundering Scheme', 19 October 2022, at www.justice.gov/usao-edny/pr/five-russian-nationals-and-two-oil-traders-charged-global-sanctions-evasion-and-money.

Investigation

Commencement

The US government can learn of a potential sanctions violation in a number of ways, but the primary means of discovery are through voluntary self-disclosures (VSDs), reports of blocked and rejected transactions, referrals from other government agencies and even publicly available information, such as media reports.

If a company conducts an internal investigation or otherwise learns of a potential violation itself, it may submit a VSD to OFAC. A VSD has many benefits, described further below, including a significant reduction in the base penalty calculation for any potential enforcement action. Depending on the particular circumstances of a violation, the submission of a VSD and subsequent cooperation with OFAC should be carefully considered.

Learning of apparent violations through blocked or rejected transaction reports and other means[23]

A VSD is not the only means by which the government learns of potential violations. The government frequently learns of violations through reports generated by US persons, primarily banks, that have blocked or rejected a transaction based on a suspected sanctions violation. US persons are required under the sanctions regulations to submit blocking and reject reports to OFAC within 10 business days of the action to block or reject a transaction. Beginning in June 2019, new regulations require that all US persons report rejected transactions to OFAC within 10 days.[24] Previously, all parties already had an obligation to report transactions involving blocked property to OFAC, but only US financial institutions had the obligation to report rejected transactions. OFAC may also learn of sanctions violations through anti-money laundering reports, primarily suspicious activity reports (SARs), which are also typically submitted by banks and other financial institutions.

OFAC may also learn of potential violations through other government agencies, including those of foreign governments. Criminal investigations conducted by the DOJ and other federal and state law enforcement can lead to the discovery of sanctions violations.

---

23 See OFAC, 'Enforcement Information for June 13, 2019', at https://ofac.treasury.gov/media/16311/download?inline.

24 See 31 C.F.R. Part 501.

Notification

Once OFAC learns of a potential violation and decides to launch an investigation, it may make an initial request for information with an administrative subpoena or, depending on the nature of the violation, direct a more informal set of questions to the involved parties, including non-US persons.

Notably, a 2019 DC Circuit Court of Appeals decision – which required three Chinese banks, two of which have US branches, to comply with the government's grand jury subpoenas and document production orders in connection with the violation of the US sanctions on North Korea – expanded the ability of US federal prosecutors to subpoena the financial records of foreign financial institutions during an investigation.[25] The Court held that in instances where a foreign bank has a US branch, it consents to federal court jurisdiction on matters overseen by the Federal Reserve, including money laundering and sanctions violations.[26] The Court also held that the Attorney General's power under the Bank Secrecy Act (BSA) to compel a foreign bank to produce documents is not limited to transactions that pass directly through a foreign bank's US foreign account, but also any foreign records with a connection to the bank's US correspondent account.[27]

The DOJ's authority to issue subpoenas to foreign financial institutions was expanded under the Anti-Money Laundering Act of 2020 (AMLA). In addition to having the authority to issue subpoenas to foreign financial institutions that maintain a correspondent account in the United States for records related to the correspondent account, the AMLA expanded the DOJ's subpoena power to cover 'any account at the foreign bank, including records maintained outside of the United States' if those records are the subject of a broad list of enforcement actions, including criminal prosecutions or violations of the BSA.[28]

Competent authorities

The authorities responsible for enforcing US sanctions are primarily OFAC (responsible for civil enforcement) and the DOJ (responsible for criminal enforcement). Furthermore, financial regulators, including the New York State Department of Financial Services and the Federal Reserve Board, may impose fines and other penalties for compliance failures associated with insufficient sanctions compliance programmes.

---

25 See *In re: Sealed Case*, No. 19-5068 (D.C. Cir. 6 August 2019).

26 id. at 10.

27 id. at 9.

28 31 U.S.C. § 5318(k) as amended by the Anti-Money Laundering Act 2020.

As the United States has increasingly implemented a whole-of-government approach to tackling national security concerns and addressing foreign policy issues, we have increasingly seen significant export control restrictions being imposed alongside sanctions. Additionally, it is often the case that sanctions violations involving the export of US-origin items will also constitute a violation of US export controls. BIS is responsible for implementing and enforcing the Export Administration Regulations, and the Department of State's Directorate of Defence Trade Controls is responsible for implementing and enforcing the International Traffic in Arms regulations, each governing civil and dual-use items and defence services and products, respectively.

Substantive offences

Each sanctions programme administered by OFAC is different depending on the aims of the US government. OFAC sanctions programmes generally prohibit US persons from engaging in transactions, directly or indirectly, involving designated individuals or entities (persons). Other sanctions programmes, such as those against Cuba and Iran, are comprehensive in nature, generally prohibiting exports of goods or services by US persons or from the United States to those territories. Regardless, there are common elements for a finding of an apparent violation, generally a breach of regulations for an embargo or transaction involving Specially Designated Nationals and blocked persons or entities subject to sectoral sanctions. OFAC regulations are civil in nature, meaning they generally do not require mens rea, intent or knowledge for an apparent violation to be found and a penalty to be assessed. However, if the apparent violation included a wilful attempt at evading, avoiding, attempting or conspiring to evade or avoid, or facilitating a prohibited transaction, it could expose the party to criminal liability and prosecution by the DOJ.

OFAC's enforcement authority and procedures are further defined by its general enforcement guidelines at 31 CFR 501 Appendix A. These enforcement guidelines establish the factors for calculating the base penalty amounts, based on a number of specific factors including whether the violation is deemed egregious or non-egregious and whether the violations were voluntarily disclosed to OFAC.

Recent trends in enforcement actions

The following trends have been prevalent in recent civil enforcement actions issued by OFAC.

Piercing the corporate veil[29]

In an enforcement action against the General Electric Company (GE), OFAC signalled its willingness to pierce the veil in enforcement cases by entering enforcement proceedings against GE regarding apparent violations by three of its non-US subsidiaries. The three non-US subsidiaries of GE had accepted 289 payments from The Cobalt Refinery Company, a party owned in part by the Cuban government and on OFAC's Specially Designated Nationals and Blocked Persons List. Foreign persons that are owned or controlled by a US person are required to comply with the restrictions imposed by the Cuban Assets Control Regulations.

In an enforcement action against Berkshire Hathaway Inc, OFAC again pierced the veil by entering an enforcement proceeding against Berkshire for apparent violations of the Iranian Transactions and Sanction Regulations (ITSR) by its indirectly wholly owned Turkish subsidiary. Of note, these actions were conducted under the direction of certain senior managers in Turkey despite Berkshire and other Berkshire subsidiaries' repeated communications and policies being sent to the Turkish subsidiary regarding US sanctions against Iran and the application of the ITSR to its operations in Turkey. The ITSR explicitly state that a penalty shall be imposed against the US parent for a foreign subsidiary's prohibited dealings with Iran.

Indirect contact with US financial institutions[30]

In an enforcement action against British Arab Commercial Bank (BACB), OFAC considered even tenuous and indirect contact with US financial institutions as grounds for an enforcement action. OFAC found that BACB had violated Sudanese sanctions, and despite the fact that the transactions at issue were not processed to or through the US financial system, the bank did operate a nostro account in a country that imports Sudanese-origin oil to facilitate payments involving Sudan. The bank funded the nostro account with large, periodic US dollar wire transfers from banks in Europe, which in turn transacted with US financial institutions in a manner that violated OFAC sanctions.

29 See OFAC, 'Enforcement Information for October 1, 2019', at https://ofac.treasury.gov/media/26481/download?inline; and OFAC 'Enforcement Release: October 20, 2020', at https://ofac.treasury.gov/media/48756/download?inline.

30 See OFAC, 'Enforcement Information for September 17, 2019', at https://ofac.treasury.gov/media/26036/download?inline.

Expanded jurisdiction[31]

In an enforcement action against Société Internationale de Télécommunications Aéronautiques SCRL (SITA), OFAC showed its willingness to penalise non-US companies for transactions that would not have been covered by OFAC's jurisdiction if they had not used US servers. OFAC's basis for jurisdiction over SITA, a global information technology services provider headquartered in Switzerland and serving commercial air transportation, was that the technology provided to sanctioned parties was hosted on and incorporated functions that routed messages through US servers and contained US origin software.

Enforcement tracked to OFAC's Framework for Compliance Commitments[32]

In an enforcement action against Eagle Shipping International, OFAC stated:

As noted in OFAC's Framework for Compliance Commitments, this case demonstrates the importance for companies operating in high-risk industries (e.g., international shipping and trading) to implement risk-based compliance measures, especially when engaging in transactions involving exposure to jurisdictions or persons implicated by US sanctions.

Scrutiny of the cryptocurrency industry[33]

In an enforcement action against BitPay, Inc, OFAC signalled that companies involved in providing digital currency services would be subject to the same compliance requirements as financial institutions. BitPay offers a payment processing solution for its direct merchant customers to accept digital currency. Specifically, BitPay would receive digital currency payments on behalf of its merchant customers and converts the digital currency to fiat currency before relaying that currency to the merchant. While BitPay screened its direct customers, it failed to screen location data it obtained about its merchant buyers. As a result, BitPay processed 2,102 transactions on behalf of individuals located in sanctioned jurisdictions.

---

31 See OFAC, 'Enforcement Information for February 26, 2020', at https://ofac.treasury.gov/media/33096/download?inline.

32 See OFAC, 'Enforcement Information for January 27, 2020', at https://ofac.treasury.gov/media/33086/download?inline.

33 See OFAC, 'Enforcement Information for October 11, 2022', at https://ofac.treasury.gov/media/928746/download?inline.

Conducting transactions indirectly that would otherwise be considered a violation[34]

In an enforcement action against Generali Global Assistance, Inc (GGA), OFAC highlighted the importance of ensuring that sanctions compliance policies and procedures address both direct and indirect sanctions compliance risks. GGA served as a travel services provider on behalf of two Canadian insurers that offered policies for Canadian subscribers who travelled to Cuba, providing medical expense claim processing and payment services to one of the Canadian insurers. For payments intended for Cuban service providers, GGA would intentionally refer the requests to a Canadian affiliate and then reimburse that affiliate for the amounts paid. In the enforcement action, OFAC specifically noted the sanctions risks of implementing a procedure to process, indirectly, transactions whose direct processing would be prohibited by US sanctions laws.

In addition to these trends, the 30 March 2023 enforcement action detailing Wells Fargo Bank, NA's US$30 million settlement related to apparent violation of three sanctions programmes was notable because Wells Fargo was not involved in the apparent violations.[35] Wachovia Bank, a US bank that was acquired by Wells Fargo in 2008, provided a foreign bank, located in Europe, with software that was then used to process trade finance transactions with sanctioned persons and jurisdictions. OFAC found that Wachovia either knew or should have known that the foreign bank was using the platform to manage the transactions and that, after acquiring Wachovia, Wells Fargo did not identify or stop the foreign bank's use of the software platform for seven years despite the internal concerns that were raised at the time. This enforcement action highlights the need for comprehensive due diligence during the process of a merger or acquisition to identify and address potential violations of US sanctions.

Mitigating and aggravating factors

OFAC regulations outline the general factors that it will consider when determining the appropriate enforcement response to an apparent violation of its regulations.

34 See OFAC, 'Enforcement Release: October 1, 2020', at https://ofac.treasury.gov/media/48326/download?inline.

35 See OFAC, 'Enforcement Release: March 30, 2023', at https://ofac.treasury.gov/media/931541/download?inline.

Factors that OFAC will consider to be aggravating or mitigating include:

- wilful or reckless violation of law, including factors such as concealment, a pattern of conduct and management involvement;[36]
- awareness of the conduct at issue;[37]
- harm to sanctions programme objectives, including factors such as economic benefit to the sanctioned country and whether the conduct was likely to have been eligible for an OFAC licence;[38]
- individual characteristics of the party in question, such as commercial sophistication and whether the party has received a penalty notice or a finding of violation from OFAC in the five years preceding the date of the transaction giving rise to the violation;[39]
- the existence, nature and adequacy of a compliance programme in place at the time of the violation;[40]

---

36 OFAC's enforcement action against UniCredit Bank AG highlighted the bank's wilful intent to circumvent US sanctions, citing formal UniCredit Bank documents containing policies and procedures that instructed bank personnel to ensure payment structures were formatted in a way that hid the participation of OFAC-sanctioned parties. See OFAC 'Enforcement Information for April 15, 2019', at https://ofac.treasury.gov/media/16521/download?inline.

37 OFAC found that Standard Chartered Bank had actual knowledge or reason to know of its apparent violations of several sanctions regulations, including the Cuban Assets Control Regulations and the Iranian Transactions and Sanctions Regulations, which OFAC deemed an aggravating factor. See OFAC 'Enforcement Information for April 9, 2019', at https://ofac.treasury.gov/media/26286/download?inline.

38 OFAC found that Jiangsu Guoqiang Tools Co Ltd (GQ), a subsidiary of Stanley Black & Decker, Inc, which agreed to pay the penalty for both itself and GQ, harmed the objectives of the Iranian Transactions and Sanctions Regulations by conferring an economic benefit to Iran in a systematic scheme involving the export and attempted export of several shipments of power tools and spare parts to a third country with knowledge that the goods were intended specifically for supply, transshipment or re-exportation to Iran. See OFAC 'Enforcement Information for March 27, 2019', at https://ofac.treasury.gov/media/9321/download?inline.

39 In OFAC's enforcement action against Cubasphere Inc for violations of the Cuban Assets Control Regulations, it considered the fact that Cubasphere was a small company with few employees as a mitigating factor. By contrast, in OFAC's enforcement action against Apollo Aviation Group, LLC (Apollo) for violations of the Sudanese Sanctions Regulations, it highlighted Apollo's size and sophistication as an aggravating factor. See OFAC 'Enforcement Information for June 13, 2019', at https://ofac.treasury.gov/media/16321/download?inline; and OFAC, 'Enforcement Information for November 7, 2019', at https://ofac.treasury.gov/media/25941/download?inline.

40 In OFAC's enforcement action against Haverly Systems, Inc for violations of the Ukraine Related Sanctions Regulations, it considered the fact that Haverly did not have a formal

- the remedial response that the party took upon learning of the violation;[41] and
- cooperation with OFAC, through a VSD or subsequent cooperation during the investigation (or both).[42]

A key factor, as evidenced by recent OFAC decisions, is the existence and maintenance of an adequate compliance programme in line with OFAC's Framework for Compliance Commitments. Since 2020, each of the decisions published by OFAC has included a paragraph referencing the Framework.[43]

As with OFAC, the DOJ generally views voluntary disclosure, full cooperation and timely and effective remedial measures as mitigating factors, as described in its updated VSD policy.[44]

OFAC sanctions compliance programme at the time the apparent violations occurred an aggravating factor. See 'OFAC Enforcement Information for April 25, 2019', at https://ofac.treasury.gov/media/16626/download?inline.

41 In OFAC's enforcement action against Union de Banques Arabes et Françaises (UBAF), it considered the remedial actions taken by UBAF a mitigating factor. Those remedial measures included the adoption of a new Financial Security Charter, providing training for UBAF employees, reviewing its business lines and terminating certain services that were deemed high risk, and establishing a Compliance Committee to monitor company-wide compliance. See 'OFAC Enforcement Release: January 4, 2021', at https://ofac.treasury.gov/media/50346/download?inline.

42 In OFAC's enforcement action against TD Bank, N.A. (TDBNA), it found that TDBNA's cooperation with OFAC by providing well-organised and user-friendly information in a prompt manner was a mitigating factor. See 'OFAC Enforcement Release: December 23, 2021', at https://ofac.treasury.gov/media/917121/download?inline.

43 See, for example, 'OFAC Enforcement Release: December 30, 2020', BitGo, Inc, at https://ofac.treasury.gov/media/50266/download?inline ('On May 2, 2019, OFAC published A Framework for OFAC Compliance Commitments in order to provide organizations subject to US jurisdiction, as well as foreign entities that conduct business in or with the United States or US persons, or that use US-origin goods or services, with OFAC's perspective on the essential components of a sanctions compliance program. The Framework also outlines how OFAC may incorporate these components into its evaluation of apparent violations and resolution of investigations resulting in settlements. The Framework includes an appendix that offers a brief analysis of some of the root causes of apparent violations of US economic and trade sanctions programs OFAC has identified during its investigative process.').

44 In addition to the DOJ's Export Control and Sanctions Enforcement Policy for Business Organizations, the DOJ Criminal Division's Corporate Enforcement Policy similarly emphasises the importance of disclosure and cooperation. See DOJ Criminal Division, Corporate Enforcement and Voluntary Self-Disclosure Policy, 17 January 2023, at https://www.justice.gov/criminal-fraud/file/1562831/download.

The guidelines from the DOJ's updated VSD policy,[45] discussed in further detail below, break down full cooperation as:

- timely disclosure of all non-privileged facts;
- proactive cooperation;
- timely voluntary preservation, collection and disclosure of relevant documents (Guidelines list examples); and
- deconfliction of witness interviews, and, when requested and subject to the individuals' Fifth Amendment rights, making company officers and employees available for interviews.

The updated policy notes that not all companies will satisfy all the components of full cooperation and, while the benefits will be markedly less than for full cooperation depending on the extent to which the company is lacking, companies should still be eligible for partial credit if they provide all relevant non-privileged information related to individual accountability.

The updated policy also lays out what the DOJ considers as aggravating factors during an investigation for criminal sanctions violations, which include:[46]

- conduct that involves a grave threat to national security;[47]
- egregiousness or pervasiveness of criminal conduct within the company;
- exports of items controlled for nuclear non-proliferation or missile technology reasons to a proliferator country;
- exports of items known to be used in the construction of weapons of mass destruction;
- exports to a foreign terrorist organisation or specially designated global terrorist;
- exports of military items to a hostile foreign power;
- repeated violations, including similar administrative or criminal violations in the past;

45 DOJ, National Security Division (NSD), 'NSD Enforcement Policy for Business Organizations' (1 March 2023), at https://www.justice.gov/file/1570996/download.

46 ibid.

47 This aggravating factor was added in the latest update to the NSD Enforcement Policy for Business Organizations. The NSD clarifies that, by their nature, wilful violations of sanctions, export controls or other laws within the NSD's jurisdiction often pose serious risks to national security. The Policy further states that these risks will need to be weighed accordingly to determine whether or not the DOJ will seek a guilty plea.

- a significant profit to the company, relative to the company's overall profits, from the misconduct; and
- concealment or involvement of upper management in the criminal conduct.

The DOJ released an update to its 'Evaluation of Corporate Compliance Programs'[48] guidance document on 1 March 2023. The 'Principles of Federal Prosecution of Business Organizations',[49] as referenced by the Evaluation of Corporate Compliance Programs, include several factors that prosecutors should consider when conducting an investigation of a corporation, including the adequacy and effectiveness of a corporation's compliance programme at the time of an offence. Maintaining an effective compliance programme may be considered an additional mitigating factor.

When determining whether a corporation has an effective compliance programme, the DOJ considers three main questions:

- Is the corporation's compliance programme well designed?
- Is the compliance programme being applied earnestly and in good faith?
- Does the corporation's compliance programme work in practice?

Best practice for corporations in an investigation

If an investigation has commenced, it is generally in parties' best interests to endeavour to proactively collaborate with the agency conducting the investigation. OFAC enforcement actions have shown that it considers cooperation to be a mitigating factor in an enforcement case and the DOJ has stated that for a party to receive the benefits of a VSD, it must fully cooperate with the DOJ. Generally, full cooperation includes but is not limited to internal investigations to discover the root cause of an apparent violation, responding to regulators' requests for additional information in a timely and complete manner, preserving all sensitive or relevant documents, collaborating with regulators to develop and implement effective remedial measures, and, in the case of a DOJ investigation, deconflicting and making available any potential witnesses. Under no circumstances should parties attempt to hide or destroy evidence of an apparent violation once an investigation has commenced. Any indication of actions opposing an investigation is likely to lead to investigators taking a more hostile approach and may also

48 DOJ, Criminal Division, 'Evaluation of Corporate Compliance Programs' (updated March 2023), at www.justice.gov/criminal-fraud/page/file/937501/download.

49 DOJ, 'Principles of Federal Prosecution of Business Organizations', at www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.

constitute an offence of obstructing proceedings before departments, agencies and committees pursuant to 18 USC 1505 or conspiracy to obstruct justice under 18 USC 371. Parties should also consider notifying relevant non-US regulators,[50] shareholders, counterparties, insurers and other interested parties.

Self-reporting

Reporting to OFAC

As mentioned above, OFAC views the self-disclosure of apparent violations favourably. The self-disclosure of a violation can significantly reduce a potential civil penalty amount. To be considered voluntary, a disclosure must be self-initiated and made to OFAC before either OFAC or any government agency or official discovers the apparent violation. Notification of an apparent violation to another government agency, which is considered a VSD by that agency, may be considered a VSD to OFAC on a case-by-case basis. When making a VSD to OFAC, the VSD must include or be followed by a report containing sufficient details to provide a complete understanding of the circumstances of the apparent violation. In some instances, it may be beneficial to the party to make a preliminary disclosure to OFAC before knowing all the facts so as to make a timely disclosure while ensuring that the disclosure is voluntary. Parties should also ensure that their VSD and follow-up report contain all the details known at the time they are submitted. Parties submitting VSDs should also be prepared to respond to any follow-up enquiries by OFAC.[51]

However, not all notifications to OFAC of an apparent violation will be considered a VSD. Specifically, a notification will not be considered a VSD if a third party notifies OFAC of the apparent violation or substantially similar apparent violation because it blocked or rejected a transaction, or if the disclosure:

- includes false or misleading information or is materially incomplete;
- is not self-initiated;
- is made without the authorisation of senior management; or
- is in response to an administrative subpoena or other enquiry form.[52]

Filing a licence application with OFAC is also not considered a VSD.[53]

---

50 See Chapter 4 regarding The Bank of Tokyo-Mitsubishi UFJ Limited being fined for not informing the UK prudential regulator of its sanctions enforcement exposure in the US.

51 31 C.F.R. 501 Appendix A (I)(I).

52 ibid.

53 ibid.

Reports to OFAC in certain instances are required by OFAC regulations. Specifically, US persons are required to submit reports of rejected and blocked transactions to OFAC within 10 business days of the action.[54] These reports are typically made by financial institutions and must include details of the rejected or blocked transactions, such as the names of the parties, accounts involved and date and amount of payment. Additionally, annual reports on blocked property must be filed with OFAC by 30 September of each year.[55] It is important to note that these reports will not be considered a VSD to OFAC and the disclosure of violations that OFAC has already been made aware of by a reject or blocking report submitted by another party will not receive the benefits of a VSD.

Reporting to the DOJ

Under the DOJ's Export Control and Sanctions Enforcement Policy for Business Organizations, all business organisations, including financial institutions, are eligible for the full range of benefits of the DOJ's self-disclosure programme.[56] Although there is no requirement to self-report to the DOJ, owing to the timeliness requirements discussed below, a VSD must be made early in the investigation process if it is to receive credit from the DOJ.

Mirroring other DOJ self-disclosure policies, companies are eligible for credit when they (1) voluntarily self-disclose export control or sanctions violations to the National Security Division's Counterintelligence and Export Control Section (CES), (2) fully cooperate with the investigation, and (3) remediate any violations appropriately and in a timely manner. The threshold for eligibility is self-disclosure of potential violations to CES; self-disclosing to any other regulatory agency does not qualify a party as a self-discloser under the DOJ policy.[57]

For the purposes of the DOJ's VSD policy, for a party's disclosure to be considered voluntary it must be made prior to an imminent threat of disclosure or government investigation, and within a reasonably prompt time after discovery of the offence, and the party must disclose all relevant facts known to it at the time of the disclosure. The DOJ recognises that parties may not know all relevant facts at the time of disclosure, especially if the parties submit a VSD based on a

54 31 C.F.R. 501.603 and 501.604.

55 ibid.

56 See DOJ, NSD (footnote 45).

57 That said, the updated Policy clarifies that credit will be applied in instances where a corporation has made a good faith disclosure to another office or component of the DOJ, and the matter is partnered with, or transferred to and resolved with, the NSD. ibid.

preliminary investigation. The policy states that if that is the case, a party should make clear that it is making its disclosure based on a preliminary investigation or assessment of information while still providing all available information.

To receive credit for full cooperation, parties are required to disclose all relevant facts in a timely manner; to cooperate proactively with the DOJ; to preserve, collect and disclose all relevant documents and information; to deconflict witness interviews when required; and to make officers and employees of the party available for interviews by the DOJ when so requested. The policy notes that eligibility for cooperation credit does not depend on the waiver of the attorney–client privilege or the work-product protection, although experience suggests that the DOJ typically initiates a discussion on privilege at some point during corporate investigations.

Finally, to receive credit for remediation measures, parties are required to demonstrate a thorough analysis of the causes of the underlying conduct and, where appropriate: engage in remediation; implement an effective compliance programme; discipline employees identified by the party as responsible for the oversight; retain business records and prohibit the improper destruction of those records; and take any additional steps that demonstrate recognition of the seriousness of a party's misconduct.

Considerations before self-reporting

In general, costs associated with making a VSD to either OFAC or the DOJ include legal expenses, government scrutiny, reputational harm and, potentially, large monetary penalties. Tied to the additional scrutiny and investigation by government agencies, apparent violations of US sanctions laws other than those disclosed in the VSD may be discovered during the course of an investigation. When parties are deciding whether or not to submit a VSD, they must weigh these negative factors against the likelihood that a government agency independently discovers or is notified by a third party of the apparent violation and the nature and value of the apparent violation.

A VSD submitted to either OFAC or the DOJ will only be accepted if it is made before there was a significant likelihood that the government would be notified of the apparent violation or otherwise discover it on its own. Additionally, by not making a VSD, parties are forfeiting a valuable opportunity to frame the issue and present any mitigating factors before a government investigation commences.

Prior to proceeding with a VSD, parties should also consider the date a potential violation occurred. The statute of limitations for sanctions violations is generally five years from the date of the apparent violation. However, as part of the settlement process parties may enter into tolling agreements with OFAC, which

is considered a mitigating factor, to extend the statute of limitations if it is at risk of expiring during the course of the investigation and settlement process. Parties should also be aware that while the statute of limitations for sanctions violations is generally five years, a criminal investigation conducted by the DOJ may uncover violations of other statutes with significantly longer statutes of limitations.[58] If the violations that are the subject of the VSD also raise issues of potential exposure in other jurisdictions, parties should note that different jurisdictions may have different or no statutes of limitations. For example, the UK does not have a statute of limitations for indictable offences. Depending on the situation, a party may be safe in limiting its investigations and the submission of VSDs to conduct within the past five years; however, parties should be aware that there are instances where the statute of limitations is greater than five years.

Considerations before submitting a VSD to OFAC

The submission of a VSD to OFAC can have several benefits, including as a mitigating factor when calculating a penalty or, in some cases, allowing a party to avoid an enforcement action. OFAC may decline to take action if it determines that the conduct does not constitute a violation, or it may decide that the conduct does not warrant a civil monetary penalty and issue a cautionary letter instead.[59] However, the main benefit of a VSD is that, if accepted, the VSD will reduce the base amount of the penalty by approximately 50 per cent in both egregious and non-egregious cases.[60] VSDs are not the only mitigating factors that OFAC takes into account when determining the amount of a penalty. Parties should immediately take any reasonable remedial measures after discovering the apparent violation and discuss those measures in their submission. Additionally, parties should maintain a compliance programme in line with OFAC's Framework for Compliance Commitments and, to the extent possible, map the apparent violation against their compliance programme and how the party has remedied, or intends to remedy, any latent deficiencies in its programme.

Further, when submitting a VSD to OFAC, a party must consider the chance that OFAC may launch a broader investigation and uncover additional, undisclosed violations under one of its many sanctions programmes or violations that

58 One example is the bank fraud statute, which carries a 10-year statute of limitations. See 18 U.S.C. 1344. Additionally, the presence of a conspiracy to violate sanctions laws may extend the statute of limitations as it does not begin until the final overt act committed for its benefit.

59 31 C.F.R. 501 Appendix A (II)(C).

60 31 C.F.R. 501 Appendix A (V)(B)(a).

cause OFAC to notify other government agencies, including a potential referral to the DOJ for criminal enforcement. While notifications made to other government agencies may be considered a VSD for OFAC enforcement purposes, a VSD to OFAC will not qualify as a VSD made to the DOJ. Therefore, parties should carefully consider if there was an element of wilfulness in the apparent violations or other activity that could be considered criminal in nature and would cause OFAC to refer the case to the DOJ. If a party believes that the case may be referred to the DOJ, it should consider submitting a VSD to the DOJ either prior to, or simultaneously with, submitting its VSD to OFAC to benefit from the DOJ's VSD policy.

Considerations before submitting a VSD to the DOJ

If the party satisfies the three requirements of the DOJ's VSD policy – voluntarily self-disclosing a violation; fully cooperating with the investigation; and remediating any violations appropriately and in a timely manner – there is a presumption that the party will receive a non-prosecution agreement (NPA) and will pay no fine, absent aggravating factors. However, even if a party receives an NPA, at a minimum the party will not be permitted to retain any of the unlawfully obtained gain and will be required to pay all disgorgement, forfeiture or restitution resulting from the misconduct.

Additionally, even if aggravating circumstances exist, the DOJ will still recommend a fine of at least 50 per cent less for a qualifying party than otherwise would have been levied and will not require the imposition of a monitor if the party has implemented an effective compliance programme at the time of resolution. In addition to maintaining compliance programmes in line with OFAC's Framework, parties should ensure their programmes meet the criteria laid out in the DOJ's updated 'Evaluation of Corporate Compliance Programs' guidance document.

While the DOJ's VSD policy certainly has issues that businesses must consider before self-reporting, for businesses and financial institutions, the revised policy is also a potential lifeline to protect them from large financial penalties and potential

criminal prosecution as seen in recent DOJ cases regarding UniCredit,[61] Société Générale[62] and Halkbank.[63] Despite this, there are still issues with the policy that may deter business organisations from submitting VSDs to the DOJ.

One factor to take into consideration under the DOJ's VSD policy is that it makes clear that a VSD to a regulatory agency will not be enough to qualify for the benefits of the DOJ policy. This is in contrast to OFAC's position that notification of an apparent violation to another government agency that is considered a VSD by that agency may be considered a VSD by OFAC based on a case-by-case assessment. This, coupled with the requirement that a VSD be made before any imminent threat of disclosure or government investigation, means that parties must decide early in their investigation of a potential violation of sanctions or export laws if they need to file both with regulatory agencies and the DOJ. Investigations can take unexpected turns, however, transforming an ostensible civil issue into a potential criminal matter if evidence of wilfulness is discovered. However, by filing with the DOJ, a party could expose itself to a potential criminal investigation and heavy, continuing disclosure obligations.

Moreover, the policy applies only to the DOJ and does not bind other regulators, including state banking regulators such as the New York State Department of Financial Services or the Federal Reserve. Those other enforcement authorities have their own programmatic mandates, which may be inconsistent with the outcomes available under the DOJ's VSD policy. Put differently, self-reporting to the DOJ may earn you the carrot from the DOJ, but you may still face the stick from other regulators.

The key to effectively utilising this policy rests in the foundation of a party's compliance policies and procedures. Even if the policies and procedures fail to prevent a violation from occurring, they can assist a party in quickly determining the nature and degree of the violation. This should help parties recognise earlier in their investigation of a potential violation whether they need to issue a VSD to the DOJ.

---

61 See Press Release, DOJ, 15 April 2019, at www.justice.gov/opa/pr/unicredit-bank-ag-agrees-plead-guilty-illegally-processing-transactions-violation-iranian.

62 See Press Release, DOJ, 19 November 2018, at www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-criminal-charges-against-soci-t-g-n-rale-sa-violations.

63 See Press Release, DOJ, 15 October 2019, at www.justice.gov/opa/pr/turkish-bank-charged-manhattan-federal-court-its-participation-multibillion-dollar-iranian.

Other notification requirements

During the past few years, the US Securities and Exchange Commission (SEC) has taken a more active role in reviewing economic sanctions compliance. The SEC appears to have taken an interest because of the risks associated with a violation of US sanctions laws. The SEC has increasingly used comment letters[64] to request additional information from parties regarding the financial and reputational risks from costly regulatory action that may be associated with their disclosures to OFAC and their business activities in sanctioned countries.[65] Despite this, the SEC has not traditionally acted as an enforcement agency in the mould of OFAC or the DOJ, only seeking disclosure and reporting of sanctions-related risks.[66] While parties should consider notifying the SEC of apparent violations, this should be done while keeping in mind the requirements for VSD submissions to OFAC and the DOJ. In addition to the SEC, parties should be aware that OFAC maintains memoranda of understanding with several state and federal banking regulatory agencies outlining how they will share information.[67] Banking regulators, such as the Federal Reserve, may impose penalties on the financial institutions they oversee in connection with apparent violations of US sanctions laws. Accordingly, financial institutions should consider notifying their

64 SEC 'comment letters' refer to either letters submitted in response to requests for public comment, or, in this instance, to correspondence between SEC staff and SEC filers. The SEC may use comment letters to request that a party provide additional supplemental information, revise disclosure in a document on file with the SEC, provide additional disclosure in a document on file with the SEC, or provide additional or different disclosure in a future filing with the SEC. There may be several rounds of letters as the SEC's staff and the filer work to resolve a particular issue.

65 Menghi Sun and Mark Maurer, 'SEC Questions More Companies About Sanctions Disclosures', *The Wall Street Journal* (28 August 2019) (citing Audit Analytics), at www.wsj.com/articles/sec-questions-more-companies-about-sanctions-disclosures-11567018243.

66 However, in a recent Foreign Corrupt Practices Act case against Quad/Graphics, the SEC found that, in addition to violating anti-bribery and bookkeeping offences, Quad/Graphics participated in a scheme to circumvent US sanctions and export control laws. See Press Release, Securities and Exchange Commission, 26 September 2019, at www.sec.gov/news/press-release/2019-193. The DOJ had declined to prosecute Quad/Graphics despite finding evidence of bribery and did not reference the sanctions evasion scheme. See DOJ Response Letter, *Re: Quad/Graphics Inc.*, at www.justice.gov/criminal-fraud/file/1205341/download.

67 The US Department of the Treasury maintains a list of memoranda of understanding between OFAC and state and federal banking regulators at https://ofac.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information/2019-enforcement-information/memoranda-of-understanding-between-ofac-and-bank-regulators.

banking regulators of apparent violations if they plan to submit a VSD to OFAC. However, this should be done while conscious of the requirements for VSD submissions to OFAC and the DOJ.

Parties should also assess whether the apparent violation of US sanctions laws also violates the sanctions laws of other jurisdictions. For example, if a party operates in both the United States and the United Kingdom and commits an apparent violation that would be in breach of sanctions law in both countries, the party should consider making a disclosure to both OFAC and the UK's Office of Financial Sanctions Implementation (OFSI), as foreign regulatory agencies may share information regarding apparent violations directly or learn of an apparent violation if it is published by a foreign regulator. This aspect of cross-jurisdictional cooperation with respect to enforcement was brought to the forefront in October 2022 when OFAC and OFSI announced their enhanced partnership initiative after a technical exchange between the two regulators in London.[68] As another example of why parties should be aware of cross-jurisdictional cooperation, recent sanctions designations in Cyprus have been attributed to US government investigations into the affairs of Alisher Usmanov and individuals and entities that are alleged to assist him with concealing details of his assets.[69] Accordingly, a party should ensure that it considers whether its actions violate non-US sanctions laws and whether the party would be subject to the jurisdiction of non-US regulators.

Additionally, parties should be aware of how public perception and negative press relating to the discovery of an apparent violation can materially affect a party's reputation. A VSD and a detailed plan to implement remediation measures targeting the root cause of the apparent violations may mitigate some of the

68 See OFAC Featured Story, 'Enhancing the US–UK Sanctions Partnership', 17 October 2022, at https://home.treasury.gov/news/featured-stories/enhancing-the-us-uk-sanctions-partnership, and Office of Financial Sanctions Implementation (OFSI) Blog, 'OFAC-OFSI Enhanced Partnership', 17 October 2022, at https://ofsi.blog.gov.uk/2022/10/17/ofac-ofsi-enhanced-partnership/. This partnership is further evidenced by (among other things) the joint fact sheet published by OFAC and OFSI on humanitarian assistance and food security and their interconnection with the sanctions targeting Russia and the specified regions of Ukraine. See OFAC and OFSI, 'Humanitarian Assistance and Food Security Fact Sheet: Understanding UK and U.S. Sanctions and their Interconnection with Russia', 28 June 2023, at https://ofac.treasury.gov/media/931946/download?inline.

69 See Helena Smith, 'Cyprus handed 800-page US dossier on Russia sanctions breaches', *The Guardian*, 9 May 2023, at https://amp-theguardian-com.cdn.ampproject.org/c/s/amp.theguardian.com/world/2023/may/09/cyprus-handed-800-page-us-dossier-on-russia-sanctions-breaches.

associated reputational damage. However, regardless of how the apparent violation was reported or discovered, public scrutiny still represents a risk factor for future business partners and investors. As a result, reputational damage could lead to lost opportunities and burdensome due diligence requirements imposed by potential business partners.

Anti-money laundering

Suspicious activity reports

Anti-money laundering investigations can overlap with investigations of apparent sanctions violations. Additionally, disclosures to one regulatory authority can notify other authorities of potential violations leading to overlapping investigations for different violations caused by the same action. A financial institution that intentionally attempts to deceive US regulatory authorities or cover up an apparent violation of US sanctions laws, for example, is likely to simultaneously engage in violations of anti-money laundering laws.[70]

Under the BSA, financial institutions[71] are required to report 'any suspicious transaction relevant to a possible violation of law or regulation'. FinCEN has issued regulations implementing the BSA that require certain financial institutions, including banks, securities broker-dealers, introducing brokers, casinos, futures commission merchants and money services businesses, to report any suspicious activity above a certain dollar threshold in a SAR. Each industry has its own form and, generally, the report must be submitted within 30 days of the detection of the suspicious activity.

---

70 An example of simultaneous sanctions and anti-money laundering enforcement can be found in the ongoing case of Halkbank. The Turkish state-owned bank allegedly participated in a multibillion-dollar scheme to evade US sanctions on Iran, including facilitating fraudulent transactions designed to appear to be purchases of food and medicine. The DOJ referenced the knowing involvement of senior officers at the bank and discussions on how best to structure transactions to evade scrutiny by US regulators. As is often the case with schemes to avoid sanctions, Halkbank violated anti-money laundering laws by using fraudulent pretences and representations to defraud financial institutions. See *United States v. Halkbank*, Superseding Indictment S6 15 Cr. 867 (RMB), at www.justice.gov/opa/press-release/file/1210396/download.

71 The Bank Secrecy Act defines 'financial institutions' at 31 U.S.C. 5312. This list at 31 U.S.C. 5312(a)(2) includes, but is not limited to, insured banks, commercial banks or trust companies, private bankers, brokers and dealers in securities or commodities, investment bankers or companies, insurance companies, certain casinos and any businesses or agencies that engage in any activity that the Secretary of the Treasury determines, by regulation, to be an activity that is similar to, related to or a substitute for any activity in which any business described in 31 U.S.C. 5312(a)(2) is authorised to engage.

OFAC requires financial institutions to submit reports regarding any transactions that were rejected or blocked as a result of the involvement of a person on OFAC's Specially Designated Nationals and Blocked Persons List. These transactions would be considered suspicious activity under the BSA due to the possibility that they violate US sanctions regulations, and financial institutions would be required to submit a SAR to FinCEN. FinCEN's requirements will be satisfied by filing a rejection or blocking report to OFAC, which will then pass the information to FinCEN.[72] However, FinCEN notes that any information related to the activity that was not disclosed or included in the blocking report should be included in a separate SAR filed with FinCEN.[73]

As discussed above, a notice of an apparent violation through a third-party rejection or blocking report will negate any benefit that a party may have received from submitting a VSD. Additionally, because the information filed in a rejection or blocking report will be passed to FinCEN and made available to law enforcement, it could trigger additional investigations relating to money laundering or other civil and criminal offences. Parties should be aware of how regulators share information and how a third-party report may trigger multiple investigations from several government agencies, negating any benefit the party would receive from self-reporting the apparent violation.

In understanding and examining the risks associated with third-party reports, parties should also be aware of the AMLA, ultimately passed on 1 January 2021. The AMLA expands the BSA to include measures to strengthen FinCEN and inter-agency coordination and enforcement, among other provisions such as enhanced regulatory coverage of non-traditional exchanges of value and new beneficial ownership reporting requirements. The AMLA requires the creation of a three-year pilot programme allowing financial institutions to share SARs information with the institution's foreign branches, subsidiaries and affiliates for the purpose of combating illicit finance risks.[74] Additionally, the AMLA also requested the establishment of an exchange designed to facilitate information sharing between financial institutions, law enforcement agencies, national security agencies and FinCEN.[75]

---

72 See FinCEN Interpretive Guidance 'Interpretation of Suspicious Activity Reporting Requirements to Permit the Unitary Filing of Suspicious Activity and Blocking Reports', December 2004, at www.fincen.gov/sites/default/files/guidance/20041214a.pdf.

73 ibid.

74 31 U.S.C. § 5318(g)(8) as amended by the Anti-Money Laundering Act, 2020.

75 31 U.S.C. § 310(d) as amended by the Anti-Money Laundering Act, 2020.

As these programmes continue to develop, the enhanced information-sharing mechanisms and procedures could lead to faster detection by or notification of a potential violation to OFAC, negating any benefits that would be received by self-reporting as the report would no longer be considered voluntary by OFAC. The implementation and effect of these information-sharing programmes should be monitored by parties, and their potential impact on the time it takes for OFAC to independently discover or be notified of an apparent violation considered when deciding if and when to file a VSD.

Resolution of investigations

OFAC has a variety of enforcement options available to it upon learning of a potential violation of US sanctions. If OFAC determines that there is insufficient evidence that a violation has occurred or concludes that the conduct does not warrant an administrative response, then no action will be taken.[76] In cases where OFAC is aware that the subject of the investigation knows of OFAC's investigation, it will generally issue a no-action letter. If OFAC determines that there is insufficient evidence of a violation but that the activity in question could lead to a violation or that there is a lack of due diligence in assuring compliance with US sanctions laws, it may issue a cautionary letter.[77] A cautionary letter will generally list OFAC's concerns about the underlying conduct or concerns regarding the compliance policies, practices and procedures that led to the apparent violation. If OFAC determines that a violation has occurred but that a civil monetary penalty is not appropriate, it may issue a finding of violation.[78] Although there is no monetary penalty involved, OFAC announces findings of violations in press releases and publishes a notice containing the description of the violations and its analysis, which can cause reputational damage to a party.

76 31 C.F.R. 501 Appendix A (II)(A).

77 31 C.F.R. 501 Appendix A (II)(B).

78 See US Department of the Treasury, 'Enforcement Release: July 21, 2022: OFAC Issues a Finding of Violation to MidFirst Bank for Violations of the Weapons of Mass Destruction Proliferators Sanctions Regulations', at https://ofac.treasury.gov/media/924506/download?inline.

Cautionary letter[79]

OFAC may also impose a civil monetary penalty upon determining that a violation has occurred.[80] These penalties will be determined in line with OFAC guidelines and subject to the mitigating and aggravating factors described above. Parties may also decide to enter into a settlement with OFAC to reduce their maximum exposure to penalties.[81] Settlement discussions may be initiated by OFAC or the party that committed the apparent violation. Settlements can be made before or after the issuance of a pre-penalty notice and may include multiple apparent violations, even if they are covered under separate pre-penalty notices. Notably, OFAC settlements may be a part of a comprehensive settlement with other federal, state or local agencies.

Global settlement[82]

Finally, OFAC may refer a case to appropriate law enforcement if it determines that the activity warrants a criminal investigation or prosecution (or both).[83]

Similar to the multiple options available to, and utilised by, OFAC, the DOJ has a variety of enforcement options available to it when closing a case. First, it may choose to resolve a case using a deferred prosecution agreement (DPA) or an NPA. Under a DPA, the DOJ will bring charges against the party committing the violation but agrees not to proceed with those charges so long as the party follows a negotiated set of requirements or conditions. Under an NPA, the DOJ will not file charges against the party and will generally require the party to comply with certain conditions or pay a fine. Additionally, DPAs and NPAs may impose a corporate monitor on the party to the agreement. The party bears the costs of the corporate monitor, and the scope of the monitor's oversight responsibilities is negotiated by the party and the DOJ. The DOJ may also seek the forfeiture of assets relating to the apparent violation as part of the penalties assessed against the party.

---

79 See 'OFAC Enforcement Information for February 14, 2019', at https://ofac.treasury.gov/media/7556/download?inline.

80 31 C.F.R. 501 Appendix A (II)(E).

81 31 C.F.R. 501 Appendix A (V)(C).

82 See, e.g., Press Release, US Department of the Treasury, 'U.S. Treasury Department Announces Settlement with UniCredit Group Banks' (15 April 2019), at https://ofac.treasury.gov/news/press-releases/sm658.

83 31 C.F.R. 501 Appendix A (II)(F).

If the DOJ initiates an investigation either through a referral by another government agency or independent discovery of an apparent violation, the offending party may be charged under numerous criminal statutes, depending on the nature of the violation. For example, a single party may be charged for a wilful violation of the IEEPA while simultaneously being charged for fraud, criminal money laundering and other offences committed in coordination with the apparent violation.[84] These charges could lead to significant monetary penalties and potential imprisonment for individuals involved in the apparent violation.[85]

Looking ahead to the future of enforcement

The prolific use of cryptocurrency and other methods of evading US sanctions on Russia has led to a number of asset seizures and criminal enforcement cases. As the conflict continues and the sanctions targeting Russia expand, we anticipate that this trend will continue. We have also seen the development of a whole-of-government approach to tackling sanctions evasion schemes as they often implicate violations of US export control[86] and anti-money laundering laws. This

84 See Press Release, DOJ, 15 October 2019, at www.justice.gov/opa/pr/turkish-bank-charged-manhattan-federal-court-its-participation-multibillion-dollar-iranian ('[Halkbank] was charged today in a six-count indictment with fraud, money laundering, and sanctions offenses related to the bank's participation in a multibillion-dollar scheme to evade U.S. sanctions on Iran.').

85 One example of this is the indictment and arrest of John Can Unsalan, the president of Metalhouse LLC, for engaging in violations of US sanctions against Sergey Kurchenko and two of Kurchenko's companies. For three years, acting through Metalhouse, Unsalan transferred over US$150 million to Kurchenko and Kurchenko's companies in exchange for metal products. Unsalan was charged with conspiracy to violate US sanctions, 10 counts of violating the International Emergency Economic Powers Act, one count of conspiring to commit international money laundering and 10 counts of international money laundering. If convicted, in addition to the United States' intention to forfeit from Unsalan the proceeds of his offences, he faces a maximum of 20 years in prison for each count of conviction. See DOJ, 'President of Metalhouse LLC Indicted for Sanctions Evasion and International Money Laundering', 17 April 2023, at www.justice.gov/opa/pr/president-metalhouse-llc-indicted-sanctions-evasion-and-international-money-laundering.

86 It should also be noted that BIS has placed significant export control restrictions on Russia in support of OFAC's sanctions programmes and the US government's foreign policy objectives. This has resulted in criminal actions brought by the DOJ against persons violating the export controls against Russia as well as the imposition of temporary denial orders by BIS, suspending the export privileges of parties deemed to have violated US export controls on Russia. This includes the 24 February 2023 Temporary Denial Order suspending the export privileges of Radiotester OOO and a Russian individual, Ilya Balakaev, for the unauthorised export of controlled counter-intelligence items to Russia and North Korea and the five-count indictment in the Eastern District of New

has been evidenced by the 2 March 2023 publication of a tri-seal compliance note by OFAC, the DOJ and BIS highlighting the work of Task Force KleptoCapture and providing guidance to financial institutions and other entities on how to detect and report sanctions and export control evasion schemes.[87]

Additionally, while no civil enforcement actions have been published by OFAC with respect to apparent violation of the US sanctions on Russia in relation to activity conducted after Russia's invasion of Ukraine, it should be noted that enforcement actions are generally finalised and published by OFAC several years after the apparent violations have occurred. Accordingly, we expect to see enforcement actions related to post-invasion activities being published within the next two to three years.[88] Companies should remain up to date on the sanctions targeting Russia, as they are continuously updated by OFAC, and ensure that they are complying with all applicable prohibitions.

Recent OFAC and DOJ actions also suggest that enforcement bodies will focus enforcement of violations by persons outside of the traditional banking sector, historically the target of OFAC's largest penalties, towards new high-risk sectors such as financial technology businesses and those involved in cryptocurrency trading. We have already seen this occurring with the Bittrex, Inc enforcement action and expect to see further development in this space in light of the use of cryptocurrencies to evade Russian sanctions.

As companies look to strengthen their compliance programmes in an effort to mitigate the risk of violations and subsequent enforcement, OFAC's Framework will continue to be a valuable guide to what it will look for in a risk-based compliance programme and the key factors it will consider as aggravating and mitigating

---

York brought against Balakaev in a related action. See BIS, *Ilya Balakaev et al.*, Temporary Denial Order, 24 February 2023, at https://efoia.bis.doc.gov/index.php/documents/export-violations/export-violations-2023/1467-e2806/file; Indictment, *United States v. Balakaev*, Case 1:13-cr-00079 (E.D.N.Y. 21 February 2023), at www.justice.gov/d9/press-releases/attachments/2023/02/24/us_v._balakaev_indictment_0.pdf.

87 See 'Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note: Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls', 2 March 2023, at www.bis.doc.gov/index.php/documents/enforcement/3240-tri-seal-compliance-note/file.

88 While potentially a standard request for information from OFAC, reports on the regulator's recent requests to Raiffeisen Bank International with respect to its role in the Russian economy and exposure in Russia could be an initial insight into how OFAC is pursuing enforcement of its sanctions targeting Russia. See John O'Donnell, Francesco Canepa and Alexandra Schwarz-goerlich, 'Exclusive: U.S. sanctions authority probes Raiffeisen on Russia', Reuters, 20 February 2023, at www.reuters.com/business/us-sanctions-authority-asks-raiffeisen-about-business-related-russia-2023-02-17/.

factors in the event of an enforcement action. Companies should also look to guidance provided in OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry and be aware of the red flags indicating attempts to evade Russia-related sanctions detailed in the tri-seal compliance note referenced above. Finally, companies should ensure that they understand the latest developments in the sanctions compliance space and are able to effectively identify and address any gaps in their compliance programmes and procedures.

CHAPTER 7

Export Controls in the European Union

Anahita Thoms[1]

Introduction

Export controls can be described as restrictions on international trade in certain sensitive goods, software and technology (hereinafter, items). Generally, this involves licensing requirements or prohibitions on the cross-border movement of items identified on specified control lists established at national or international level, or when sensitive end uses are involved, with potentially severe consequences for non-compliance.

In the European Union, export controls include both EU-wide restrictions provided for through EU legislation and EU Member State-specific export controls set out at a national level. In each case, these controls are administered and enforced at national Member State level, resulting in certain variations in how export controls are applied across the EU.

This chapter gives an overview of export control rules under EU law, covering the key types of controls on items subject to EU export controls; the circumstances in which export controls apply; export licensing requirements and practicalities; and the potential consequences of non-compliance.

Overview of EU export controls

EU export controls consist of a patchwork of EU-wide rules set out pursuant to EU legislation and local rules applied by individual Member States. These rules predominantly implement export controls on items agreed pursuant to international frameworks to which the EU or its Member States are party (i.e., the

1 Anahita Thoms is a partner at Baker McKenzie.

Wassenaar Arrangement, the Australia Group (chemical weapons), the Nuclear Suppliers Group, the Chemical Weapons Convention and the Missile Technology Control Regime).

In line with these international frameworks, EU export controls apply to both tangible and intangible exports of controlled items (i.e., types of goods, software or technology specifically identified on relevant export control lists, such as the EU list of dual-use controlled items as described below). Each of these controlled items will be classified under a relevant export control regime, with a specific control entry (the EU equivalent of a US Export Control Classification Number); otherwise, the item will be classified as 'NLR' (no licence required). EU export control rules can also apply to exports of non-listed items (i.e., those that do not specifically appear on export control lists) if there is knowledge, awareness or (in some cases) suspicion of a sensitive end use (known as 'catch all' end-use controls). This includes certain end uses relating to the military sector or weapons of mass destruction.

The two main export control regimes in the EU are those concerning: (1) dual-use export controls (i.e., items that can be used for commercial or civilian purposes but also for military purposes); and (2) military export controls, generally in relation to listed items that are specially designed or modified for military use. As noted below, certain other regimes apply in the EU, including in relation to torture equipment.

Key questions for assessing transactions under EU export control rules

When considering any transaction under EU export control rules, key questions to consider include the following.

- Classification: are any items involved in the transaction classified on any relevant EU export control list (and, if so, which list and which specific export control entry applies)? This analysis can be complex, requiring detailed understanding of both the export control lists and the technical specifications of the items in question, given both the breadth and detail of relevant export control lists (which also often include various exceptions and exemptions).
- End use: is there evidence indicating that the items may be intended for a controlled end use? In some cases, an exporter may be informed by a relevant authority or they may be clearly aware of a controlled end use and will thus need to apply for a licence. In other cases, there may be red flags in a transaction that give rise to suspicion of a controlled end use, which must be carefully considered in each individual case under the relevant laws.

- Export: is there a licensable 'export' or other controlled activity? Only certain types of dealings with controlled items (or transactions involving controlled end uses) will require a licence under export controls. For example, in respect of EU dual-use export controls, a licence is generally required for any physical shipment or intangible transfer of a controlled dual-use item from within to outside the territory of the EU. In certain more sensitive cases, transfers of items between EU Member States (or even within an individual EU Member State), or the arrangement or negotiation of transfer between third countries, may require an export licence.
- Destination and end user: where and to whom will the item be exported? These questions will often determine which type of licence may be required or may be available, or whether the relevant authority will grant a licence at all. In this respect, EU export controls often overlap with EU sanctions where the destination or end user are subject to restrictive measures under an EU sanctions regime. In assessing transactions, it is also important to consider the risk of an item being diverted to a destination or end user other than those intended.
- Exporter: which entity is the exporter? This will often depend on which party holds the contract and has the power to determine the export of an item. The exporter will be responsible for obtaining any necessary export licence and be at risk of penalties in the event of any breach of export control rules. Under EU dual-use export controls, the country of establishment of the exporter will also determine which EU Member State will be responsible for licensing in respect of the relevant export.
- Licensing: what kind of export licence may be available (if any), and which conditions and requirements apply? Even if an exporter can obtain or register to use a relevant export licence, it is imperative to ensure that its exports are within the scope of that licence and that all conditions are fully complied with (including in respect of registration, record-keeping and end-user undertakings).

EU dual-use export control regime

In the EU, the key dual-use export control legislation is currently the EU Dual-Use Regulation.[2] This sets out EU-wide controls that are directly applicable in all EU Member States, including controls on specifically listed dual-use items and in respect of exports relating to controlled end uses.

EU dual-use items

Definition and scope of dual use

Under the EU Dual-Use Regulation, dual-use items are defined as:

> *items, including software and technology, which can be used for both civil and military purposes, and includes items that can be used for the design, development, production or use of nuclear, chemical or biological weapons or their means of delivery, including all items that can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices.*[3]

The EU Dual-Use Regulation sets out lists of specific types of dual-use items for which a licence (referred to within the Regulation as an 'authorisation') must be obtained in advance of export. Items covered by the EU Dual-Use Regulation include:

- goods (i.e., physical items);
- software – defined to cover a collection of one or more 'programs'[4] or 'micro-programs'[5] fixed in any tangible medium of expression. This includes software stored on computer hardware, and on removable storage such as USB drives, CDs and DVDs; and

2 Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 most recently amended by Commission Delegated Regulation (EU) 2023/66 of 21 October 2022, setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.

3 id., Chapter I, Article 2(1).

4 id., Annex I, defines 'program' as 'a sequence of instructions to carry out a process in, or convertible into, a form executable by an electronic computer'.

5 id., Annex I, defines 'microprogram' as 'a sequence of elementary instructions, maintained in a special storage, the execution of which is initiated by the introduction of its reference instruction into an instruction register'.

- technology – defined to cover specific information necessary for the 'development', 'production' or 'use' of goods (or software), with those terms further defined within the EU Dual-Use Regulation.[6] This information takes the form of 'technical data'[7] or 'technical assistance'.[8]

Annex I to the EU Dual-Use Regulation

The main list of controlled items can be found in Annex I, which, in summary, specifies items for which a licence must be obtained before they are exported from within to outside the EU territory. Certain record-keeping and paperwork requirements also apply in respect of intra-EU transfers of items listed in Annex I.

Annex I currently consists of 10 categories of controlled items on more than 300 pages of the Regulation, with control entries including specific technical parameters (such as detailed definitions, exemptions and exceptions). The items controlled in Annex I include various goods, software and technology used in a range of sectors, including marine, aerospace, chemicals, oil and gas, mining, pharmaceutical and nuclear. Statistical estimates published by the European Commission indicate that, in 2020, authorised dual-use trade amounted to €31 billion, representing 2.3 per cent of total extra-EU exports.

In line with international export control frameworks as noted above, the 10 categories in Annex I to the EU Dual-Use Regulation are as follows:

- Category 0: nuclear materials, facilities and equipment;
- Category 1: special materials and related equipment;
- Category 2: materials processing;
- Category 3: electronics;
- Category 4: computers;
- Category 5: telecommunications (Part 1) and information security (Part 2);
- Category 6: sensors and lasers;
- Category 7: navigation and avionics;
- Category 8: marine; and
- Category 9: aerospace and propulsion.

---

6 id., Annex I.

7 id., Annex I notes that 'technical data' may take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices, such as disk, tape and read-only memories.

8 id., Annex I notes that 'technical assistance' may take forms such as instructions, skills, training, working knowledge and consulting services and may involve the transfer of 'technical data'.

Each of these categories is further subdivided into sections, covering:

- A: systems, equipment and components;
- B: test, inspection and production equipment;
- C: materials;
- D: software; and
- E: technology.

Each of these sections is then further subdivided into individual control entries for particular items, often very technical and detailed in nature, with certain exceptions and exemptions. There are also a number of general exceptions from export control. These cover, for example, software and technology that is in the public domain.

By way of example of an Annex I dual-use item, a server with controlled encryption functionality may be caught within Annex I control list entry 5A002a1, denoting that:

- this is an 'information security' ttem (Category 5, Part 2);
- this is from the 'systems, equipment and components' subcategory (subcategory A, within Category 5, Part 2); and
- the server meets the specific control parameters of entry 5A002a1 (a control entry derived from the Wassenaar Arrangement).

Annex IV to the EU Dual-Use Regulation

A much shorter list of more sensitive items is set out at Annex IV to the EU Dual-Use Regulation. Annex IV is divided into two parts. Items listed in Part I can be transferred within the EU on the basis of a National General Authorisation. In contrast, Part II contains items for which a licence is also required for intra-EU transfers. These items include highly sensitive items, such as cryptanalytic items, most nuclear-related items, stealth-related technology and items relating to missiles and chemical warfare.

Additional national Member State dual-use controls

In addition to control lists set out under the EU Dual-Use Regulation, EU Member States may also set out their own lists of controlled dual-use items. Germany, for instance, has done so by including some dual-use items on the national export list[9] that are not already covered by the EU Dual-Use Regulation, if they are to be exported to certain countries. One example is entry 6A908, which

9 Foreign Trade and Payments Act, Annex 1, Part 1, Section B on dual-use items.

refers to radar-based navigation or surveillance systems for shipping or air traffic or components thereof that are not already covered under Annex I to the EU Dual-Use Regulation, if the destination of the items is Iran.

End-use controls under the EU Dual-Use Regulation

As noted above, a licence may be required in respect of items that are not controlled under a relevant list, when the transaction may involve a controlled end use. These are the 'catch all' controls, as any item could in theory be subject to a licensing requirement depending on the end use.

Key end-use controls under the EU Dual-Use Regulation include the following:

- weapons of mass destruction-related end use (WMD end use): a licence will be required if an exporter has been informed by a competent Member State authority that an item is or may be intended, in its entirety or in part, 'for use in connection with the development, production, handling, operation, maintenance, storage, detection, identification or dissemination of chemical, biological or nuclear weapons or other nuclear explosive devices or the development, production, maintenance or storage of missiles capable of delivering such weapons';[10]
- military end use: a licence will be required if an exporter has been informed that an item is or may be intended, in its entirety or in part, for a specified 'military end-use'. In short, these military end uses cover situations in which: (1) the item is or may be intended for use with military equipment in a destination subject to an EU or Organization for Security and Co-operation in Europe arms embargo; or (2) the item may be intended for use as parts of military goods illegally obtained from the EU, irrespective of destination; and
- a licence will be required if an exporter has been informed that a cyber-surveillance item is or may be intended, in its entirety or in part, for use in connection with internal repression or the commission of serious violations of human rights and international humanitarian law. Cyber-surveillance items are dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunications systems.

10 Regulation (EU) 2021/821, Chapter II, Article 4.

If an exporter becomes aware that items it proposes to export are intended for any of these end uses, it shall notify the competent authority. Member States may extend this control to apply when a person has grounds for suspecting this type of end use.

In addition, under Article 9 of the EU Dual-Use Regulation, EU Member States may decide to prohibit or impose a licensing requirement on the export of non-listed items for reasons of public security, including the prevention of acts of terrorism or human rights considerations.

Types of activities controlled under the EU Dual-Use Regulation

Exports

A licence will be required for any export of Annex I-listed items or of any non-listed items in respect of a controlled end use.[11] The concept of an export captures both (1) shipments of tangible (physical) goods from within to outside the territory of the EU (including hand carries of items), and (2) intangible transfers of controlled software or technology from within the EU to legal and natural persons and partnerships outside the EU. These exports can occur intra-group and need not involve any sale, consideration or transfer of ownership.

The concept of an intangible transfer under EU export controls is particularly broad and is a common area in which companies can fall foul of the rules. Examples include:

- sending or making available controlled software or technology to a recipient in another country by email or file transfer protocol;
- reading controlled technology to a person in another country over a voice transmission medium; and
- placing controlled software or technology on a server or shared drive and making that software or technology accessible in another country, such as over an intranet site (including if the server to which the items are uploaded is in the same country).

Brokering and transit controls

Licences are also required in certain circumstances when a person or entity in the EU is involved in brokering (e.g., negotiating or arranging) the sale or supply of items between two third (i.e., non-EU) countries.[12] Provided they carry out brokering services from the EU into the territory of a non-EU country, this also

11 id., at Chapter II, Article 3.

12 id., at Chapter II, Article 6.

applies to non-EU persons or entities. These controls typically apply when the relevant EU broker has been informed or is aware of a controlled WMD or military end use in respect of a listed Annex I item. However, Member States are also permitted to extend brokering controls to capture:

- non-listed dual-use items that are or may be intended for a controlled WMD or military end use; and
- circumstances in which there are grounds for suspecting a WMD or military end use.

Likewise, while items in transit through the EU (i.e., passing through the EU from and to a non-EU destination) are not subject to EU dual-use export controls, Member States may prohibit items in transit if they are or may be intended for a controlled WMD or military end use.

Intra-EU transfers

As the EU is a single customs territory allowing for free movement of goods, export controls principally apply to exports of dual-use goods from the EU to a destination outside the EU. Intra-EU movements of most dual-use items do not normally require a licence. However, there are a few important points to note:

As noted below, military controlled items generally require a licence for transfers between EU Member States, as these controls are set at national level.

As noted above, certain sensitive dual-use items as listed under Annex IV to the EU Dual-Use Regulation require an authorisation to be transferred between EU Member States. Those items listed in Part I of Annex IV can be transferred on the basis of a National General Authorisation while items listed in Part II of Annex IV cannot.

Licences may be required for intra-EU movement of dual-use items when the items will be re-exported from the EU without being further processed, and a licence would be required to export them from the EU. This is an optional control that only certain EU Member States have implemented.

All intra-EU transfers of items listed in Annex I to the EU Dual-Use Regulation must be accompanied by a statement that the items are subject to control if exported from the EU. The statement should appear in the relevant commercial documents (e.g., contracts, order confirmations, invoices and dispatch notes). Additionally, records of intra-EU transfers must be kept for at least three years from the end of the calendar year in which the transfer took place and shall be produced, on request, to the competent authority.

Technical assistance

Licences are also required in certain instances where an entity provides technical assistance related to items listed in Annex I from the territory of the EU into the territory of a third country; or an EU entity provides technical assistance within the territory of a third country or to a resident of a third country temporarily present in the EU. These controls typically apply when the relevant supplier has been informed or is aware of a controlled WMD or military end use in respect of the items in question.

Technical assistance is any technical support related to repairs, development, manufacture, assembly, testing, maintenance or any other technical service, and may take forms such as instruction, advice, training, transmission of working knowledge or skills or consulting services, including by electronic means as well as by telephone or any other verbal forms of assistance.

Military export controls in the European Union

Export controls in relation to military items are controlled by each EU Member State. The EU does maintain a common military list setting out a list of military items subject to export controls. This list is adopted annually by the Council, pursuant to Council Common Position 2008/944/CFSP defining common rules governing control of exports of military technology and equipment. However, this list is non-binding, and it is up to each Member State to legislate for and implement its own, national military export controls.

Generally, controls on military items as adopted by individual Member States – and pursuant to the EU common military list – capture items that are either 'specially designed' or 'modified' for military use. These terms are not currently defined on a pan-EU basis but are generally very broadly interpreted. This can apply (for example) to items that are simply developed or customised for a military customer even if they have civilian applications.

The EU common military list currently captures 22 categories of military-controlled items, again capturing goods, software and technology. Items caught by this list are set out in entries ML1 to ML22, inclusive, covering a range of items, such as:

- weapons and firearms;
- ammunition;
- bombs, rockets, missiles and other explosives and explosive devices;
- military vehicles, vessels, aircraft and drones;
- chemical and biological agents and radioactive materials;
- armoured or protective equipment;

- imaging equipment and other electronic equipment; and
- certain software and technology (in each case specifically designed or modified for military use).

Germany, for example, distinguishes between military items and war weapons. All military items are subject to a licence requirement for exports. However, some of these items are also war weapons, which are subject to further restrictions under the German War Weapons Control Act.

Additional types of controlled items in the EU

In addition to dual-use and military items, a number of other items may be controlled under separate export control lists either at EU or Member State level.

By way of example, the EU's Anti-torture Regulation[13] is a reflection of the EU's commitment to eradicate torture and the death penalty. The measures seek to prevent the trade in certain goods that could be used for capital punishment, torture or other cruel, inhuman or degrading treatment. The Regulation:

- prohibits the import, export, transit, advertising of goods, brokering services or training for goods that have no practical use other than for the purpose of capital punishment or for the purpose of torture and other cruel, inhuman or degrading treatment or punishment;
- requires a prior export authorisation for any export of goods that could be used for capital punishment, torture or for cruel, inhuman or degrading treatment or punishment; and
- regulates the trade in certain pharmaceutical chemicals that could be used in lethal injection executions, without limiting trade of those chemicals for legitimate purposes.

As a specific example of the dynamic nature of export controls, during 2020 we also saw the introduction and subsequent removal of controls in relation to personal protective equipment, in response to the covid-19 pandemic.[14] In 2021, export control restrictions in relation to the covid-19 vaccine were implemented[15] and were in force until the end of 2021.

---

13 Regulation (EU) 2019/125 of the European Parliament and of the Council of 16 January 2019 concerning trade in certain goods that could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment.

14 Commission Implementing Regulation (EU) 2020/402 of 14 March 2020 making the exportation of certain products subject to the production of an export authorisation.

15 Commission Implementing Regulation (EU) 2021/442 of 11 March 2021.

Licensing and compliance under EU export controls

Within the EU, individual Member States are each responsible for licensing in respect of exports (whether in respect of EU-wide controls on dual-use items, or national controls). There is no EU-wide export licensing body.

For example, in Germany, the central authority responsible for issuing licences is the Federal Office for Economic Affairs and Export Controls (BAFA).[16] BAFA offers an online tool through which licences can be obtained and can assist in classifying goods. There are a number of very useful general export authorisations available in Germany, in addition to the EU-wide general export authorisations explained below.

Different types of licences may be available depending on the item and transaction in question (including, in particular, the relevant destination). The EU Dual-Use Regulation sets out certain common forms for licences as follows:

- individual export authorisations (i.e., an authorisation granted to one specific exporter for one end user or consignee in a third country and covering one or more dual-use items);
- global export authorisations (i.e., an authorisation granted to one specific exporter in respect of a type or category of dual-use item that may be valid for exports to one or more specified end users, and in one or more specified third countries);
- large project authorisations (i.e., an individual export authorisation or a global export authorisation granted to one specific exporter, in respect of a type or category of dual-use item that may be valid for export to one or more specified end user in one or more specified third country for the purpose of a specified large-scale project); and
- general export authorisations (GEAs) (i.e., an off-the-shelf export authorisation for exports to certain countries of destination available to all). These may be EU-wide or granted by individual Member States. In particular, EU-wide GEAs are publicly available licences set forth in Sections A to H of Annex II to the EU Dual-Use Regulation and available, on registration, for exports of certain less sensitive items to specific countries, subject to certain conditions. By way of example, the original EU GEA 001 covers all items listed in Annex I to the EU Dual-Use Regulation, with certain exceptions, covering exports to Australia, Canada, Iceland, Japan, Liechtenstein, New Zealand, Norway, Switzerland, the United Kingdom and the United States. Five additional, more limited, EU GEAs were introduced in January 2012 and two GEAs were

16 Bundesamt für Wirtschaft und Ausfuhrkontrolle.

introduced with the recast of the Dual-Use Regulation in 2021. Following the implementation of further sanctions against Russia in 2022, three EU GEAs, that could formerly be used for exports to Russia, were amended.[17]

Each licence covers exports of certain items, to certain destinations, in some cases only to certain end users or consignees. In addition, each licence will have specific conditions, exclusions and requirements. These include obligations to obtain written undertakings from consignees or end users prior to export. For example, these undertakings can include certifications from the end user that they are the intended end user of the goods to be supplied by the licensee, and that the goods will not be used for any purpose connected with chemical, biological or nuclear weapons, or missiles capable of delivering those types of weapons. It is critical for exporters to ensure full compliance with the terms of any export licence. This is a typical area of non-compliance, with authorities in the EU commonly conducting audits in which they scrutinise exports for compliance with all licence conditions.

Certain licences may only be granted when the EU exporter can demonstrate that it has implemented an internal compliance programme (i.e., sufficient export compliance policies and procedures). Again, export authorities may audit exporters to determine whether appropriate policies and procedures are in place. In 2019, the European Commission made specific recommendations in respect of the key elements it would expect to see in an internal compliance programme, which include the following:

- top-level management commitment to compliance;
- organisation structure, responsibilities and resources;
- training and raising awareness;
- transaction screening process and procedures;
- performance review, audits, reporting and corrective actions;
- record-keeping and documentation; and
- physical and information security.[18]

Under the EU Dual-Use Regulation, the relevant export licence must be obtained by the exporter from the Member State authority in which it is established (e.g., where it is incorporated) or, if the exporter is established outside the EU,

17 Commission Delegated Regulation (EU) 2022/699 of 3 May 2022 amending Regulation (EU) 2021/821 of the European Parliament and of the Council by removing Russia as a destination from the scope of Union general export authorisations.

18 Commission Recommendation (EU) 2019/1318 of 30 July 2019 on internal compliance programmes for dual-use trade controls under Council Regulation (EC) No. 428/2009.

by the competent authority of the Member State where the items are located. A licence granted in one EU Member State should be valid for exports from any other Member State (although certain local restrictions can apply in practice). The exporter is currently defined to include (in summary):

- in respect of physical shipments, the party that holds the contract with the consignee in the third country and has the power for determining the sending of the item out of the customs territory of the EU; and
- in respect of intangible transfers, the party that decides to transmit or make available software or technology to a destination outside the customs territory of the EU.[19]

Determining which entity is the exporter, and in which EU Member State it is established (and thus from which Member State's competent authority the relevant export licence must be obtained), is a key matter that is not always straightforward in more complex supply chains. Different Member States can also take different approaches to the concept of 'establishment'.

Consequences of non-compliance with EU export controls

The EU has in place an enforcement coordination mechanism with a view to establish direct cooperation and exchange of information between competent authorities and enforcement agencies. However, the implementation and enforcement of export controls in the EU is also the responsibility of individual EU Member States. The EU Dual-Use Regulation states that each Member State shall take appropriate measures to ensure proper enforcement, including penalties that are effective, proportionate and dissuasive.

Penalties for breaches of export controls can include civil or criminal penalties, or broader legal and practical consequences, varying by jurisdiction. Typical penalties may involve:

- civil or criminal fines;
- imprisonment;
- disqualification of company directors;
- seizure of items that were the subject of the violation; or
- revocation of export licences (including the ability to use general licences).

19 Regulation (EU) 2021/821, Chapter I, Article 2(3).

More broadly, export violations may damage an exporter's relationships with relevant licensing authorities, potentially hampering the ability to obtain export licences in the future (which can significantly affect business activities). Export violations may also damage relationships with banks and other counterparties and key stakeholders, as well as a company's reputation.

CHAPTER 8

Export Controls in the United Kingdom

Tristan Grimmer, Ben Smith and Sophie Armstrong[1]

Overview of UK export controls

Post-Brexit, the UK now has an export control regime that is independent from that of the European Union, governing the movement of dual-use and other sensitive goods from the UK (alongside pre-existing stand-alone UK export controls on military and other items).

The UK's export control regime still remains broadly aligned to that of the European Union, such that the majority of the core principles set out in Chapter 7 continue to apply equally in the UK, and we do not cover those further in this chapter.

However, although broadly related to the EU's regime, there are certain key differences between the UK and EU export control regimes, as well as a number of additional requirements and complexities resulting from the disentanglement of the UK from the EU dual-use export control regime. This chapter summarises these key considerations from a UK export perspective, supplementing the core principles under EU export controls covered in Chapter 7. We also note that the UK's trade sanctions programme increasingly imposes heightened export-related restrictions in supplement to standard UK export controls (see Chapters 3 and 4 for more information on UK trade sanctions).

1 Tristan Grimmer and Ben Smith are partners, and Sophie Armstrong is an associate, at Baker McKenzie.

UK dual-use export controls

Impact of Brexit

Prior to 31 December 2020, the EU Dual-Use Regulation[2] governed the movement of dual-use goods from the European Union to countries outside of the EU and was directly applicable in the UK. Following the end of the Brexit transition period, the UK retained and transposed the Regulation (and the EU Torture Regulation) as applicable at that time into UK law,[3] meaning that it continued to operate in the UK effectively as it did prior to the end of the transition period (alongside pre-existing independent UK dual-use and military export controls). However, post-Brexit, the UK is now treated as a 'third country' from the perspective of EU export controls and vice versa (with the exception of Northern Ireland; see below). At the time of writing, the UK has not yet adopted equivalent changes as were implemented in the current, recast EU Dual-Use Regulation[4] (though these changes have been adopted with respect to Northern Ireland, and the UK has updated its strategic export control lists in line with international developments).

UK controlled items

In the UK, goods, software and technology subject to export controls (items) are consolidated and listed within the UK Strategic Export Control Lists.[5] This includes not only military and dual-use listed items, but also certain other lists, including torture equipment, non-military firearms and radioactive sources.

Given that the UK transposed Regulation (EC) No. 428/2009 into UK law, and remains a party to the same relevant international export control frameworks (i.e., the Wassenaar Arrangement, the Australia Group (chemical weapons), the Nuclear Suppliers Group and the Missile Technology Control Regime), the current UK and EU export control lists remain very closely aligned.

Dual-use exports between Great Britain and the European Union – requirement for export licences

As a result of Brexit, export licences are now required for the export of all controlled dual-use items between Great Britain (i.e., England, Scotland and Wales) and the European Union.

---

2 At that time, Regulation (EC) No. 428/2009.

3 Article 3(1) European (Withdrawal) Act 2018.

4 Regulation (EU) 2021/821.

5 UK Strategic Export Control Lists, June 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948279/uk-strategic-export-control-list.pdf.

The UK and the European Union both sought to mitigate the impact of this by issuing general licences that permit the export of dual-use items between Great Britain and the EU as follows:

- the UK's Export Control Joint Unit (ECJU) issued an Open General Export Licence for the export of dual-use items from and to EU Member States (as well as Iceland and the Channel Islands) (EU-27 OGEL);[6] and
- the EU added the UK to the Union General Export Authorisation EU001[7] (EU GEA 001), joining the eight existing territories to which the majority of EU dual-use items can be exported under this authorisation, namely Australia, Canada, Japan, New Zealand, Norway, Switzerland (including Liechtenstein) and the US.

The EU-27 OGEL and EU GEA 001 avoid the need for exporters to apply for specific individual licences for exports of dual-use items between Great Britain and the European Union. They also remove any waiting time for authorisation before proceeding with an export, as both licences simply require the exporter to register for their use. However, there is an increased administrative burden on exporters, given the need to comply with the relevant requirements under these licences, as follows.

- Registration: in the UK, exporters need to sign up to the UK's online export licence system (SPIRE) and register for the EU-27 OGEL; likewise, in EU Member States, exporters will also have to register with the relevant EU Member State authority if using the EU GEA 001 (with registration requirements varying, sometimes significantly, between those Member States).
- Licence conditions: exporters are also required to meet certain conditions under both the EU-27 OGEL and EU GEA 001, including record-keeping. Failure to do so can be a criminal offence, and could result in being restricted from using the licence in the future. Notably, the EU-27 OGEL does not apply in certain situations where an exporter knows that the final destination of the items concerned is outside the EU and no processing or working is to be performed within the EU (other than where the end destination would be covered by an existing UK licence available to the exporter).

---

6 Open General Export Licence: Export of Dual-Use items to EU Member States, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1062835/open-general-export-licence-export-of-dual-use-items-to-eu-member-states.pdf.

7 Regulation (EU) 2021/821.

- Audits: registration for the EU-27 OGEL will likely also result in the registrant being subject to audits by the UK ECJU.

Dual-use exports from the EU or UK to the rest of the world

Previously, exporters exporting dual-use goods from the EU or UK to the rest of the world (ROW) could apply for a licence in either the UK or another EU Member State and subsequently export from any country in the EU (subject to certain restrictions in respect of specific licences and the position of relevant EU Member State export authorities).

However, post-Brexit, this is no longer possible as:

- UK-issued export licences are no longer valid for exports from the EU to the ROW;
- EU Member States-issued export licences are no longer valid for exports from the UK to the ROW; and
- the 'exporter' (i.e., the entity that holds the relevant licence) must be established in the EU to export from the EU, and in the UK to export from the UK.

In certain cases, there may be applicable licensing requirements in both the UK and the EU. This may include situations where a UK exporter exports an item to the EU, knowing that the item will then be transferred to outside the EU – potentially triggering both UK and EU licensing requirements to the final destination. Given UK and EU rules on 'brokering' (including arranging the movement of items between third countries), there may also be situations where EU and UK export and brokering licensing requirements apply in parallel.

The impact of the Northern Ireland Protocol

Although the UK is treated as a third country from the perspective of EU export controls and vice versa, conversely, the now-updated EU Dual-Use Regulation continues to apply directly in Northern Ireland, pursuant to the Protocol on Ireland/Northern Ireland.[8]

The EU and UK agreed the Protocol on Ireland/Northern Ireland to prevent a hard border between Northern Ireland and the Republic of Ireland, by keeping Northern Ireland in the EU's single market for goods. This has an impact from a dual-use export control perspective. Whereas the older version of the EU

8 Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, Protocol on Ireland/Northern Ireland.

Dual-Use Regulation has continued to apply as 'retained EU law' in Great Britain, the updated version of the EU Dual-Use Regulation that applies in the EU applies in Northern Ireland.

Further changes may also be implemented in due course relating to transfers between Great Britain and Northern Ireland pursuant to the Windsor Framework, a political agreement in principle between the European Commission and the UK government.

Exports between Northern Ireland and the EU

The EU has made it clear that, in line with the Protocol on Ireland/Northern Ireland, exports between the EU and Northern Ireland are treated as intra-EU transfers in both directions and will not need a licence (other than in respect of items controlled under Annex IV to the EU Dual-Use Regulation or in respect of military-controlled goods). Therefore, the majority of dual-use goods being exported between Northern Ireland to the EU do not require an export licence.

Exports between Great Britain and Northern Ireland

The UK government has made it clear that there are no export licensing requirements to move dual-use items from Northern Ireland to GB, or vice versa.

Military export controls

As noted in Chapter 7, export controls in relation to military items are the preserve of each EU Member State. Consequently, the UK's departure from the EU did not have a material impact on the UK's military export regime, and the export of military items from the UK to the EU (and indeed between all EU Member States) still requires an export licence. UK Guidance also clarified that the position has not changed regarding Northern Ireland in respect of these controls.

The items subject to the UK's military export controls are set out in Schedule 2 of the UK's Export Control Order 2008[9] and are listed within the UK Strategic Export Control Lists.[10] This currently remains closely aligned with the EU common military list.

9 Export Control Order 2008 (SI 2008/3231) (as amended).

10 UK Strategic Export Control Lists, June 2021 (footnote 5).

Updated UK military end-use controls

With effect from 19 May 2022, the UK expanded its military export end-use control to capture non-listed dual-use items where (with certain exceptions) the exporter has been informed that the items may be intended for use by any military forces, para-military forces, police forces, security services or intelligence services of a country subject to an arms embargo. This supplements the pre-existing military and weapons of mass destruction (WMD)-related end-use controls, broadly aligned with those of the EU, as described in Chapter 7. At present, the UK has not extended its end-use controls to capture cyber-surveillance items intended for, or for use in connection with, internal repression or certain human rights abuses, as introduced in the recast EU Dual-Use Regulation (although these controls do apply for exports from Northern Ireland).

Consequences of non-compliance with UK export controls

The main enforcement body for export control in the UK is His Majesty's Revenue and Customs (HMRC). In addition to referring cases to the Crown Prosecution Service (CPS) for a potential prosecution, HMRC is also able to issue administrative penalties (sometimes known as 'compound' penalties) as a way of settling an investigation that it would otherwise refer to the CPS for a potential criminal prosecution. The power for HMRC to issue compound penalties is found in Section 152 of the Customs and Excise Management Act 1979. Compound penalties are sometimes made public in an anonymised form, and whether or not HMRC seeks to settle a breach by way of a compound penalty, or recommends a criminal prosecution, depends on a variety of factors.

In the UK, there are a number of criminal offences that may be triggered by an export control violation, depending on the nature of the breach. The majority of UK offences are set out in the Export Control Order 2008, in addition to the Customs and Excise Management Act 1979, and these fall into one of four categories:

- offences concerning prohibited or controlled goods. These offences relate to:
  - military goods;[11]
  - goods that may be used for purposes relating to WMD;
  - providing any technical assistance for the supply, delivery, manufacture or maintenance of WMD;[12]

11 See Export Control Order 2008, at Articles 34 and 3.

12 See id., at Articles 34 and 19.

    - supplying or delivering, or agreeing to supply or deliver, or doing anything to promote the supply or delivery of certain goods between any overseas country and embargoed destinations;[13] and
    - supplying or delivering, or agreeing to supply or deliver, or doing anything to promote the supply or delivery of Category A goods,[14] Category B goods[15] or Category C[16] goods from one third country to another third country (namely the items on the UK's control list of military items, categorised according to their sensitivity);
- offences concerning dual-use goods (i.e., dual-use items or any item that is usable for both civil and military purposes[17]);[18]
- offences concerning the Torture Regulation;[19] and
- offences concerned with making misleading statements for obtaining a licence.[20]

Although there are a number of offences that can be triggered by a breach, we have seen UK enforcement authorities increasingly use their administrative powers of settlement. For example, between January 2017 and December 2021, HMRC received 47 compound settlements totalling over £1.4 million; more recently, during November and December 2022, HMRC issued compound settlement offers to four UK exporters totalling over £3.6 million.

13 See id., at Articles 34 and 20.
14 See id., at Articles 34 and 21 and Schedule 1, Part 1 for Category A goods.
15 See id., at Articles 34 and 22 and Schedule 1, Part 2 for Category B goods.
16 See id., at Articles 34, 23 and 2(1) for Category C goods.
17 id., at Article 2(1).
18 id., at Article 35.
19 id., at Article 36 and 36A.
20 id., at Article 37.

CHAPTER 9

Export Controls in the United States

Meredith Rathbone and Ryan Pereira[1]

Introduction

The US government controls exports of sensitive equipment, software and technology for reasons of national security and foreign policy. Generally, the goals of US export controls are to (1) protect the national security of the United States by limiting access to the most sensitive US technology and weapons, (2) promote regional stability, (3) prevent the proliferation of weapons and technologies, and (4) protect human rights around the world.

US export controls frequently apply extraterritorially, extending US export controls compliance obligations to non-US persons. For example, an item of US origin can remain controlled under US laws even after its initial export, and require a licence or authorisation for reexport – or even transfer within a single country – from one non-US person to another non-US person. Even certain items produced outside the United States may be subject to US export controls if they are the direct product of certain technology, software or machinery of US origin. In other cases, items that are not of US origin can become subject to US jurisdiction if they contain more than 25 per cent (or in some cases even less) controlled US-origin components, technology or software.

This chapter provides an overview of the US export controls regimes, with a focus on the Export Administration Regulations (EAR),[2] administered by the US Department of Commerce's Bureau of Industry and Security (BIS), which controls dual-use items – meaning items that can be used for civil or military

---

1 Meredith Rathbone is a partner and Ryan Pereira is an associate at Steptoe & Johnson LLP. The authors are grateful to Hena Schommer for her significant contributions and insights as a co-author of earlier versions of this chapter.

2 15 Code of Federal Regulations (C.F.R.) § 730 et seq.

purposes – as well as certain less-sensitive defence articles, and the International Traffic in Arms Regulations (ITAR),[3] administered by the US Department of State's Directorate of Defense Trade Controls (DDTC), which controls 'defense articles' and 'defense services'.

In this fourth edition of *The Guide to Sanctions*, we note the continuing US trend of expanding the scope and applicability of US export controls rules targeting specific destinations, regions and end users in support of the US goals to protect US national security, promote regional stability and protect human rights. Since the first edition, we have seen a distinct broadening of the scope and applicability of US export controls. For example, in 2022, following Russia's invasion of Ukraine, expansive new US export controls were issued in relation to Russia and Belarus. The new rules impact numerous exports involving Russia and Belarus, including through: the imposition of new licence requirements for the export to Russia and Belarus of all items on the EAR's Commerce Control List (CCL); the expansion of jurisdiction to more foreign-produced items; and the introduction of specific military end user licence requirements.[4] In recent years, we have also seen an increased focus on coordination with other countries that have shared policy goals with the United States. For example, in 2023, on the one-year anniversary of Russia's invasion of Ukraine, BIS amended and expanded US export controls on items in certain industrial, chemical and luxury goods sectors.[5] The amendments are intended to better align US export controls with controls implemented by US allies and partners.

We also see a continued focus on China, which is another target of the expanded use of export controls. In recent years, the protection of human rights has also become an increasingly prominent element of US export controls policy. For example, in 2023, the United States issued a revised version of the US Conventional Arms Transfer (CAT) policy that articulates the framework under which the US government reviews and evaluates proposed arms transfers.[6] The revised CAT broadens the range of human rights-related harms considered in

3 22 C.F.R. § 120 et seq.

4 See Expansion of Sanctions Against Russia and Belarus Under the Export Administration Regulations (EAR), 87 Fed. Reg. 22130 (8 April 2022); Implementation of Additional Sanctions Against Russia and Belarus Under the Export Administration Regulations (EAR) and Refinements to Existing Controls, 87 Fed. Reg. 57068 (15 September 2022).

5 Implementation of Additional Sanctions Against Russia and Belarus Under the Export Administration Regulations (EAR) and Refinements to Existing Controls, 88 Fed. Reg. 12175 (24 February 2023).

6 Memorandum on United States Conventional Arms Transfer Policy, National Security Memorandum/NSM-18 (23 February 2023).

connection with potential arms transfers and also strengthens a restriction on arms transfers that could contribute to atrocity crimes, lowering the standard from 'actual knowledge' that arms would be used to commit atrocities to a commitment not to transfer arms that would 'more likely than not'[7] contribute to atrocity crimes, including but not limited to genocide, crimes against humanity and the intentional targeting of civilian objects or civilians. In addition, in 2023, BIS amended the criteria for Entity List designations to confirm its position that 'the protection of human rights' is a foreign policy interest considered in assessing whether the activities of an entity are 'contrary to the national security or foreign policy of the United States'.[8] BIS has also issued guidance formalising its policy of providing for enhanced consideration of human rights concerns when reviewing almost all licence applications.[9] The guidance also sets forth BIS's expectation that exporters will exercise due diligence when submitting a licence application that may implicate human rights concerns and provides resources to help exporters assess whether a proposed export is destined for countries, end users and end uses that may implicate human rights concerns.[10]

The US government has continued to prioritise engagement with the private sector and universities as a means to support export compliance and prevent circumvention of US and allied export controls. In 2022, BIS announced the Academic Outreach Initiative, which prioritised engagement with universities that either possess ties to foreign universities on the Entity List, host a strategic Department of Defense University Affiliated Research Center or conduct research in sensitive technologies subject to the EAR.[11] Through this initiative, these universities have been assigned a specific agent from their local BIS office to help with export compliance. In addition, BIS has provided guidance to the private sector on red flags of potential Russian and Belarusian export control

7 ibid.

8 Additions to the Entity List; Amendment To Confirm Basis for Adding Certain Entities to the Entity List Includes Foreign Policy Interest of Protection of Human Rights Worldwide, 88 Fed. Reg. 18983 (28 March 2023).

9 Bureau of Industry and Security, Human Rights FAQs (March 2023).

10 ibid.

11 Matthew S Axelrod, Memorandum for All Export Enforcement Employees: 'Addressing the National Security Risk that Foreign Adversaries Pose to Academic Research Institutions' (28 June 2022).

evasion attempts.[12] The above reflects an ongoing effort by the US government to enable the private sector and academic institutions to support compliance with US export controls.

As discussed in other US-related chapters in this Guide, the United States Department of the Treasury's Office of Foreign Assets Control (OFAC) also restricts the export of items to certain destinations and entities. Sometimes there is overlapping jurisdiction between OFAC sanctions programmes and other US export control regimes, such as the EAR. In some cases, a licence may be required from one or even multiple authorities to export items subject to US jurisdiction, particularly to embargoed destinations. It is important to determine which US export control regimes may apply to a specific transaction and assess licensing requirements accordingly.

Various other US government entities also play a role in administering US export controls, including the US Department of Commerce's Census Bureau, which is responsible for ensuring the accuracy of the trade control data reporting; the Nuclear Regulatory Commission and the Department of Energy, which regulate exports relating to nuclear items and technology; the Federal Emergency Management Agency, which is more recently responsible for overseeing exports of personal protective equipment from the United States; and the US Patent and Trademark Office, which administers regulations overseeing exports of technology in connection with patent applications and related filings.[13] Additional information about other US government agencies and offices with export control responsibilities is available at the BIS website.[14]

Export Administration Regulations

The EAR,[15] administered by BIS, control the export, reexport or transfer (in-country) of certain items of US origin and, in some cases, of non-US origin. The EAR's CCL[16] sets out a technically focused list of goods, software and technology with varying levels of controls based on a variety of national security and

12 'FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts', FIN-2022-Alert003 (28 June 2022).

13 See 37 C.F.R. Part 5.

14 See www.bis.doc.gov/index.php/about-bis/resource-links.

15 15 C.F.R. § 730 et seq. The Export Control Reform Act (ECRA), 50 U.S.C. §§ 4801–4852 (2018), became law on 13 August 2018 and provides the permanent statutory authority for the EAR.

16 15 C.F.R. § 744 (Supplement 1).

foreign policy reasons and the country of destination. Apart from the CCL-based controls, the EAR also control the export of certain items to restricted destinations, end uses and end users. BIS has various offices dedicated to overseeing technical review, licensing, providing support to exporters, and investigating and enforcing potential regulatory violations.[17]

Scope of the EAR

The EAR apply to items that are in the United States, items of US origin, wherever located, foreign-produced items that contain more than a *de minimis* amount of controlled US-origin content, and items that are the direct product of certain US-origin technology or software. The EAR also apply to US person activities in certain circumstances. For example, in 2022, the US government implemented new restrictions on US person activities in support of certain semiconductor activities in China.[18] This means that both US and non-US persons and companies may have compliance obligations under the EAR, and both US-origin and foreign-produced items may be subject to the EAR.

Items subject to the EAR

All items physically located in the United States are subject to the EAR, including hardware, software and technology, and remain subject to the EAR after export[19] from the United States, for reexport and transfer (in-country), with some exceptions. An item subject to the EAR that is sent from one foreign country to another foreign country is a 'reexport'.[20] In relation to this, a 'transfer (in-country)'[21] under the EAR is a change in end use or end user within the same foreign country, which could trigger a licensing obligation. In some cases, items in the United States, such as technology, can be considered exported even though the technology has not left the United States, if it is transferred to a non-US person located in the United States. This is referred to as a 'deemed export'.[22] The EAR

17 An organisation chart is available from the US Department of Commerce's Bureau of Industry and Security (BIS), at www.bis.doc.gov/index.php/documents/about-bis/692-bis-organization-chart/file.

18 15 C.F.R. § 744.6.

19 The term 'export' is defined at 15 C.F.R. § 734.13(a) and includes: 'An actual shipment or transmission out of the United States, including the sending or taking of an item out of the United States, in any manner.'

20 15 C.F.R. § 734.14.

21 15 C.F.R. § 734.16.

22 See 15 C.F.R. § 734.13(a)(2).

further clarify: 'Any release in the United States of "technology" or source code to a foreign person is a deemed export to the foreign person's most recent country of citizenship or permanent residency.'[23]

Some items in the United States are not subject to the EAR; these are discussed further below. Additionally, there are foreign products that are subject to the EAR in certain circumstances if the foreign-produced item contains more than a *de minimis*[24] amount of controlled US content (the De Minimis Rule), and certain foreign produced items that are the direct product[25] of US-origin technology and software that is controlled for national security reasons, or are produced by a complete plant or a 'major component' of a plant that is the direct product of that technology or software (the Foreign-Produced Direct Product Rule).[26] In 2020, the Foreign-Produced Direct Product Rule was modified to specifically target certain companies on the Entity List by expanding the scope of non-US origin (i.e., foreign-produced) items that are subject to US export licensing requirements when being transferred to, or for use by, the relevant Entity List entities.[27] In 2022, a new Russia/Belarus Foreign Direct Product (FDP) Rule and a Russia/Belarus-Military End User FDP Rule[28] were implemented. These new rules apply to an expanded scope of foreign-produced items destined for Russia and Belarus. In 2023, a new Iran Foreign Direct Product Rule[29] was implemented to address the use of Iranian Unmanned Aerial Vehicles by Russia in its war against Ukraine. The new Rule applies to foreign-produced items identified in new Supplement No. 7 to Part 746 of the EAR when they are destined for Russia, Belarus or Iran, as well as to certain foreign-produced items specified in any Export Control Classification Number (ECCN) Categories 3 to 5 or 7 on the CCL when destined for Iran.

---

23 15 C.F.R. § 734.13(b).

24 See 15 C.F.R. § 734.3.

25 See 15 C.F.R. § 734.3(a)(4).

26 See 15 C.F.R. §§ 734.3(a)(4)–(5) and 734.9.

27 See EAR: Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule), 85 Fed. Reg. 51,596 (20 August 2020); Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List, 85 Fed. Reg. 29,849 (19 May 2020).

28 See 15 C.F.R. § 734.9(f) and (g).

29 See Export Control Measures Under the Export Administration Regulations (EAR) To Address Iranian Unmanned Aerial Vehicles (UAVs) and Their Use by the Russian Federation Against Ukraine, 85 Fed. Reg. 12155 (24 February 2023).

Items not subject to the EAR

Items not subject to the EAR include those that are under the exclusive jurisdiction of another US government agency; certain publications, including books, newspapers and periodicals; and information and software that are published, arise during, or result from, fundamental research, are released in an academic institution course (in certain circumstances) or appear in published patent applications.[30]

EAR basics

The EAR can be a complex area of US export controls. We provide the basics of the EAR below; further background details regarding the EAR can be found in Part 732 of the EAR, 'Steps for Using the EAR'.[31]

To determine obligations under the EAR, first, basic information regarding the transaction must be determined.

- What is it? Knowing an item's classification on the CCL is an important first step to determining obligations under the EAR.
- Where is it going? The country of ultimate destination often determines the licence requirements under the EAR.
- Who will receive it? It is important to screen the end users to confirm that they are not restricted, and to determine whether certain licence exceptions may apply.
- What will they do with it? Certain end uses can independently trigger licensing requirements under the EAR.
- What else does the end user do? Some activities, such as proliferation activities, undertaken by end users may prevent dealings with them.[32]

The General Prohibitions at Part 736 of the EAR set out various restrictions applicable to the export of items subject to the EAR. General Prohibitions one to ten[33] cover a broad set of prohibited activities touching on almost all aspects of the EAR, including exports or reexports to prohibited end uses or end users (General Prohibition Five); exports or reexports to embargoed destinations (General Prohibition Six); and proceeding with a transaction with knowledge that a violation has occurred or is about to occur (General Prohibition Ten). General Prohibition Ten can particularly affect non-US companies, especially if they have

30 See 15 C.F.R. § 734.3(b) for a complete list of items that are not subject to the EAR.

31 15 C.F.R. Part 732.

32 See 15 C.F.R. § 732.1(b).

33 www.bis.doc.gov/index.php/documents/regulation-docs/413-part-736-general-prohibitions/file.

items in their possession that may have been involved in violations of the EAR. In some cases, authorisation from BIS may be needed prior to the return, disposal or any other dealings in items subject to the EAR if there is knowledge that a violation has or is about to occur in relation to those items.[34] In 2021 and 2022, BIS expanded the scope of General Prohibition Seven.[35] The rule imposes additional licence requirements under the EAR for US persons that are involved in a broad array of activities related to proliferation activities and certain military intelligence end uses or end users in China, Russia, Venezuela, Belarus, Myanmar and other US embargoed destinations.

Jurisdiction

Jurisdiction is a threshold question in determining whether an item is subject to the EAR. For purposes of the EAR, an item may be subject to the EAR unless it is under the exclusive control of another US regime, such as military items that are controlled under the ITAR. In that sense, the EAR are something of a catch-all regime. Items subject to the EAR also include:

- all items located in the United States;
- items moving in transit through the United States;
- all US-origin items wherever located;
- foreign-made items that incorporate more than a *de minimis* amount of controlled US-origin content; and
- foreign-made items that are the foreign-produced direct product of certain US-origin technology or software.[36]

Classification

If an item is subject to the jurisdiction of the EAR, a review of the CCL should be conducted to determine whether the item is listed. The CCL contains a (mostly) positive list of items used by BIS to identify more sensitive dual-use or civil items, as well as some less sensitive defence articles not falling within ITAR control that BIS controls for export, reexport or retransfer. The CCL entries contain technical parameters that often require the review of technical experts to make a

34 See 15 C.F.R. § 736.2(b)(10).

35 See 15 C.F.R. § 736.2(b)(7). See also Federal Register: Expansion of Certain End-Use and End-User Controls and Controls on Specific Activities of U.S. Persons, 86 Fed. Reg. 4865 (15 January 2021) and 86 Fed. Reg. 18433 (9 April 2021); Imposition of Sanctions Against Belarus Under the Export Administration Regulations (EAR), effective 2 March 2022, 87 Fed. Reg. 13048 (8 March 2022).

36 See 15 C.F.R. § 734.3(a) for a complete list of items that are subject to the EAR.

determination. The CCL entries are identified by ECCNs, which are denoted by a five-digit alphanumeric reference. They begin with a number between zero and nine, indicating the general category of the item that is controlled (e.g., electronics, computers and information security); followed by a letter identifying the product group of the item (e.g., software and technology); followed by a final three digits that indicate the type or reason for control (e.g., missile technology, nuclear non-proliferation and Wassenaar Arrangement Munitions List).[37]

If an item is determined to be subject to the jurisdiction of the EAR but is not listed on the CCL, it is classified as EAR99, which is a catch-all classification. In general, EAR99 items may be exported to most destinations without a licence. However, key exceptions are detailed in the EAR, including where a General Prohibition applies. For example, an EAR99 item may not be exported without a licence to certain restricted destinations, for certain prohibited end uses or to certain prohibited end users.[38] Currently, the destinations that are subject to heightened restrictions under the EAR include Iran, North Korea, Syria, Cuba, Iraq, Russia and the Crimea and so-called 'Donetsk People's Republic' and 'Luhansk People's Republic' regions of Ukraine.[39]

Licence determination and licence exceptions

Determining whether a licence is required is a key step under the EAR, as the regime only requires a licence for certain exports. For items listed in an ECCN, it must be determined whether the item is controlled for the end destination as specified in the ECCN entry on the CCL and detailed in the Commerce Country Chart.[40] The Commerce Country Chart identifies the 'reasons for control' of the items and cross-references the reasons for control with each potential destination country. If the end destination is not subject to the ECCN's reason for control

37 For more guidance, visit BIS's website or review the BIS presentation on how to classify your item, at www.bis.doc.gov/index.php/documents/compliance-training/export-administration-regulations-training/247-howtoclassifyitem-pdf/file.

38 See, generally, C.F.R. § 736.2. The General Prohibitions provide the framework for restrictions on activities or circumstances when a licence may be required.

39 See 15 C.F.R. Part 746. This part of the EAR, 'Embargoes and Other Special Controls', imposes comprehensive and targeted controls.

40 15 C.F.R. § 738 (Supplement 1).

then a licence is not required for reasons based on the product's classification and the end destination. In 2020, BIS changed its treatment of Hong Kong under the EAR, and Hong Kong is now subject to the same licence requirements as China.[41]

A licence may also be required if one of the 10 General Prohibitions is triggered. As noted above, General Prohibitions can trigger licence requirements, even for EAR99 items not otherwise subject to a licence requirement under the EAR, if they involve a restricted end use or end user, among other things. For example, General Prohibition Nine specifically prohibits violations of any order, term or condition of a licence or licence exception.[42] General Prohibition Five prohibits knowingly exporting or reexporting any items subject to the EAR to or for a prohibited end user or end use as described in Part 744 of the EAR. For example, certain exports to military end users and for military end uses are prohibited under Section 744.21 of the EAR (the MEU Rule).[43] In 2020 and 2021, the MEU Rule was revised and broadened in scope and application to military end users and for military end uses in Myanmar, China, Russia and Venezuela.[44] A non-exhaustive Military End-User List (the MEU List) was also added.[45] In 2022, the new Section 746.8 (Sanctions Against Russia and Belarus) was added to the EAR, containing expansive new US export control licence requirements applicable to exports, reexports or in-country transfers to these destinations.[46]

41 See Federal Register: Removal of Hong Kong as a Separate Destination under the Export Administration Regulations, 85 Fed. Reg. 83,765 (23 December 2020); Revision to the Export Administration Regulations: Suspension of License Exceptions for Hong Kong, 85 Fed. Reg. 45,998 (31 July 2020).

42 See 15 C.F.R. § 736.2(b)(9).

43 See 15 C.F.R. §§ 736.2(b)(5) and 744.21.

44 See Federal Register: Expansion of Export, Reexport, and Transfer (in-Country) Controls for Military End Use or Military End Users in the People's Republic of China, Russia, or Venezuela, 85 Fed. Reg. 23,459 (28 April 2020); Expansion of Export, Reexport, and Transfer (in-Country) Controls for Military End Use or Military End Users in the People's Republic of China, Russia, or Venezuela (Correction), 85 Fed. Reg. 34,306 (3 June 2020); Burma: Implementation of Sanctions, 86 Fed. Reg. 13,173 (8 March 2021).

45 See EAR: Addition of 'Military End User' (MEU) List to the Export Administration Regulations and Addition of Entities to the MEU List, 85 Fed. Reg. 83,793 (23 December 2020).

46 See 15 C.F.R. § 746.8. See also, Federal Register: Implementation of Sanctions Against Russia Under the Export Administration Regulations (EAR), 87 Fed. Reg. 12226 (24 February 2022); Imposition of Sanctions Against Belarus Under the Export Administration Regulations (EAR), 87 Fed. Reg. 13048 (8 March 2022).

With limited exceptions, BIS reviews applications for the export, reexport or transfer (in-country) of any item requiring a licence pursuant to Section 746.8 under a policy of denial.[47]

As a final step, if a licence appears to be required under the EAR for the export, reexport or transfer of an item, the licence exceptions at Part 740 of the EAR should be reviewed to determine whether any of the licence exceptions may apply. The application of an EAR licence exception is fact-specific; each exception varies in application and has detailed compliance requirements.

BIS lists of parties of concern

BIS has three lists of parties of concern.[48] Inclusion on these lists can have a dramatic effect on the listed parties' ability to lawfully obtain items subject to US jurisdiction.

The BIS Entity List prohibits the listed entities from being a 'party to a transaction'[49] when receiving, using, purchasing or acting as intermediate consignee, for some or all items subject to the EAR without a licence.[50] The Entity List has been increasingly used in recent years against entities determined to be acting contrary to US national security or foreign policy interests, including the protection of human rights worldwide.[51] For instance, in 2023, 11 entities were added to the Entity List for their alleged involvement in human rights violations and abuses in Burma, China, Nicaragua and Russia.[52]

The Denied Persons List is a list of individuals and entities that have been denied export privileges from the United States.[53] An order to deny export privileges generally restricts the ability of the named party to participate in export and reexport transactions that involve, or restrict access to, items subject to the EAR.

---

47 See 15 C.F.R. § 746.8.

48 BIS, Lists of Parties of Concern, www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern.

49 BIS clarified its position in August 2020 here: Clarification of Entity List Requirements for Listed Entities When Acting as a Party to the Transaction Under the Export Administration Regulations (EAR), 85 Fed. Reg. 51,335 (20 August 2020).

50 See 15 C.F.R. Part 744 (Supplement 4), Entity List.

51 Additions to the Entity List; Amendment To Confirm Basis for Adding Certain Entities to the Entity List Includes Foreign Policy Interest of Protection of Human Rights Worldwide, 88 Fed. Reg. 18983 (28 March 2023).

52 ibid.

53 See, generally, 15 C.F.R. Part 766.

Finally, the Unverified List (UVL) is a 'list of parties whose bona fides BIS has been unable to verify'.[54] BIS conducts end-use and end-user visits all over the world via its export enforcement officers (EEO), who are embedded at US embassies. Generally, if an EEO is unable to verify an end user or the end use of an item that was previously exported to a non-US party under a BIS licence, the party is placed on the UVL. In 2022, BIS clarified that a sustained lack of cooperation by the host government in a country where an end-use check is to be conducted that effectively prevents BIS from determining compliance with the EAR, will be grounds for adding an entity to the Entity List.[55] No licence exceptions may be used to export to UVL parties and a UVL statement must be obtained before shipping anything subject to the EAR (even if not subject to a licence requirement).[56] The UVL statement must include the name of the UVL party, its complete physical address, an end-use statement and a commitment to cooperate with BIS's end-use checks.[57] In 2023, 14 persons in China were added to the UVL because BIS was unable to verify the persons' bona fides or complete an end-use check.[58]

Extraterritorial aspects of the EAR

In addition to the foregoing discussion regarding reexports or transfers of unchanged or unmodified US-origin items that remain subject to the EAR, wherever located, we highlight a few other key extraterritorial aspects of the EAR.

The De Minimis Rule

The De Minimis Rule described in Part 734 of the EAR requires that certain foreign-produced items that incorporate controlled items of US origin be subject to the EAR if the percentage of controlled US-origin content is over 25 per cent or (for some countries) 10 per cent. There are a few items that are not eligible for the De Minimis Rule, such as some types of computers and certain encryption technology. General Prohibition Two prohibits the reexport and export from abroad of foreign-made items incorporating more than a *de minimis* amount of

54 BIS, Lists of Parties of Concern (footnote 48).

55 See Revisions to the Unverified List; Clarifications to Activities and Criteria That May Lead to Additions to the Entity List, 87 Fed. Reg. 61971 (7 October 2022).

56 15 C.F.R. § 744.15(b).

57 ibid.

58 See Federal Register: Revisions to the Unverified List, 88 Fed. Reg. 17706 (24 March 2023).

controlled US content. Non-US companies should be aware of the potential compliance obligations under the EAR of incorporating controlled US-origin content into foreign-made items.

Foreign-Produced Direct Product Rule

The Foreign-Produced Direct Product Rule is found in Part 734.3(a), Paragraphs (4) and (5) of the EAR. The Foreign-Produced Direct Product Rule applies to certain foreign-made items that are the direct product of certain US-origin technology or software described in General Prohibition Three.[59] General Prohibition Three also applies to certain items produced in a plant or by a major component of a plant outside the United States that are the direct product of certain technology or software of US origin. It is important to understand that items produced outside the United States may, in some cases, be caught by the Foreign-Produced Direct Product Rule under the EAR and be subject to US export controls. In 2022, BIS added two new foreign direct product rules targeting Russia and Belarus, including the addition of the Russia/Belarus-Military End User FDP Rule.[60] BIS also significantly expanded the scope of items subject to the Foreign-Produced Direct Product Rule restrictions for 28 existing Entity List entities located in China, and established two new foreign direct product rules for 'supercomputers',[61] advanced computing integrated circuits and computer commodities that contain integrated circuits that are exported, reexported or transferred (in-country) to or within China or Hong Kong.[62] In 2023, these controls were expanded to Macau because of the potential risk of diversion of items subject to the EAR from Macau to China.[63]

---

59 See 15 C.F.R. § 736.2(b)(3).

60 15 C.F.R. § 734.9(f) and (g).

61 A 'supercomputer' is defined as a 'computing "system" having a collective maximum theoretical compute capacity of 100 or more double-precision (64-bit) petaflops or 200 or more single-precision (32-bit) petaflops within a 41,600 ft3 or smaller envelope.' 15 C.F.R. § 772.1.

62 Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification, 87 Fed. Reg. 62186 (7 October 2022).

63 Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification; Updates to the Controls To Add Macau, RIN 0694–AI94 (17 January 2023).

EAR export compliance programme

An effective BIS export compliance programme (ECP) is crucial to any company that interacts with items of US origin or items subject to the EAR. As demonstrated above, the EAR are a complex regime and require a tailored and targeted compliance programme to ensure that appropriate regulatory compliance processes and procedures are in place. Compliance programmes should be tailored to the risk faced by a company. For example, two non-US based companies may have different needs depending on their exposure to items subject to the EAR. Other relevant factors include a company's industry, its geographic reach, its workforce, its customers and the size and frequency of its transactions. BIS provides several resources on BIS compliance programmes on its website, including elements of an ECP, export compliance guidelines and other background documents.[64] The EAR also contain resources (in Part 732), including an export control decision tree, know-your-customer guidance and red flags at Supplement Nos. 1 and 3, respectively. Proactively identifying US export control risks in a company and establishing a targeted export compliance programme that fits its business is a first step to preventing future violations and identifying potential past problematic transactions.

International Traffic in Arms Regulations

US export controls on most defence articles and defence services are regulated by the ITAR,[65] administered by DDTC.[66] The ITAR implement the Arms Export Control Act[67] and regulate temporary and permanent exports, as well as temporary imports, of defence articles on the United States Munitions List (USML), defence services, and brokering of defence articles and services. The ITAR also contain reporting requirements for certain political contributions, fees or commissions.

Virtually every item subject to the ITAR requires a licence for export, reexport or transfer from DDTC, unless an ITAR exemption applies.

DDTC has offices focused on licensing, policy, and compliance and enforcement.[68]

---

64 See BIS website for further information, at www.bis.doc.gov/index.php/compliance-a-training/export-management-a-compliance/compliance.

65 See 22 C.F.R. Parts 120–130.

66 See www.pmddtc.state.gov/ddtc_public.

67 See 22 U.S.C. § 2778. The Arms Export Controls Act of 1976, as amended (AECA) is the primary statutory authority for the International Traffic in Arms Regulations (ITAR).

68 www.pmddtc.state.gov/ddtc_public?id=ddtc_public_portal_org_chart.

Scope of the ITAR

Similar to the EAR, the ITAR cover a broad array of items. In understanding the ITAR it is helpful to have an overview of certain key terms, set out below.

'Defense article'

A 'defense article' is any item or technical data designated in the USML,[69] typically having a military, satellite or intelligence application or purpose. It includes 'forgings, castings, and other unfinished products, such as extrusions and machined bodies, that have reached the stage in manufacturing where they are clearly identifiable by mechanical properties, material composition, geometry, or function as defense articles'.[70]

It also includes 'technical data'[71] recorded or stored in any physical form that reveal technological information directly related to USML items, or 'software' directly related to 'defense articles'. Specifically, the technical data definition captures information 'required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation'.[72] Technical data does not include information relating to general scientific, mathematical or engineering principles commonly taught at education institutions; information in the public domain,[73] or basic marketing information on function or purposes or general system descriptions of 'defense articles'.[74] Neither does it include technical data that has been approved for public release by the responsible US government agency.[75]

---

69 See 22 C.F.R. Part 121.

70 22 C.F.R. § 120.31.

71 22 C.F.R. § 120.33.

72 ibid. The technical data definition also includes: classified information relating to 'defense articles' and 'defense services' (and some items controlled on the EAR's Commerce Control List); information covered under an invention secrecy order; and software related to 'defense articles'. See id., at § 120.33(a), Paragraphs (2)–(4).

73 See 22 C.F.R. § 120.33(b). Generally, items in the public domain are public information, which is published, generally accessible or available to the public through news sources, libraries, unlimited distribution at conferences and trade shows, and available through unlimited distribution, not necessarily in published form, including fundamental research, as described in § 120.34(a)(8).

74 See 22 C.F.R. § 120.31(b).

75 The agency responsible for these reviews is the Department of Defense, Defense Office of Prepublication and Security Review; more information is available at www.esd.whs.mil/DOPSR/.

'Defense service'

A 'defense service'[76] is defined to include (1) the furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarisation, destruction, processing or use of 'defense articles'; (2) the furnishing to a foreign person of any technical data controlled under the ITAR, whether in the United States or abroad; and (3) military training of foreign units and forces, broadly defined.

US persons and foreign persons

A US person is defined under the ITAR as a person who is a lawful, permanent US resident or protected individual as defined in US law, and corporations or other entities that are incorporated to do business in the United States, and any government (federal, state or local) entity.[77]

A foreign person, as defined in the ITAR, is 'any natural person who is not a lawful permanent resident' or certain other protected individuals (such as certain refugees or asylees) under US law, as well as foreign companies and other entities that are not incorporated or organised to do business in the United States. International organisations, foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions) are also considered foreign persons under the ITAR.[78]

Items subject to the ITAR

USML

Identifying whether an item is on the USML[79] is the first step in determining what ITAR controls may apply to the export or transfer of that item. There are 21 categories of 'defense articles' described on the USML, including certain military electronics, launch vehicles, guided missiles and personal protective equipment. Within each category, the USML describes the types of 'defense articles', technology and software controlled, in general by describing, for each category, the controlled: end items; major systems and equipment; parts components, accessories and attachments; and technical data and 'defense services' relating to the USML category. Certain USML items and related technical data are identified

76 See 22 C.F.R. § 120.32.

77 See 22 C.F.R. § 120.62 for the definition of 'person' under the ITAR.

78 22 C.F.R. § 120.63.

79 See 22 C.F.R. § 121.1.

as significant military equipment[80] and are subject to more stringent controls.[81] Certain items on the USML are controlled only if they are 'specially designed' for a certain purpose, and must be assessed according to specified criteria as set out in the ITAR.[82] Non-US origin items containing content subject to the ITAR will typically be subject to ITAR jurisdiction through the 'see-through' rule.[83]

If it is unclear whether an item is controlled under the ITAR, an exporter may seek a commodity jurisdiction determination (CJ determination) from DDTC. A CJ determination is submitted to DDTC via its online application system and may involve review by several US government agencies, including BIS and the Department of Defense, and any other agencies relevant to the specific application. Some CJ determinations are available on DDTC's website.[84]

Registration requirements

The US government maintains registration requirements for (1) any person who engages in the United States in the business of manufacturing or exporting or temporarily importing 'defense articles' or furnishing 'defense services'[85] and (2) any US person, wherever located, any foreign person located in the United States and any foreign person located outside the United States that is owned or controlled by a US person that is performing brokering activities (defined to mean any action on behalf of another to facilitate the manufacture, export, permanent import, transfer, reexport or retransfer of a US or foreign 'defense article' or 'defense service', regardless of its origin).[86] Note that manufacturers of 'defense articles' located in the United States are required to register with DDTC, even if they do not export any of their products.[87] Registration is required to be renewed annually and comes with various notification requirements to DDTC, such as the requirement to notify DDTC within five days of any material change to the information contained in the registration statement (e.g., changes in senior

80 See 22 C.F.R. § 121(a)(2).
81 See 22 C.F.R. § 120.41.
82 ibid.
83 See 22 C.F.R. § 121.11(c).
84 The US Department of State's Directorate of Defense Trade Controls' (DDTC) website contains more information regarding commodity jurisdiction determinations, at www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=%20249f7c0adb6cf7007ede365e7c9619fd.
85 See 22 C.F.R. § 122.1 (registration requirements for manufacturers and exporters).
86 See 22 C.F.R. § 129.3 (registration requirements for brokering activities subject to the ITAR).
87 See 22 C.F.R. § 122.1(a).

management or business structure)[88] as well as a 60-day notification in advance of a sale or transfer of ownership or control to a foreign person.[89] Registration with DDTC does not authorise the export of 'defense articles'. Registration, rather, is a prerequisite to submission of a licence or eligibility to use an ITAR exemption.

Exports

Export of 'defense articles'

Any person intending to export, or temporarily import, a 'defense article', including hardware, software or technical data, must obtain authorisation from DDTC prior to the transaction, unless an exemption or exception applies. Additionally, DDTC authorisation is required to transfer technical data in the United States to a foreign person, and to reexport, resell, transfer, trans-ship or dispose of ITAR-controlled items, to a new non-US end user, end use or destination, unless authorised by DDTC under a licence or other form of authorisation, exemption or exception. DDTC licences and other specific authorisations discussed below must be applied for, and come with defined time periods, strict limitations and requirements regarding compliance. Exemptions may be used by an exporter without submitting a specific application to DDTC provided all the requirements of the exemption are met. ITAR exemptions can be nuanced; a careful review of the requirements of an exemption should be undertaken to ensure all compliance responsibilities and requirements are understood and met before proceeding. In addition, DDTC has other vehicles for authorising certain activity. For example, 'general correspondence' letters are often used to authorise reexports or retransfers from abroad. In addition, DDTC uses 'technical assistance agreements' to authorise certain instances in which US persons are providing non-US persons with continuing technical assistance; for example, to provide 'defense services' or to support certain design, development or manufacturing activity. DDTC uses 'manufacturing licence agreements' to authorise the granting of a licence to a non-US entity to manufacture ITAR-controlled items, such as items manufactured using ITAR-controlled technical data.

In addition, DDTC has published Open General Licenses (OGL) Nos. 1 and 2, which authorise certain persons in Australia, Canada and the United Kingdom to reexport or retransfer certain types of 'defense articles', services and technical

88 See id., at § 122.4(a).

89 See id., at § 122.4(b).

data controlled under the ITAR between and among the three countries.[90] These OGLs are valid until 31 July 2026 and are intended to facilitate defence trade between the US and these three key allies. A careful review of the requirements of the OGLs should be undertaken to ensure all compliance responsibilities and requirements are understood and met before proceeding with a reexport or retransfer.

Part 126.1 – proscribed countries

It is DDTC's policy to deny licences and other authorisations for exports and temporary imports of 'defense articles' and 'defense services' involving countries listed in Part 126.1 of the ITAR.[91] These countries are proscribed for various reasons, including being the subject of a United Nations arms embargo or as countries determined by the US Secretary of State to be state sponsors of terrorism. At the time of writing, exports to the following proscribed countries are subject to a licensing policy of denial: Belarus, Myanmar, China, Cuba, Iran, North Korea, Syria and Venezuela.[92] There are additional countries at ITAR Section 126.1(d)(2), to which Russia was added in 2021, that are not authorised to receive ITAR-controlled items, except as specifically detailed in that Section of the ITAR.

Brokering and political contributions under the ITAR

Brokering

In addition to the controls described above, the ITAR also control 'brokering' of 'defense articles' and 'defense services'.[93] In addition to covering the 'brokering activities' of US persons, the ITAR brokering restrictions can cover the activities of non-US persons – particularly of foreign persons located in the United States, and foreign persons who are owned or controlled by a US person.[94] Brokering activities include, but are not limited to: 'financing, insuring, transporting, or freight forwarding defense articles and defense services; soliciting, promoting,

90 See ITAR: Issuance of Open General Licenses 1 and 2, 87 Fed. Reg. 43366 (20 July 2022); see also, DDTC Issuance and Publication of Open General License Pilot Program Extended Validity Period (27 March 2023).

91 See 22 C.F.R. § 126.1, see also 22 C.F.R. §§ 126.2 and 126.3 for suspension, modification or exceptions that may be granted by the Deputy Assistant Secretary for Defense Trade Controls.

92 id., at 126.1(d)(1).

93 See 22 C.F.R. Part 129.

94 id., at § 129.2.

negotiating, contracting for, arranging, or otherwise assisting in the purchase, sale, transfer, loan, or lease of a defense article or defense service'.[95] An entity that engages in brokering activities subject to the ITAR may be subject to registration and reporting requirements. There are some carve-outs to the brokering restrictions, including in relation to activities by US persons in the United States that are limited exclusively to US domestic sales not intended for export, US government employees acting in their official capacity, and regular employees acting on behalf of an employer, subject to certain limitations.[96]

Part 130 – political contributions, fees and commissions

The ITAR contain reporting requirements for political contributions, fees or commissions 'offered, or agreed to pay, related to any sale for which a licence or approval is requested'.[97] Generally, these rules apply to certain authorisations under the ITAR valued at US$500,000 or more and 'being sold commercially to or for the use of the armed forces of a foreign country or international organization'.[98] Suppliers contracting with the Department of Defense for the sale of 'defense articles' or 'defense services' also have reporting requirements under Part 130.[99]

ITAR compliance programme

An effective ITAR compliance programme (ICP) is crucial to any company that interacts with 'defense articles', 'defense services' and ITAR-controlled technical data. In 2022, DDTC issued new ITAR Compliance Program Guidelines outlining DDTC's expectations for an effective ICP.[100] The ITAR Compliance Program Guidelines are similar to compliance programme guidelines issued by other federal agencies such as OFAC and BIS, although the ITAR Compliance Program Guidelines also provide guidance on ITAR-specific topics such as the DDTC Registration requirement and Part 129 and Part 130 record-keeping and reporting obligations. Proactively identifying ITAR compliance risks in a company and establishing a targeted ICP that fits its business is a first step to preventing future violations and identifying potential past problematic transactions.

---

95 id., at § 129.2(b)(1), Paragraphs (i) and (ii).

96 See id., at §§ 129.2(b)(2) and 126.18, for further details regarding exemptions for intra-company, intra-organisation and intra-governmental transfers.

97 See id. at § 130.9(a)(1).

98 id., at § 130.2.

99 See id., at §§ 130.7 and 130.9(b).

100 ITAR Compliance Program Guidelines, Bureau of Political-Military Affairs Directorate of Defense Trade Controls.

Enforcement

Both US persons and non-US persons can be subject to significant penalties and other consequences for violations of the EAR and ITAR. Both civil and criminal penalties can be assessed on companies and individuals, including criminal or deferred prosecution agreements for companies and imprisonment for individuals. In recent years, the US government, through its individual agencies, has intensified enforcement of US export control laws, assessing steep penalties and imposing other consequences, such as debarment from exports of 'defense articles' under the ITAR, placement on the BIS Entity List, restricting access to items subject to the EAR or the BIS Denied Persons List, and denying export privileges from the United States. These restrictions can have a significant effect on a company's bottom line, cut off access to US-origin items, technology and software, and result in the investigation and prosecution of individuals within a company, among other things.

Penalties

Penalties for violations of the ITAR and EAR can be severe.[101]

For violations of the EAR, criminal penalties can include a fine of up US$1 million per violation for a company and up to US$1 million or imprisonment for up to 20 years, or both, for an individual.[102] Civil penalties can include penalties of up US$300,000 (adjusted annually for inflation) or twice the value of the transaction for each violation, whichever is greater.[103] Other penalties under the Export Control Reform Act include revocation of a licence issued by BIS, and prohibitions or restrictions on a person or company's ability to export, reexport or transfer any items subject to the EAR.[104]

Criminal penalties for violations of the ITAR include a fine of up to US$1 million per violation for a company and the same monetary penalty or imprisonment for up to 20 years, or both, for an individual.[105] Civil penalties can exceed US$1 million per violation, as modified each year for inflation.[106] The

101 The relevant penalties to be considered include those set forth under the AECA, 22 U.S.C. §§ 2778–2780 (2012); ECRA, 50 U.S.C. §§ 4801–4852 (2018); and 18 U.S.C. § 3571 (2012) (the alternative criminal fine provision). Note that penalties provisions are frequently amended and penalty amounts are adjusted for inflation.

102 See ECRA, 50 U.S.C. § 4819(b) (2018).

103 See id., at § 4819(c)(1)(A) (2018).

104 See id., at § 4819(c)(1), Paragraphs (B) and (C) (2018).

105 See AECA, 22 U.S.C. § 2778(c).

106 See 22 C.F.R. § 127.10(a)(1)(i) ('for each violation of 22 U.S.C. 2778').

ITAR also contain 'statutory' and 'administrative' debarment as both a civil and criminal penalty. Debarred persons are prohibited from participating in the export of 'defense articles' (including technical data) and 'defense services', directly or indirectly.[107] Settlements with DDTC are done under consent agreements.

In recent years, the use of monitorships to oversee a company's compliance has been used by both BIS and DDTC and factored into the penalty assessment, as monitorships can last for years and be costly to the company under scrutiny. Other types of penalties include seizure and forfeiture of property, which may also be available in some enforcement actions under both the EAR and ITAR.

Voluntary self-disclosure

Companies seeking to mitigate potential penalty exposure may choose to file a voluntary self-disclosure (VSD) with the appropriate agency. Whether to voluntarily self-disclose an export control violation is a fact-specific decision. There are some benefits that may come with submission of a VSD, such as mitigation of penalties and credit for cooperation.

Although a VSD is by definition voluntary, there are situations in which a disclosure is mandatory, or in which a company finds itself in a situation of needing to disclose a prior violation. The ITAR, for example, require immediate notification to DDTC if there is a violation of the ITAR with respect to a country that is proscribed pursuant to Part 126.1 of the ITAR.[108] Certain ITAR consent agreements also mandate disclosure of violations.

The need to conduct activity on a forward-looking basis may also compel a disclosure as a practical matter. Under General Prohibition Ten of the EAR, it is prohibited to engage in virtually any activity with respect to an item that is known to have been exported in violation of the EAR. This means that any time a company wants to do something involving an item that has been unlawfully exported, it must seek BIS permission – which is often accompanied by a voluntary disclosure. Finally, under both the EAR and the ITAR, companies applying for a licence for forward-looking activity, when the applicant has been involved previously in substantially similar activity involving the same product and customer without proper authorisation, may also feel compelled to disclose past violations in an effort to avoid a 'material omission' in their licence application.

107 See id., at § 127.7.

108 See id., at § 126.1(e)(2).

BIS strongly encourages the submission of VSDs by providing a 50 per cent reduction in the base penalty amount in most cases, with possible full penalty suspension for VSD cases with a combination of mitigating factors, such as cooperation.[109] Without a VSD, mitigation will generally not exceed 75 per cent of the base penalty.[110] BIS often closes VSD cases without imposing a penalty.

In addition, in 2023, BIS announced that the deliberate non-disclosure of a significant potential violation (meaning one reflecting possible national security harm, as opposed to minor, technical violations) would be treated as an aggravating factor to adjust the base penalty amount upwards.[111] BIS also announced that whistle-blowing of significant potential violations by another party that ultimately results in a BIS enforcement action will be considered a mitigating factor in any future enforcement action involving the whistle-blower, even for unrelated conduct. These policy changes are the latest initiative by the US government to incentivise corporate investment in export compliance by targeting companies involved in significant EAR violations. For instance, in a June 2022 memorandum designed to strengthen BIS's administrative enforcement of US export controls, BIS announced, among other major changes, that it would fast-track VSDs involving minor or technical infractions while focusing BIS's resource on investigating EAR violations that reflect serious national security harm.[112]

DDTC also strongly encourages disclosure and may consider the submission of a VSD to be a mitigating factor.[113] DDTC will also consider the failure to submit a VSD to be an adverse factor when determining the disposition of a case.[114] DDTC often resolves VSDs without imposing any penalties – typically reserving the imposition of penalties for more egregious cases threatening US national security, or cases where DDTC believes the exporter acted wilfully or with gross negligence.

For both DDTC and BIS, to be deemed voluntary a disclosure must be received before any government agency obtains knowledge of the 'same or substantially similar information from another source'.[115]

---

109 15 C.F.R. Part 766 (Supplement 1).

110 ibid.

111 Matthew S Axelrod, Memorandum for All Export Enforcement Employees: 'Clarifying Our Policy Regarding Voluntary-Self Disclosures and Disclosures Concerning Others' (18 April 2023).

112 Matthew S Axelrod, Memorandum for All Export Enforcement Employees: 'Further Strengthening Our Administrative Enforcement Program' (30 June 2022).

113 See 22 C.F.R. § 127.12(a) (2018).

114 ibid.

115 See, generally, 15 C.F.R. § 764.5(b)(3); 22 C.F.R. § 127.12(b)(2).

Other US government agencies, such as OFAC and the Department of Justice, also have VSD rules that, depending on the scope of the violation, should be considered when evaluating whether to submit a VSD.

VSD rules are codified in each of the relevant regulations and generally include the opportunity for a high-level initial notification to the government agency followed in a timely manner by a full report of the potential violations. The timeline requirements for disclosures are found in each agency's regulations.[116]

Other enforcement information

Key enforcement trends for both BIS and DDTC include the use of: (1) monitorships (or under the ITAR, a special compliance officer) to monitor a company's compliance with the relevant regulations for a specified period after settlement and provide the results via written reports to the regulators;[117] (2) interim measures, such as placement on the BIS Entity List or revocation of export privileges, to encourage cooperation during an active enforcement investigation;[118] and (3) global settlements to address violations of various US laws involving related conduct.[119] More recently, particularly in the context of Russia-related enforcement, BIS has been relying on its power to issue temporary denial orders[120] when it deems doing so necessary to prevent an 'imminent violation' of applicable export controls.

BIS has published administrative enforcement guidelines 'to promote greater transparency and predictability to the administrative enforcement process'.[121] These guidelines align fairly closely with those issued by OFAC, discussed elsewhere in this Guide. DDTC has not provided similar enforcement guidelines.

---

116 See, generally, 15 C.F.R. § 764.5; 22 C.F.R. § 127.12.

117 See US Department of State, Bureau of Political-Military Affairs, *In the Matter of: Airbus SE* (29 January 2020), at www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=136d4db3db6204907ede365e7c9619ea, as an example under the ITAR; see also Judgment, *United States v. ZTE Corp.*, No. 3:17-cr-00120-K-1 (N.D. Tex. 22 March 2017), as an example under the EAR.

118 See Addition of an Entity to Entity List, 81 Fed. Reg. 12004, 15 C.F.R. Part 744 (2016) (adding ZTE Corporation and several affiliates to the Entity List).

119 See Press Release, US Department of Justice, 'Airbus Agrees to Pay Over $3.8 Billion in Global Penalties to Resolve Foreign Bribery and ITAR Case' (31 January 2020), at www.justice.gov/opa/pr/airbus-agrees-pay-over-39-billion-global-penalties-resolve-foreign-bribery-and-itar-case.

120 15 C.F.R. § 766.23.

121 See 15 C.F.R. § 766 (Supplement 1) ('Guidance on Charging and Penalty Determinations in Settlement of Administrative Enforcement Cases').

Conclusion

US export controls are a complex area of US law that can have a far-reaching extraterritorial effect if items, software or technology of US origin are involved. To ensure compliance, it is important to identify potential risk exposure under US export controls and design a compliance programme to address that risk adequately, such as implementation of appropriate due diligence and ensuring an understanding of items in the supply chain that may be subject to US controls. Not all US and non-US companies will have the same level of risk under US export controls, but failure to identify the potential risks can lead to serious issues for US and non-US companies alike.

CHAPTER 10

Sanctions in Latin America

Eric J Kadel, Jr and Jacob M Marco[1]

Introduction

In recent years, sanctions targeting Russia, Iran and North Korea have received significant attention. Yet, some of the longest-standing and most comprehensive sanctions programmes of the US target individuals and governments in Latin America and the Caribbean. Businesses with operations in the Americas must be aware of these risks and design effective compliance programmes to mitigate them.

Companies (and their subsidiaries) operating in Latin America must navigate country-specific sanctions, such as those against Cuba, Venezuela and Nicaragua, and subject matter-related sanctions, such as narcotics trafficking sanctions under the Counter Narcotics Trafficking Sanctions or the Foreign Narcotics Kingpin Designation Act (the Kingpin Act), and human rights sanctions under the Global Magnitsky Human Rights Accountability Act (the Magnitsky Act). It has been said that in Latin America, sanctions have become one of the central pillars of US policy to defend democracy and combat corruption.[2]

As discussed in this chapter, while many sanctions programmes have been consistently in force for years, other aspects of sanctions programmes have diverged between successive US presidential administrations. Legal advisers must maintain awareness of these developments when advising clients.

---

1 Eric J Kadel, Jr is a partner and Jacob M Marco is an associate at Sullivan & Cromwell LLP. The authors would like to thank Samuel Cutler, previously an associate at the firm, for contributing to the chapter.

2 Christopher Sabatini, Opinion, 'America's List of "Undemocratic and Corrupt Actors" Just Keeps Growing', *New York Times* (5 October 2021), www.nytimes.com/2021/10/05/opinion/us-sanctions-venezuela.html.

This chapter surveys trends relating to sanctions targeting Latin America and certain considerations for legal advisers, with a focus on US sanctions. It also discusses certain sanctions programmes enacted by Latin American governments. Sanctions tend to be used by Latin American countries relatively infrequently, perhaps in part due to a history of non-alignment of foreign policy in the region.

Country-specific US sanctions

At the time of writing, three countries in the Latin America region – Cuba, Nicaragua and Venezuela – are targeted by US sanctions. Cuba is subject to the longest-running and broadest set of sanctions. Venezuela is also subject to broad sanctions against its government, whereas sanctions on Nicaragua are targeted and directed solely at certain individuals and government entities.

Cuba

Since 1962, the US has implemented a comprehensive embargo against Cuba, which is now codified under the Cuban Assets Control Regulations (CACR), at 31 Code of Federal Regulations (CFR) Part 515. The CACR restrict US persons, non-US persons within the US and non-US entities owned or controlled by US persons from trading or engaging in other transactions with Cuba. The CACR are generally maintained and enforced by the US Department of the Treasury's Office of Foreign Assets Control (OFAC).[3]

The legal basis for restrictions against Cuba dates back to the Trading with the Enemy Act (TWEA) of 1917, which authorised the US President to restrict trade between the US and its enemies in times of war.[4] Determinations of restrictions under the TWEA are made on an annual basis, and in September 2022, President Biden extended TWEA restrictions against Cuba for an additional year.[5] Cuba is currently the only country subject to restrictions under the TWEA. The Foreign Assistance Act of 1961 further barred the US government from providing foreign aid to the government of Cuba and authorised the President to establish and maintain a total embargo on trade between the US and Cuba.[6] The

3 The US Department of State maintains certain other lists, such as the Section 515.582 list, which lists authorised imports into the US from independent Cuban entrepreneurs.

4 50 U.S.C. § 4301 et seq.

5 Presidential Determination No. 2022-22 of 2 September 2022. See Continuation of the Exercise of Certain Authorities Under the Trading With the Enemy Act, 87 Fed. Reg. 54859 (8 September 2022), www.govinfo.gov/content/pkg/FR-2022-09-08/pdf/2022-19532.pdf.

6 22 U.S.C. § 2370.

embargo was tightened by the Cuban Democracy Act (CDA) of 1992,[7] which restricted foreign aid to other nations that provided aid to Cuba, and which may be viewed as an early precursor to the use of secondary sanctions.[8] The CDA also enacted sanctions on vessels engaging in trade with Cuba, and authorised donations of food and exports of medicine and medical supplies. The embargo against Cuba was codified by the Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996.[9] The LIBERTAD Act also authorised a private right of action against persons who traffic in property confiscated by the Cuban government on or after 1 January 1959 (though, as discussed below, this provision had no effect until recently), and defined a difficult standard by which the embargo may be lifted. The Trade Sanction Reform and Export Enhancement Act of 2000 authorised certain exports of medical or agricultural goods to Cuba and some related travel and financial transactions under certain conditions.[10]

Although constrained by the parameters of the embargo's statutory underpinnings, within these limitations, in recent years, US presidential administrations have taken differing approaches to the US relationship with Cuba. In December 2014, the Obama administration announced an intent to re-establish diplomatic relations with Cuba.[11] These changes occurred by way of several rounds of regulatory changes and policy decisions, including prisoner exchanges;[12] easing of travel restrictions; allowing certain remittances;[13] and the authorisation

---

7 The Cuban Democracy Act is also known as the Torricelli Act.

8 22 U.S.C. § 6001 et seq.

9 22 U.S.C. § 6021 et seq. The Cuban Liberty and Democratic Solidarity Act is also known as the Helms-Burton Act.

10 22 U.S.C. § 7201 et seq. Specifically, the law barred the President from imposing unilateral agricultural or medical sanctions against a foreign country or entity, subject to certain conditions and exceptions. The law also contained several Cuba-specific provisions, such as clarifying that the law does not modify the prohibition on imports of any Cuban-origin goods and limiting travel to Cuba and financial transactions with Cuban entities for purposes authorised by the law.

11 Press Release, White House, 'President Barack Obama, Statement by the President on Cuba Policy Changes' (17 December 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/12/17/statement-president-cuba-policy-changes.

12 See, e.g., Adam Goldman, 'U.S. spy freed by Cuba was longtime asset', *The Washington Post* (18 December 2014), www.washingtonpost.com/world/national-security/us-spy-freed-by-cuba-was-longtime-asset/2014/12/17/a3b374c4-8612-11e4-a702-fa31ff4ae98e_story.html, and Dana Ford and Juan Carlos Lopez, 'Cuba releases 53 political prisoners', CNN (12 January 2015), www.cnn.com/2015/01/12/americas/cuba-prisoners-release/.

13 Family travel and remittances were authorised in 2009. In 2011, the administration authorised educational travel, including people-to-people educational travel and non-family remittances. Restrictions on travel and remittances were further relaxed throughout

of a limited number of other transactions with Cuba.[14] The administration also rescinded Cuba's designation as a state sponsor of terrorism.[15] However, the Trump administration reversed and limited some of these changes, beginning in November 2017.[16] Notably, the changes disallowed the 'U-turn exception' (which had allowed US financial institutions to process certain US dollar payments relating to Cuba in which both the originator and beneficiary were outside of the US), created a Cuba Restricted List identifying entities determined to support Cuban military or security services with whom persons subject to the jurisdiction of the US are barred from transacting, lowered the *de minimis* threshold for export controls relevant to Cuba from 25 per cent to 10 per cent, and restricted travel and remittances. Additionally, the Trump administration allowed the previous suspension of the private right of action under Title III of the LIBERTAD Act to lapse, which has allowed a number of lawsuits against persons accused of trafficking in property confiscated by the Cuban government.[17] In January 2021, the Trump administration re-designated Cuba as a state sponsor of terrorism.[18]

As at the time of writing, the only significant change that the Biden administration has made with respect to the Cuba sanctions has been certain amendments to the CACR announced in May 2022.[19] These changes followed a review of US policy towards Cuba and aimed to increase support for the Cuban people by facilitating family reunification, expanding authorised travel, easing restrictions on remittances and supporting Cuba's private sector. According to

---

2015 and 2016. See Mark P Sullivan, 'Cuba: U.S. Restrictions on Travel and Remittances', Congressional Research Service (15 December 2022), https://crsreports.congress.gov/product/pdf/RL/RL31139.

14 Cuban Assets Control Regulations, 80 Fed. Reg. 2291 (16 January 2015), https://ofac.treasury.gov/media/7211/download?inline.

15 Press Release, White House, 'Certification – Report to Congress with Respect to the Proposed Rescission of Cuba's Designation as a State Sponsor of Terrorism' (14 April 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/04/14/certification-report-congress-respect-proposed-rescission-cubas-designat.

16 Cuban Assets Control Regulations, 82 Fed. Reg. 51998 (9 November 2017), https://ofac.treasury.gov/media/7181/download?inline.

17 Secretary of State Michael R Pompeo's Remarks, US Embassy in Chile (published 18 April 2019; remarks made 17 April 2019), https://cl.usembassy.gov/secretary-of-state-michael-r-pompeos-remarks/.

18 'U.S. Announces Designation of Cuba as a State Sponsor of Terrorism', US Embassy in Cuba (11 January 2021), https://cu.usembassy.gov/u-s-announces-designation-of-cuba-as-a-state-sponsor-of-terrorism/.

19 Cuban Assets Control Regulations, 87 Fed. Reg. 35088 (9 June 2022), https://ofac.treasury.gov/media/923666/download?inline.

a State Department spokesperson, the changes will provide Cubans with 'additional tools to pursue life free from Cuban government oppression and to seek greater economic opportunities'.[20] Earlier in the Biden administration, in 2021, new sanctions targeting leaders of the Cuban police force were issued in the wake of anti-government demonstrations by the Cuban people protesting the country's ongoing economic crisis as it was battling the covid-19 pandemic.[21] The Biden administration also met with Cuban officials in Havana on 28 April 2023 to discuss, among other things, the listing of Cuba as a state sponsor of terrorism.[22] The Biden administration has said that it is reviewing Cuba's status on the terrorism list, but has yet to make any changes. Practitioners should continue to monitor this area for developments.

Venezuela

The Venezuela Sanctions Regulations are maintained at 31 CFR Part 591; they reflect a number of sanctions implemented against Venezuela in recent years. The US implemented broad sanctions against the government of Venezuela in March 2015 in response to human rights violations by the Nicolás Maduro regime and accompanying civil unrest and regime instability.[23] In August 2017, the US prohibited transactions relating to new debt of the state-owned oil company Petróleos de Venezuela, SA (PdVSA) or new debt or equity of the Venezuelan government. Facilitating profit distributions to the Venezuelan government from any entity owned or controlled by the Venezuelan government was also prohibited.[24] In March 2018, the US prohibited transactions involving digital currency, coins or tokens issued by the Venezuelan government.[25] In May 2018, the US prohibited transactions involving debt owed to the Venezuelan government in an effort to reduce public corruption.[26] In January 2019, the US amended previous

20 US Dep't of State press statement, 'Biden Administration Expands Support to the Cuban People' (16 May 2022), www.state.gov/biden-administration-expands-support-to-the-cuban-people/.

21 Press Release, US Dep't of Treasury, 'Treasury Sanctions Cuban Police Force and Its Leaders in Response to Violence Against Peaceful Demonstrators' (30 July 2021), https://home.treasury.gov/news/press-releases/jy0298.

22 Dave Sherwood, 'Cuba, US Officials Meet in Havana to Discuss Anti-terrorism Measures', Reuters (28 April 2023), www.reuters.com/world/americas/cuba-us-officials-meet-havana-discuss-anti-terrorism-measures-2023-04-29/.

23 Executive Order 13692, 80 Fed. Reg. 12747 (11 March 2015).

24 Executive Order 13808, 82 Fed. Reg. 41155 (29 August 2017).

25 Executive Order 13827, 83 Fed. Reg. 12469 (21 March 2018).

26 Executive Order 13835, 83 Fed. Reg. 24001 (24 May 2018).

sanctions to recognise the swearing-in of interim President Juan Guaido and to ensure that earlier sanctions against the 'Government of Venezuela' remained focused on the Maduro regime.[27] In August 2019, the US designated the entire Venezuelan government as a Specially Designated National (SDN), broadly defining the government to include many entities sanctioned under previous executive orders, including political subdivisions, the Venezuelan central bank, PdVSA, entities owned by these and any person acting or purporting to act for or on behalf of these entities.[28] Additionally, the Venezuelan gold, defence and security, financial and oil sectors have been targeted for additional sanctions enforcement.[29] In November 2022, the Biden administration eased some restrictions on the Venezuelan oil industry by allowing Chevron Corporation to resume certain transactions related to its joint ventures in Venezuela.[30]

In addition, OFAC has applied sanctions to several non-Venezuelan companies deemed to have operated in the Venezuelan oil sector and to have provided material assistance to sanctioned Venezuelan entities in the oil sector. This includes Mexico-based entities Libre Abordo and Schlager Business Group,[31] which were accused of assisting PdVSA through brokering crude oil exports, and Russia-based Evrofinance Mosnarbank, which was accused of financing PdVSA's operations.[32]

Nicaragua

US sanctions involving Nicaragua have been mostly limited to specific senior government leaders in connection with allegations of human rights abuses under the Daniel Ortega administration. The US imposed sanctions against four senior

27 Executive Order 13857, 84 Fed. Reg. 509 (30 January 2019).

28 Executive Order 13884, 84 Fed. Reg. 38843 (7 August 2019).

29 Executive Order 13850, 83 Fed. Reg. 55243 (2 November 2018). See also Press Release, US Dep't of Treasury, 'Treasury Sanctions Venezuela's State-Owned Oil Company Petroleos de Venezuela, S.A.' (28 January 2019), https://home.treasury.gov/news/press-releases/sm594.

30 General License No. 41, Venezuela Sanctions Regulations, US Dep't of Treas. (26 November 2022), https://ofac.treasury.gov/media/929531/download?inline. See also General License No. 8K, Venezuela Sanctions Regulations (26 November 2022), https://ofac.treasury.gov/media/929526/download?inline.

31 Press Release, US Dep't of Treasury, 'Treasury Targets Sanctions Evasion Network Supporting Corrupt Venezuelan Actor' (18 June 2020), https://home.treasury.gov/news/press-releases/sm1038.

32 Press Release, US Dep't of Treasury, 'Treasury Sanctions Russia-based Bank Attempting to Circumvent U.S. Sanctions on Venezuela' (11 March 2019), https://home.treasury.gov/news/press-releases/sm622.

members of the Ortega administration between December 2017 and July 2018 under the Magnitsky Act, which authorises sanctions against those accused of human rights abuses around the world. As the government continued its crackdown on protests, in November 2018 President Trump issued Executive Order 13851, which provided an independent basis for sanctions relating to human rights abuses in Nicaragua specifically.

Additionally, the Nicaragua Human Rights and Anticorruption Act of 2018, passed in December 2018, imposed targeted sanctions on Nicaraguan officials designated as responsible for human rights violations and restricted lending to the Nicaraguan government by international financial institutions.[33] These provisions were further strengthened by the Reinforcing Nicaragua's Adherence to Conditions for Electoral Reform Act of 2021, which: increased sanctions on key actors of the Ortega administration; expanded sanctions coordination with Canada, the European Union and nations in Latin America and the Caribbean; and required a formal review of whether Nicaragua should continue to be allowed to remain in the Central America Free Trade Agreement.[34]

OFAC has since designated several dozen high-ranking Nicaraguan officials and associates of President Ortega as SDNs under the order. Sanctions against Nicaragua are maintained at 31 CFR Part 582.

Subject matter-related US sanctions

Human rights

The US has imposed sanctions under the Magnitsky Act targeting those responsible for serious human rights abuses and corruption around the world. There have been several instances of OFAC designating individuals from Latin American countries. For example, in May 2019, OFAC designated Roberto Sandoval Castañeda, a Mexican national and former governor of the Mexican state of Nayarit, for his alleged role in accepting bribes from and having ties to Mexican drug cartels.[35] In 2021, OFAC used Magnitsky Act authorities to target

33 Nicaragua Human Rights and Anticorruption Act of 2018, PL 115-335, 20 December 2018, 132 Stat 5019.

34 Reinforcing Nicaragua's Adherence to Conditions for Electoral Reform Act of 2021, PL 117-54, 10 November 2021, 135 Stat 413.

35 Press Release, US Dep't of Treasury, 'Treasury Works with Government of Mexico Against Perpetrators of Corruption and their Networks' (17 May 2019), https://home.treasury.gov/news/press-releases/sm692.

a Guatemalan politician for corruption,[36] two senior El Salvadorean officials and a related family member with ties to international criminal gang MS-13,[37] and two affiliates of the governments of Guatemala and El Salvador for corruption.[38] More recently, Magnitsky authorities have been used against former and current Paraguayan officials.[39]

Narcotics trafficking

US sanctions related to foreign drug trafficking date to October 1995, when President Clinton signed Executive Order 12978 and created the Counter Narcotics Trafficking Sanctions programme, which targeted Colombian narcotics traffickers specifically. In 1999, President Clinton signed into law the Kingpin Act, which authorises sanctions against foreign narcotics traffickers regardless of country, and notably carries significantly higher penalties than the Counter Narcotics Trafficking Sanctions.[40] While the Counter Narcotics Trafficking Sanctions are limited to Colombian trafficking, the Kingpin Act has been used

36 Press Release, US Dep't of Treasury, 'Treasury Sanctions Current and Former Guatemalan Officials for Engaging in Corrupt Activities' (26 April 2021), https://home.treasury.gov/news/press-releases/jy0147.

37 Press Release, US Dep't of Treasury, 'Treasury Targets Corruption Networks Linked to Transnational Organized Crime' (8 December 2021), https://home.treasury.gov/news/press-releases/jy0519.

38 Press Release, US Dep't of Treasury, 'Treasury Issues Sanctions on International Anti-Corruption Day' (9 December 2021), https://home.treasury.gov/news/press-releases/jy0523.

39 Press Release, US Dep't of Treasury, 'Treasury Sanctions Paraguay's Former President and Current Vice President for Corruption' (26 January 2023), https://home.treasury.gov/news/press-releases/jy1221.

40 Individuals who violate the Kingpin Act are subject to criminal penalties of up to 10 years' imprisonment or fines, or both, under Title 18 of the US Code. Entities that violate the Kingpin Act are subject to criminal penalties of up to US$10 million. Their officers, directors and agents who knowingly participate in a violation are subject to criminal penalties of up to 30 years' imprisonment or a US$5 million fine, or both. Individuals and entities are also subject to civil penalties of up to US$1.7 million. See 21 U.S.C. § 1906(a) and 31 C.F.R. § 598.701. The maximum civil penalty under the Counter Narcotics Trafficking Sanctions is US$356,579, or twice the value of the transaction, whichever is greater; criminal penalties are limited to those who wilfully violate these sanctions and may not exceed US$1 million and 20 years' imprisonment. See 31 C.F.R. § 536.701.

to target individuals in Ecuador,[41] Mexico,[42] the Dominican Republic[43] and Panama,[44] as well as Colombia.[45]

Lessons from select US enforcement action examples

Ensure wholly owned subsidiaries maintain compliance programmes

Potential violations of the CACR continue to represent the most significant sanctions-related risk arising out of commercial dealings in Latin America.

On 21 April 2022, OFAC announced a US$141,442 settlement with multinational mining conglomerate Newmont Corporation for violations of the CACR. In 2016, Newmont, through its subsidiary Newmont Suriname, entered into an agreement with a Suriname-based third-party distributor to supply explosives for use in a gold mining project in Suriname. The distributor contracted with a Cuban entity, Unión Latinoamericana de Explosivos, to source the explosives, with the importation of Cuban-origin explosives occurring on at least four occasions. Under the CACR, wholly owned subsidiaries of US corporations are subject to the same prohibitions as their US parent company. According to OFAC, a Newmont Suriname employee, who had not participated in export and trade sanctions training, did not understand the implications of US sanctions on Cuba when processing the transaction. Furthermore, Newmont Suriname's purchase orders did not include standard sanctions-related representations and warranties, and the subsidiary did not require suppliers to provide country-of-origin information for goods. OFAC also concluded a US$45,908 settlement with Florida-based Chisu International Corporation, a small, individually managed, Florida-based explosives distributor. Based on OFAC's settlement notice, it appears that Chisu oversaw Newmont's Suriname explosives distributor.

---

41 Press Release, US Dep't of Treasury, 'Treasury Sanctions Major Ecuadorian and Mexican Narcotics Traffickers With Ties to the Sinaloa Cartel and CJNG' (10 February 2022), https://home.treasury.gov/news/press-releases/jy0592.

42 Press Release, US Dep't of Treasury, 'Treasury Identifies Sinaloa-based Mexican Narcotics Trafficker That Helps Fuel the US Opioid Epidemic' (12 May 2021), https://home.treasury.gov/news/press-releases/jy0172.

43 Press Release, US Dep't of Treasury, 'Treasury Designates Dominican Republic-Based Peralta Drug Trafficking Organization Under the Kingpin Act' (20 August 2019), https://home.treasury.gov/news/press-releases/sm755.

44 Press Release, US Dep't of Treasury, 'Treasury Sanctions the Waked Money Laundering Organization' (5 May 2016), https://home.treasury.gov/news/press-releases/jl0450.

45 Press Release, US Dep't of Treasury, 'Treasury Targets Colombians Linked to Oficina de Envigado Crime Boss Under Kingpin Act' (14 February 2018), https://home.treasury.gov/news/press-release/sm0289.

As this enforcement action makes clear, Cuba sanctions can impact firms doing business outside of Latin America in unexpected ways. As such, wholly owned subsidiaries of US companies should be fully cognisant of their compliance responsibilities and ensure that employees of foreign subsidiaries receive adequate compliance training that emphasises the identification of red flags. Companies should also take steps to analyse suppliers' and vendors' compliance programmes to reduce the risk of importing potential sanctions liability from a third party's own compliance failures.

Maintain compliance focus when exploring new areas of business

The ever-changing nature of US sanctions affecting various jurisdictions in Latin America can also provide both opportunities and risks that must be managed. When the Obama administration relaxed certain sanctions affecting Cuba in 2015, numerous companies took steps to take advantage of the relaxed rules. But there were risks in taking advantage of the relaxed rules, and on 3 January 2022, OFAC published a US$91,172.29 settlement with Airbnb Payments, Inc (Airbnb) for violations of the CACR.[46] According to OFAC, Airbnb facilitated payments related to non-approved categories of travel to Cuba and failed to keep required records of its customers' Cuba travel related to transactions authorised under the Obama administration's 2015 easing of travel-related restrictions. Under the relaxed travel rules, the CACR identified 12 categories of approved Cuba-related travel, including family visits, journalistic activity, support for the Cuban people and educational activities. Notably, pure tourist travel was not one of the identified categories. Travellers utilising the authorisations were required to adhere to the specific qualifying conditions for each approved category.

OFAC suggested that the violations resulted from Airbnb's failure to effectively manage sanctions risks while rapidly scaling up its Cuba business following the 2015 regulatory changes. After conducting an internal review of its compliance programme, Airbnb discovered that it had facilitated thousands of transactions in violation of the CACR, including those related to individuals travelling for non-approved purposes. Airbnb also engaged in inadequate record-keeping related to traveller activities and facilitated Cuba-related transactions with non-US persons prior to receiving a specific licence.

46 US Dep't of the Treasury, 'Enforcement release: January 3, 2022: OFAC Settles with Airbnb Payments, Inc. for $91,172.29 Related to Apparent Violations of the Cuban Assets Control Regulations' (3 January 2022), https://ofac.treasury.gov/media/917236/download?inline.

The Airbnb enforcement action offers a number of lessons for companies entering new areas of business following regulatory changes. First and foremost, when establishing new operations in sanctioned jurisdictions, it is important that the centrality of sanctions compliance is emphasised across departments within the company. In Airbnb's case, some of the record-keeping violations resulted from the continued operation of an older version of the Airbnb mobile application, which allowed customers to book travel to Cuba without the required attestation regarding the purpose of the travel. Robust compliance training for technology teams can help prevent technical defects inadvertently causing violations. Additionally, when potential violations are discovered, conducting a proactive internal investigation, prompt disclosure to OFAC and transparent cooperation are essential; the maximum statutory penalty in Airbnb's case was over US$600 million, yet the company paid only US$91,172.29.

Consider sanctions risk throughout the region

While many practitioners may be familiar with sanctions programmes against Cuba, Venezuela or Nicaragua, they should note that limiting business activities in these countries alone would not eliminate sanctions risk. As noted above, Magnitsky Act, Kingpin Act and other authorities have been used to target individuals in Mexico, Guatemala, El Salvador, the Dominican Republic, Paraguay, Ecuador, Colombia and Panama. An effective compliance programme considers all potential risks of conducting business activities in the region.

Pay attention to changes in restrictions and enforcement

As noted above, different US administrations have taken varied approaches to sanctions and their enforcement. Aside from ideological differences and competing policy priorities, new administrations will face different environments with new facts and trade-offs. Practitioners should consider the potential future changes – both tightening and loosening – of sanctions programmes in the region.

As an example, on 27 May 2022, OFAC announced a US$255,937.86 settlement with Banco Popular de Puerto Rico (BPPR) for violations of the Venezuela Sanctions Regulations. According to OFAC, BPPR failed to adequately implement the new August 2019 sanctions against the government of Venezuela, resulting in the bank providing account services, including 337 transactions totalling US$852,126, to two low-level GoV employees. Transactions with these customers continued for a period of 14 months, despite BPPR recognising the need to implement Executive Order 13884 shortly after its issuance. The penalty

demonstrates the importance of having sufficient know-your-customer policies and procedures in place to facilitate sanctions compliance reviews when new prohibitions come into effect.

Design an effective compliance programme

When advising corporate clients in Latin America, advisers should begin by considering the 2020 Framework for OFAC Compliance Commitments (the Framework). Under the Framework, entities that 'conduct business in or with the US, US persons, or using US-origin goods or services' are encouraged to 'employ a risk-based approach' to sanctions compliance. According to OFAC, there are five essential components of an effective OFAC compliance programme:

- management commitment;
- risk assessment;
- internal controls;
- testing and auditing; and
- training.

Constructing an effective compliance programme is important not only for avoiding a potential enforcement action, but also for mitigating the severity of a potential response by OFAC in the event that violative conduct is discovered – a fact the Framework emphasises.

Compliance with US sanctions is the responsibility of any entity that touches on US jurisdiction. OFAC has previously penalised companies where the only US touchpoint was back-office functions performed on behalf of a foreign affiliate.[47] Latin American companies should understand exactly where there is jurisdictional nexus to the US, to ensure that any high-risk activity is avoided. This includes US employees.

Additionally, even with an effective compliance programme in place, human error can still result in compliance failures. For instance, on 23 December 2021, OFAC announced a US$9,766.39 settlement with TD Bank, NA (TDBNA) resulting from violations of the Foreign Narcotics Kingpin Sanctions Regulations. According to OFAC, over a period of four years, TDBNA processed 145 transactions totalling US$35,514.13 on behalf of an SDN customer. In February 2016, TDBNA opened two accounts for Esperanza Caridad Maradiaga

47 US Dep't of Treasury, 'Enforcement Information for July 10, 2012: Great Western Malting Co. Settles Apparent Violations of Cuban Assets Control Regulations' (10 July 2012), https://ofac.treasury.gov/media/13786/download?inline.

Lopez, who was designated by OFAC in 2013. Despite TDBNA's compliance programme issuing a sanctions screening alert due to last name and date of birth matches, TDBNA analysts improperly dismissed the alert. Analysts would dismiss an additional three alerts over the following four years, until a fifth alert resulted in closure of the account. Then, after the account was closed, TDBNA's fraud unit accidentally credited and re-opened one of the accounts, apparently unaware of the sanctions issues. The settlement demonstrates that even in a relatively sophisticated institution with a robust compliance programme, human error and inadequate cross-departmental information sharing can result in compliance failures.

Consider sanctions risk in the context of mergers and acquisitions

Mergers and acquisitions represent one area in particular that presents heightened compliance challenges. First, when conducting pre-transaction due diligence, it is important to consider that an acquirer will be liable for any sanctions violations of the target that occurred within the statute of limitations. For example, in 2019, OFAC announced a US$66,212 settlement with Chubb Limited regarding CACR violations committed between 2010 and 2014 by ACE Limited.[48] These violations occurred before ACE and Chubb merged in 2016, but Chubb was nonetheless responsible for ACE's earlier violations. In explaining the relatively small size of the settlement, OFAC noted Chubb's substantial cooperation and voluntary self-disclosure of the violations.

Second, getting an accurate picture of the target's existing sanctions compliance architecture will assist in identifying potential risks going forward. For instance, for a target with limited US exposure, sanctions compliance is not necessarily an important consideration. But once incorporated into a multinational corporation or one that does significant business with the US, the target's use of Cuban contractors may present issues.

Latin American countries' sanctions programmes

Most Latin American countries do not have a tradition of enacting, or specific domestic legal authorities by which they can enact, their own sanctions. For example, the largest economy in the region, Brazil, does not have independent

48 US Dep't of Treasury, 'Enforcement Information for December 9, 2019: Chubb Limited (as Successor Legal Entity of the Former ACE Limited) Settles Potential Liability for Apparent Violations of the Cuban Assets Control Regulations' (9 December 2019), https://ofac.treasury.gov/media/25921/download?inline.

authorities to impose unilateral sanctions, but has a law pursuant to which it will implement United Nations sanctions.[49] In addition, on some occasions, Latin American countries have relied on the legal authority of the Inter-American Treaty of Reciprocal Assistance (the Rio Treaty) to implement sanctions. Even so, this practice has been relatively rare compared to the sanctions programmes implemented by the US or the European Union.

The Rio Treaty was signed in 1947 as a collective security pact among 19 countries in the western hemisphere.[50] Beyond the mutual defence provisions, the Treaty authorises its signatory nations collectively to engage in 'partial or complete interruption of economic relations'.[51]

This provision has been used to enact collective economic sanctions several times. Most recently, in September 2019, several Treaty members, including the US, Argentina, Brazil, Chile, Colombia, the Dominican Republic, El Salvador, Guatemala, Haiti, Honduras and Paraguay, supported a resolution convening consultations regarding the Venezuelan crisis.[52] After the consultations, the parties voted to investigate and sanction certain members of the Maduro regime.[53] The same provisions were used to enact since-repealed sanctions against the Dominican Republic in 1960[54] and against Cuba in 1964.[55]

While sanctions under the Rio Treaty tend to be rare, they are nonetheless notable. Even Latin American countries with no independent domestic sanctions authority may rely on the Treaty to implement sanctions as a collective organisation. Practitioners should continue to monitor this area for developments.

---

49 Law No. 13,810 (8 March 2019) (Brazil).

50 Inter-American Treaty of Reciprocal Assistance (Rio Treaty), 2 September 1947, 62 Stat. 1681, 21 U.N.T.S. 77.

51 id., Article 8.

52 Press Release, Organization of American States (OAS), 'States Parties to the [Inter-American Treaty of Reciprocal Assistance] in the Permanent Council Approve Establishment of Organ of Consultation and Convene Meeting of Foreign Ministers' (11 September 2019), www.oas.org/en/media_center/press_release.asp?sCodigo=E-065/19.

53 Press Release, OAS, 'Resolution to the Thirtieth Meeting of Consultation of Ministers of Foreign Affairs, Acting as the Consultative Organ in Application of the Inter-American Treaty of Reciprocal Assistance (TIAR)' (23 September 2019), www.oas.org/en/media_center/press_release.asp?sCodigo=S-018/19.

54 'Sixth Meeting of Consultation of Ministers of Foreign Affairs', OAS (16–21 August 1960), www.oas.org/consejo/MEETINGS%20OF%20CONSULTATION/Actas/Acta%206.pdf.

55 'Ninth Meeting of Consultation of Ministers of Foreign Affairs', OAS (21–26 July 1964), www.oas.org/consejo/MEETINGS%20OF%20CONSULTATION/Actas/Acta%209.pdf.

Sanctions enactment by individual Latin American countries has been rarer still. For example, no Latin American country has implemented its own sanctions against Russian entities in response to Russia's invasion of Ukraine, and only one country, Costa Rica, has instructed its businesses to comply with US sanctions directives against Russia.[56] The leaders of the two largest economies in the region, Brazil and Mexico, have both stated that their countries will not be implementing sanctions against Russian entities.[57] Mexico has also implemented its own blocking statute, through which persons within Mexico are prohibited from taking action affecting commerce or investment so as to comply with foreign laws, including sanctions.[58] In some instances, companies may need to weigh risks of compliance with US sanctions against the risks of Mexico's blocking law. For example, in 2006, Starwood Hotels & Resorts Worldwide Inc was caught in a diplomatic dispute between the US and Mexico. US officials asked the Hotel Maria Isabel Sheraton in Mexico City to expel a group of Cuban officials meeting with US energy executives. To comply with US sanctions, the hotel complied with the request, but then faced complaints from Mexican government officials over its apparent violation of Mexico's blocking law.[59] Companies should carefully consider the facts and circumstances of each situation when determining how to manage sanctions compliance risks.

Because it is relatively rare for Latin American countries to implement their own sanctions, the primary risk in navigating sanctions compliance in Latin America remains compliance with US sanctions programmes.

---

56 Chase Harrison, 'One Year in, What Does the Ukraine Conflict Mean for Latin America?', Americas Society/Council of the Americas (9 February 2023), www.as-coa.org/articles/one-year-what-does-ukraine-conflict-mean-latin-america.

57 Anthony Esposito, Ana Isabel Martinez and Daina Beth Solomon, 'Mexico declines to impose economic sanctions on Russia', Reuters (2 March 2022), www.reuters.com/world/mexicos-president-says-will-not-take-any-economic-sanctions-against-russia-2022-03-01/. See also Jalen Small, 'Mexico, Brazil Leaders Ignore Their UN Delegates, Refuse to Sanction Russia', *Newsweek* (4 March 2022), www.newsweek.com/mexico-brazil-leaders-ignore-their-un-delegates-refuse-sanction-russia-1685001.

58 Law for the Protection of Trade and Investment of Foreign Standards that Violate International Law, Mexico's Official Daily of the Federation of 23 October 1996.

59 'Cubans' hotel ouster riles Mexico', *The Washington Times* (8 February 2006), www.washingtontimes.com/news/2006/feb/8/20060208-105309-5187r/.

CHAPTER 11

Impact of US, UK and EU Sanctions and Export Controls in the Asia-Pacific Region

Wendy Wysong and Ali Burney[1]

Introduction

Comprising dozens of nations with diverse business cultures and economies in various stages of development, the Asia-Pacific region (APAC) is responsible for a substantial portion of annual global trade. Whether a company is based in APAC or is operating there, economic sanctions and export control risks are now a daily concern. With long-standing US and United Nations (UN) sanctions and export control programmes targeting North Korea, multilateral sanctions and export controls targeting China and Myanmar, and, as of 2022, unprecedented sanctions against Russia (an important trading partner), APAC has, in many ways, supplanted the Middle East as the world's sanctions and export control hotspot.

In 2020 and 2021, the United States intensified its use of sanctions and export controls in relation to Hong Kong, China's Xinjiang Uyghur Autonomous Region (XUAR) and the South China Sea. In March 2021, the EU, UK and Canada joined with the United States in imposing targeted sanctions on Chinese officials over allegations of human rights abuses in the XUAR. In October 2022, as tensions in the US–China relationship intensified, the United States implemented expansive new export controls on China, with a focus on the semiconductor and advanced computing industries in the country (including Hong Kong).

1 Wendy Wysong and Ali Burney are partners at Steptoe & Johnson HK LLP.

In June 2021, the US Department of Treasury's Office of Foreign Assets Control (OFAC) also made amendments to its Chinese Military-Industrial Complex Companies (CMIC) sanctions to broaden the definition of CMICs to include any entities determined to operate or have operated in the defence and related materiel sector or the surveillance technology sector of the economy of China. These sanctions are limited in scope and generally prohibit US persons from any purchase or sale of publicly traded securities, or any publicly traded securities that are derivative of these securities or are designed to provide investment exposure to these securities, of any CMIC. These sanctions do not prohibit US persons from providing various support services related to the purchase or sale of covered securities of CMICs (e.g., clearing, execution, settlement, custody, transfer agency or back-end services).

Meanwhile, the Chinese government unveiled a framework for Chinese unilateral sanctions and a 'blocking order' against foreign sanctions deemed inimical to China's national interests. Multinational companies – and at least one UK barristers' chambers – were confronted with legal and political risks on all sides. In February 2023, China also announced its first ever use of its Unreliable Entity List by designating two US companies. Outside of Greater China, in February 2021 the clock seemed to reverse after a military coup in Myanmar, which led to the reimposition of many sanctions that were lifted just a few years before. In 2022 and 2023, Australia, Japan, New Zealand, Singapore and South Korea joined a coalition of nations imposing sanctions against Russia following its invasion of Ukraine.

For legal and compliance practitioners, this environment presents unique challenges, especially when balancing the interests of stakeholders in multiple regions, which may be operating from different perspectives. In this chapter, we describe the sanctions and export control risks for business transactions in APAC and share best practices for managing these risks from the front lines.

'Long-arm' jurisdiction

Economic coercion is a fact of life in Asia, owing to the high degree of state intervention in many economies. China, in particular, regularly withdraws economic opportunities (including tourism) from its neighbours to achieve political objectives. We distinguish these trade-boycott practices from sanctions and export controls whereby governments regulate private commerce to gain economic leverage over a foreign adversary. With the exception of multilateral UN sanctions, few countries in Asia rely on sanctions and export controls as a tool of foreign policy. (Apart from trade boycotts, China's use of unilateral sanctions has so far been limited.) Australia, Japan and a handful of other countries have

unilateral (or autonomous) sanctions, but they do not enforce these sanctions or export controls outside their home jurisdictions for the most part. In 2022 and 2023, New Zealand and Singapore were among the countries that adopted novel legal tools for imposing Russia-related sanctions outside of existing UN frameworks. For companies in APAC, the greater risk still arises from 'long-arm' or extraterritorial US sanctions and, to a lesser extent, sanctions from the European Union or United Kingdom.

Extraterritorial sanctions that impact companies in APAC are broadly divided into primary sanctions and secondary sanctions. Primary sanctions are jurisdiction-based prohibitions that are enforceable against individuals or entities through traditional criminal or administrative means. For instance, UK sanctions on Myanmar's military holding companies, introduced in March 2021, apply to UK persons and UK-incorporated companies globally, while US primary sanctions apply to US persons and US-incorporated companies globally. Secondary sanctions, on the other hand, are intended to discourage activities that are beyond the traditional legal jurisdiction of the sanctioning state by threatening the imposition of sanctions on persons engaged in certain activity outside that jurisdiction. The Hong Kong Autonomy Act is an example. It threatens secondary sanctions against foreign financial institutions that 'knowingly' engage in 'significant transactions' with Chinese and Hong Kong officials identified by the US State Department. These officials include no less than the current and former chief executives of Hong Kong.

During the past decade, companies in APAC have faced an increasing risk of primary and secondary sanctions. This shift is due in part to the companies' foray into western markets, where primary sanctions jurisdiction is most likely to exist, and greater efforts by western governments to investigate and prosecute activities that threaten their security or foreign policy aims. For these reasons, compliance with foreign sanctions is often the only commercially reasonable choice, particularly for companies that want to minimise the risk of losing access to the US markets and the US financial system.

As explained in greater detail below, the first step in managing sanctions and export control risk is identifying and assessing it in business transactions. A risk assessment for primary sanctions requires understanding and mapping the somewhat intricate rules of foreign legal jurisdiction to business operations. For example, a Chinese manufacturer exporting products to Iran should identify any financial transactions that may implicate the US financial system. A risk assessment for secondary sanctions requires imagining how emerging geopolitical risks may disrupt existing commercial arrangements. That same manufacturer should consider US secondary sanctions that may apply to its Iranian exports and

whether suffering US reprisals is a commercially sensible trade-off. Nowadays, the manufacturer may also need to think about the potential for retaliation from local authorities or the public who may discourage their compatriots from giving in to foreign economic pressures. After Russia's invasion of Ukraine, many APAC companies scrambled to reassess long-standing business in Belarus and Russia in light of sweeping new sanctions and export controls impacting every facet of the supply chain in many sectors. Understanding how these risks manifest themselves in a dynamic environment can challenge even the most experienced practitioners.

Conditions that increase sanctions risks

First, APAC is a target-rich environment for new sanctions. Some nations – North Korea, Myanmar and, less recently, Vietnam, for example – are currently, or historically have been, targeted with broad embargoes by the United States or significant sanctions by the European Union, Canada, Australia, other western allies and the UN. The region also has a significant share of companies and individuals targeted for sanctions in response to human rights abuses, proliferation of weapons of mass destruction, narcotics trafficking, organised crime and other threats to regional and international peace and security. The United States, in particular, has used sanctions and export controls to target Chinese officials and firms that have committed violations of US laws or acted contrary to US national security or foreign policy interests. This trend accelerated under the Trump administration and has continued under the Biden administration, albeit with renewed diplomatic overtures.

Second, questions about sanctions or export control compliance often come not from government investigators, but from banking partners, suppliers and other counterparties. Sanctions authorities have long considered commercial actors to be 'force multipliers' in amplifying the effects of their sanctions. The abundance of multinational enterprises and cross-border supply chains in APAC offers endless touchpoints for introducing sanctions requirements through due diligence, compliance undertakings and internal guidelines to police the behaviour of counterparties. The presence of many large, regional and multinational financial institutions – a number of which have faced significant sanctions enforcement actions – has put pressure on customers to commit 'voluntarily' to abide by US, EU and UK sanctions and export controls. Some banks demand that customers implement formal compliance programmes as a condition of services. A number of significant internal corporate investigations have started as a result of enquiries from banks about customers' payments potentially involving sanctions targets.

Third, given the complexity of sanctions and export controls and the threat of secondary sanctions, many companies and banks in APAC implement compliance programmes with little regard to the nuances of legal jurisdiction, leading to examples of over-compliance or de-risking, whereby companies and banks walk away from business that is legally permissible. This is especially true in the region's major trading hubs, such as Hong Kong and Singapore, where OFAC regulations are almost universally observed, regardless of their legal applicability, owing in large part to the high concentration of risk-averse banks. For instance, many financial institutions in the region were quick to sever ties with Myanmar Economic Holding Limited, Myanmar Economic Corporation and other entities targeted in early 2021 by the US, UK and the EU, despite their lack of jurisdiction over many of their activities. Similarly, many Asia-based companies, especially those with strong business ties to the US or EU, have voluntarily complied with sanctions against Belarus and Russia. Some US officials began calling the phenomenon 'self-sanctioning' to the extent companies were not already subject to US jurisdiction.

On the other hand, where US sanctions have been applied against major corporates, such as subsidiaries of China Ocean Shipping Company Limited (COSCO), we have observed a marked willingness among financial institutions and corporates to take a more nuanced, albeit still cautious, approach. This was especially the case in response to US Executive Order 13959, later amended under Executive Order 14032, which prohibited US persons from purchasing or selling publicly traded securities of CMICs, including some of China's most prominent multinationals. Rather than let go of profitable investments, many Asian and European investors read the 'fine print' of the Executive Order and continued to trade in the securities, as permitted. The same can be said for the foreign subsidiaries of US companies, which fell outside the definition of 'US person' for the purposes of the Order. For its part, OFAC raised no public objections to this legalistic approach to sanctions, and clarified in FAQs that even US persons could continue to engage in some activities in relation to the covered securities.

The convergence of these three factors (that is, a high number of sanctions targets, counterparty demands and de-risking) presents a daunting compliance challenge, as in the following examples.

Sanctioned countries and governments

Transactions involving countries, territories or governments subject to comprehensive or broad unilateral US sanctions (currently, Cuba, Iran, North Korea, Venezuela, Syria, Crimea and the so-called 'Donetsk People's Republic' and 'Luhansk People's Republic' regions of Ukraine) or UN sanctions are not

uncommon in the region and, for domestic political reasons, are sometimes encouraged. Many of these transactions are indirect transactions conducted through trading houses or shell companies in major trading hubs, such as Hong Kong, Singapore or Dubai. Careful due diligence of counterparties and their business activities is needed to identify transshipment or diversion risk.

Sanctioned persons

The number of sanctioned individuals and entities located, or with economic interests, in APAC has increased dramatically in recent years. They may appear as direct counterparties to a transaction or indirectly as beneficial owners or shareholders of counterparties. Once identified, companies must determine whether the involvement of a sanctioned person precludes their participation in a proposed transaction. This issue came to the fore in April 2018 when OFAC designated numerous Russian individuals and entities as Specially Designated Nationals (SDNs), including one listed on the Hong Kong Stock Exchange. In September 2019, OFAC designated two subsidiaries of COSCO as SDNs for engaging in exports of petroleum from Iran. In July 2020, OFAC named China's Xinjiang Production and Construction Corps (XPCC), a quasi-governmental conglomerate with significant commercial interests, as an SDN under the Global Magnitsky sanctions. In 2020 and 2021, the US Department of Defense identified dozens of Chinese companies as 'military companies', whose publicly traded securities were made off-limits to US investors under Executive Order 13959. The list was reborn as the Non-SDN CMIC List, in June 2021, and the US Treasury Department added several more companies to it in December 2021. One of the companies undertook a successful initial public offering shortly after its designation as a CMIC. And yet, in February 2023, OFAC added a Chinese company to the SDN List for its alleged assistance in the Russia invasion of Ukraine. In each of these cases, financial institutions and other counterparties grappled with how to maintain important commercial relationships while abiding by applicable US sanctions. The availability of general and specific licences allowed many to do so. Others have taken a legalistic view, continuing with activities outside of US jurisdiction. The United States has also added numerous Chinese companies to the Bureau of Industry and Security (BIS) Entity List for national security and foreign policy reasons, and, in certain circumstances, these listings have occurred prior to an initial public offering or exchange listing, inflicting greater costs on the targeted company and its investors. This issue will continue to be prevalent as long as the US government imposes sanctions concerning China and Hong Kong.

Supply chains

Supply chain risks attach to (1) raw materials sourced from, (2) suppliers located in, and, (3) in the case of North Korea, labour from designated countries or territories. For example, in January 2019, OFAC entered into a US$996,080 settlement with US-based e.l.f. Cosmetics, Inc for distributing false eyelash kits containing materials originating from North Korea. OFAC used the settlement to emphasise the importance of supply chain due diligence to identify the involvement of sanctioned goods or parties. In July 2020, OFAC and other US agencies published a Xinjiang Supply Chain Business Advisory, alerting the industry to sanctions and other risks associated with XPCC and the XUAR. The US government expanded its campaign later in the year by imposing import bans on certain products from the XUAR, including cotton, based on allegations of forced labour. In December 2021, the US Congress adopted the Uyghur Forced Labor Prevention Act (UFLPA), which will lead to the adoption of regulations further restricting the importation of XUAR-origin goods into the United States. As illustrated in the UFLPA Operational Guidance for Importers and the UFLPA Strategy released in June 2022, US importers are required to extend their supply chain tracing throughout the entire supply chain of an imported item or a specific component of the item. In practice, due diligence concerning these issues is often hampered by resistant counterparties, language barriers or inaccessible records. Companies often find themselves reliant on declarations or contractual representations concerning a counterparty's compliance. In some cases, third-party due diligence firms are called in to bridge the gap.

Goods, technology and software originating from the United States

BIS, located within the US Commerce Department, regulates the export, re-export and transfer of items subject to the Export Administration Regulations (EAR).[2] The risk of diversion of EAR-controlled items is high, and transshipments through trading hubs such as Hong Kong and Singapore are commonplace. Yet few companies in the region have sophisticated compliance controls for identifying and tracking items subject to the EAR, including controlled components incorporated into finished products. This is an area of emerging risk, with high enforcement potential, especially given the increasing number of Chinese technology firms targeted by the Entity List. Financial institutions, which are potentially at risk of facilitating their customers' violations of the EAR, have

2 For more information about US export controls, see Chapter 9 of this Guide, 'Export Controls in the United States'.

recently begun strengthening their export control procedures, demanding more information from customers who remain primarily responsible for understanding how the EAR applies to their activities.

Affiliates or tangential business lines

All these risk factors are compounded by the presence of many large, international, private and state-owned conglomerates. Sanctions and export control concerns frequently arise during the due diligence phase of transactions when affiliates of an investment target are found to have exposure to sanctioned persons or territories, even if that activity is seemingly unrelated to the business opportunity at hand. Use of proceeds clauses and restrictions on the transfer of goods and services offers a limited means of risk mitigation. However, given that US authorities do not accept the outsourcing or transfer of liability for sanctions risks, these provisions offer very limited protection if the company is found to have known (or should have known) about the sanctioned element and facilitated prohibited activity.

As explained above, mapping out the jurisdiction and scope of applicable sanctions and export controls is a good first step in identifying and controlling risks. The following sections offer a few reference points for managing sanctions and export control risk with an eye on recent high-profile enforcement actions.

US, EU and UK sanctions jurisdiction

Most legal systems recognise jurisdiction over activities taking place within their state's sovereign territory, regardless of nationality, as well as activities undertaken by their nationals, regardless of location. This territorial-based jurisdiction applies to most sanctions, regardless of country, and is the typical framework applied to UN sanctions enforcement in APAC.

However, jurisdiction may also exist over activities undertaken outside a state's sovereign territory conditioned on an underlying factual nexus, such as the direct or indirect involvement of nationals of the state. Long-arm or extraterritorial sanctions fall under this heading. Understanding clearly the jurisdictional hook underlying a primary or secondary sanction enhances a company's ability to decide whether and how to comply with it.

Application of sanctions to US persons

OFAC's administrative enforcement jurisdiction generally applies to 'US persons', defined to include (1) all US citizens or permanent residents (i.e., green card holders), regardless of location, (2) all entities organised under US law (including their offices and branches outside the United States), and (3) all persons in the

United States, regardless of their nationality. The basic rule is simple: US persons are required to follow OFAC regulations at all times. Additionally, OFAC regulations under the Cuba, Iran and North Korea programmes apply to the activities of non-US entities owned or controlled by US persons or (in the case of North Korea) US financial institutions.

In APAC, US jurisdiction is often based on the involvement of financial institutions (often overseas branches of US banks), offices of US-incorporated companies, subsidiaries of US-based companies, or US-based companies transacting, or investing, in the region or as individuals employed by non-US companies. While non-US subsidiaries of US companies are not subject to many OFAC programmes, it is common for subsidiaries to follow the sanctions policies of their headquarters, with limited allowances for local law. An increasing number of non-US companies are devising recusal protocols to document the ways in which their 'US person' employees are ring-fenced from transactions involving US-sanctioned persons or territories.

Non-US nationals are considered US persons when within the United States, and clients must often be reminded to abstain from engaging in activities, including phone calls or emails, concerning their companies' business with sanctioned persons or territories while visiting the United States, whether for business or pleasure. Search and seizure of business records at US borders should remain high on the list of senior executives' worries while travelling. In serious cases, extradition from a third country to the United States is also a possibility.

Application of sanctions to EU and UK persons

Jurisdiction under EU and UK law follows a similar pattern as US law, although EU Member States and the UK are less inclined to pursue 'extraterritorial' prosecutions, citing international law and comity. Broadly speaking, EU and UK sanctions apply within the territory of the European Union or the UK, aboard aircraft or vessels under their jurisdiction, to nationals of EU Member States or the UK, to entities constituted under the laws of EU Member States or the UK, and in respect of business performed in the EU territory or the UK by non-nationals. To date, neither the EU nor the UK has aggressively enforced sanctions against foreign persons processing transactions through EU or UK financial systems, in contrast to the United States. Nevertheless, EU and UK banks tend to apply a similar level of scrutiny and control to their transactions as their US counterparts.

Like US persons, EU and UK persons may appear in a variety of roles in transactions in APAC, and the presence in the region of many prominent EU and UK corporates and financial institutions makes EU and UK sanctions among the most important foreign sanctions regimes in APAC, after that of the United States.

Application of sanctions to non-US and non-EU/UK persons

As indicated above, US, EU and UK sanctions exert a significant influence on commercial activities in APAC. With respect to EU and UK sanctions, this effect is attributable mainly to the presence of many EU and UK-based corporates and financial institutions that are obliged to follow their home sanctions as a matter of law or internal policy. The case is different when it comes to US sanctions because US authorities routinely seek to assert law enforcement jurisdiction over the activities of non-US persons when those activities involve a US jurisdictional element, understood to include US persons, the US financial system and items of US origin (i.e., goods, technology and software that are subject to the EAR).

Of these three elements, it is the US financial system that has the broadest jurisdictional hook. US-dollar denominated transactions, most of which clear through US correspondent accounts, make up the lion's share of international trade in the region (and globally). OFAC and the US Department of Justice (DOJ) undertake dozens of investigations each year into transactions processed through the US financial system believed to involve prohibited trade with sanctioned persons or territories. Underpinning these cases is the legal theory, among others, that non-US persons 'cause' US financial institutions to violate OFAC regulations by initiating transactions that are cleared through US-based accounts.

For example, in July 2017, OFAC entered into a US$12,027,066 settlement with Singapore-based CSE Global Limited and CSE-Transtel Pte Ltd (Transtel) for violations of the Iranian Transactions and Sanctions Regulations (ITSR). According to the OFAC settlement notice, Transtel processed more than 100 wire transfers in its US-dollar denominated account held at a Singapore bank in connection with its business in Iran. While the business presumably was legal under Singapore law, the wire transfers cleared through the Singapore bank's US correspondent accounts, thereby triggering the ITSR's prohibition against exports of services, directly or indirectly, by US persons (i.e., the US banks holding those accounts). The Singapore bank had previously informed Transtel of this risk and obtained an attestation that the company would not use its account for its Iranian business. The Singapore bank subsequently detected the activity and disclosed it to OFAC. As noted by many commentators, the Singapore bank was not named in the settlement. Rather, OFAC penalised the bank's customer, Transtel,

for causing the violations. In the context of this case, the Singapore bank was rewarded for having effective sanctions compliance controls. However, the settlement also spotlights the conflicting interests of banks and their customers when OFAC violations are detected – a major point of contention in light of recent high-profile enforcement cases against Chinese companies.

For clients new to the subject, it may seem contradictory that a financial transaction could be illegal while the underlying trading activity – which often is not subject to OFAC jurisdiction – is perfectly fine under domestic law. Practically speaking, the challenge for practitioners is to identify transactions involving the US financial system (which can include both US financial institutions and, in some cases, non-US entities owned or controlled by them) and to interdict transactions that would be prohibited for a US bank. Some transactions can be safely processed outside the US financial system, subject to relevant secondary sanctions and the internal policies of the processing banks. While US persons are not allowed to facilitate these types of transactions, non-US persons who are familiar with the regional banking system are increasingly finding open payment channels for certain activities.

Enforcement risks from the United States: select cases

The following examples highlight important enforcement trends in APAC and compliance pitfalls to be avoided.

ZTE Technologies

In 2016, BIS added ZTE and three affiliates to the Entity List during an investigation of the company's business in US-sanctioned territories, including Iran and North Korea. To continue its business operations while it resolved the investigation, the company obtained the first ever temporary general licence, giving it continued access to US-origin goods, software and technology. However, the threat to its business operations posed by its inclusion on the Entity List led to the company's US$1.19 billion civil and criminal settlement with BIS, OFAC and the DOJ in March 2017. While US$300 million of the penalty was suspended, the settlement also mandated the hiring of a compliance monitor for three years to report to the DOJ on the company's compliance with US sanctions and export control laws and a seven-year suspended denial order. The denial order was triggered in April 2018, when the US government determined that the company had made apparent false statements to BIS. In June 2018, the company agreed to pay an additional US$1 billion, which included the hiring of an additional external compliance consultant, who will report to BIS, for 10 years.

ZTE's violations primarily involved the unlicensed re-export from China to Iran and North Korea of items subject to the EAR. The company obtained some of the items via 'isolation companies'. The US investigation into ZTE has served as a template of sorts for similar investigations and set the stage for a raft of legislative initiatives, executive orders, regulations and administrative actions aimed at reducing China's involvement in the US telecommunications sector, which continue to this day. While BIS's use of the Entity List during an investigation was novel in 2016, BIS now routinely uses it as a threat to encourage cooperation and resolution on its terms in addition to using it to advance US national security and foreign policy objectives.

US-based branches of Asian banks

Several APAC-based financial institutions have entered into settlements with US sanctions and state banking regulators, including the New York Department of Financial Services, for violations of US sanctions and anti-money laundering (AML) laws. These include Japan's MUFG Bank (2013, 2014 and 2019), Taiwan's Mega Bank (2016), the Agricultural Bank of China (2016) and South Korea's Industrial Bank of Korea (2020). In each case, the financial institutions failed to implement adequate sanctions and AML controls in their New York branches, leading to violations of the state's AML regulations, in addition to OFAC regulations.

Along with direct liability, APAC-based banks have also found themselves on the receiving end of subpoenas relating to the conduct of their customers. In a highly publicised case, in 2019 the US Court of Appeals for the District of Columbia upheld a lower court decision holding three Chinese banks in contempt for refusing to comply with subpoenas for information held outside the United States about transactions through their US correspondent accounts or branches involving a Hong Kong-based customer alleged to be a North Korean front company.

The US National Defense Authorization Act for Fiscal Year 2021 expanded the authority of the Attorney General and the Secretary of the Treasury to issue subpoenas to any non-US bank that maintains a US correspondent account in the United States to obtain records or pursue civil forfeiture of funds in relation to a broad range of financial crimes, regardless of whether the records sought relate specifically to the US correspondent account. The law also provides that the existence of a conflicting foreign secrecy or confidentiality law would not be the sole basis for quashing or modifying the subpoena.

North Korea indictments and secondary sanctions

North Korea, which is subject to both US comprehensive sanctions and broad UN sanctions, has been a constant source of risk for companies in APAC, especially since the issuance of Executive Order 13722 in March 2016. The North Korean government is widely believed to operate networks of front companies throughout the region, including in Hong Kong, and North Korean workers have historically been sent outside the country to earn revenue for the government. The US government's efforts to restrict North Korea's access to the US financial system picked up steam in mid-2017 with the sanctioning of China's Bank of Dandong, followed by sanctions against China-based trading companies and individuals alleged to act as North Korean intermediaries, as well as vessels and operators engaged in ship-to-ship transfers in apparent violation of UN sanctions.

As with Iran, the US government has issued indictments against numerous individuals and companies outside the United States for violating OFAC's North Korea Sanctions Regulations by processing transactions through the US financial system in relation to North Korean trade. These indictments are often accompanied by forfeiture orders, under which funds held in US interbank accounts can be seized in an amount equivalent to the violative transactions. Additionally, OFAC is authorised under Executive Order 13810 to target bank accounts through which North Korea-related transactions have been processed, even if those accounts are not themselves held by sanctioned persons. Recently, OFAC designated persons for attempted arms deals between North Korea and Russia under Executive Order 13551.

Commodities trading and investigations

OFAC has placed numerous APAC-based companies, individuals and vessels on the SDN List for engaging in sanctionable trade with North Korea and Iran, with or without a nexus to the United States. These include persons alleged to have engaged in exports of Iranian petroleum or petrochemical products via front companies in China, Hong Kong and the Middle East and a Singapore commodities house sanctioned for indirectly trading with North Korea through its Southeast Asian intermediaries. The DOJ and other law enforcement agencies are actively investigating and pursuing criminal enforcement actions against individuals and companies in APAC, many of whom stand accused of making illicit payments through the US financial system. In Singapore, at least one individual has been prosecuted for exporting luxury products to North Korea in violation of UN sanctions under Singapore law. Unfortunately, many clients are unaware that their activities are problematic until the moment OFAC designates a counterparty or a US bank (acting under the direction of US law enforcement)

begins freezing wire transfers passing through the United States. As a result, more companies in APAC are adopting sophisticated sanctions due diligence and transaction monitoring programmes to avoid getting entangled in costly and potentially damaging probes.

Blocking orders and other local countermeasures

Companies increasingly face a dilemma in markets such as China and Hong Kong, where local authorities may discourage compliance with some foreign sanctions. The issue came to the fore in mid-2020 with the adoption of Executive Order 13936, which authorised sanctions on Hong Kong government officials, and the Hong Kong Autonomy Act, which authorised secondary sanctions on financial institutions engaged in significant transactions with them. In response, the Hong Kong government issued statements reminding financial institutions to treat their customers fairly and stating that Hong Kong law only recognises UN sanctions. Some commentators speculated that financial institutions that complied with US sanctions could even breach the recently adopted national security law.

In September 2020, China's Ministry of Commerce (MOFCOM) announced the Provisions of the Unreliable Entity List, developing a mechanism to designate foreign companies that are considered 'unreliable'. The Unreliable Entity List was used for the first time in February 2023, when two US companies were added to the List amid heightened tensions between the United States over the 'balloon incident'. In January 2021, MOFCOM introduced an order authorising 'prohibition orders' that would restrict compliance with foreign sanctions in China. The order bore a striking resemblance to the EU blocking statute. In June 2021, China's National People's Congress adopted the Anti-Foreign Sanctions Law, giving the Chinese government new legal tools to discourage the adoption of, and compliance with, foreign sanctions perceived to threaten Chinese national interests.

It is not unusual for companies in APAC to face pressure behind the scenes not to comply with foreign sanctions that conflict with local interests or threaten profits. Sometimes that pressure is public, as was the case in 2021 when several apparel brands faced consumer boycotts over their policies on sourcing cotton from the XUAR. The possibility that a company could face administrative or criminal charges or other legal actions raises the stakes even higher. For practitioners, this means anticipating how a compliance decision made in London or Washington could impact stakeholders in APAC. We find that multinationals are relying more on team members based in the region for this much-needed perspective.

Strategies for managing multinational sanctions risks

Identification of a US, EU or UK nexus

As primary sanctions are jurisdiction-based, identifying sanctions risk is often a matter of determining whether there is jurisdiction at the outset. In addition to mapping out a company's exposure to sanctioned territories or persons, spotting touchpoints with the United States, the European Union or the United Kingdom is an essential step in implementing an effective compliance programme. This is particularly true for financial institutions and corporates whose customers and counterparties change frequently.

For example, once a nexus to the US financial system has been found, a company should adopt real-time name screening controls to filter out transactions involving sanctioned persons or territories. A distributor with a significant EU supplier should consider whether those products can be sold to persons on an EU sanctions list. For the reasons explained above, there are endless examples of these touchpoints in APAC, and it is evident that many companies have allowed themselves to become operationally dependent on US, EU or UK services without having considered the potential sanctions exposure.

In addition to traditional supply chains and financial services, companies are strongly advised not to overlook US, EU or UK connections that may exist in their data processing, including the use of US-origin software or US-based servers. In February 2020, OFAC settled with Switzerland-based SITA for US$7,829,640 for transactions involving sanctioned airlines that relied on US-origin software or servers in the United States. US agencies, including OFAC and the DOJ, are increasingly aware of how US jurisdiction may be asserted over data. The massive popularity of digital services in APAC – including cryptocurrency exchanges and other digital asset service providers – makes this an area of increasing enforcement risk for the region.

Defining common ground and expectations for sanctions compliance

It is not uncommon for companies in APAC to take the simpler and often prudent decision to implement US, EU and UK sanctions as a matter of internal policy, regardless of jurisdiction. When this is not possible for political or commercial reasons, it is necessary to define common ground to allow transaction parties to perform their roles with the least amount of residual risk. Unfortunately, it is also still commonplace for companies engaged in transactions with sanctioned persons or territories to do so in a manner that is not transparent and often without the awareness of their major suppliers or banking partners. The disruption wrought in the telecommunications sector as a result of recent US enforcement cases is an object lesson in why this approach is not advisable. The example given above

involving Singapore's Transtel offers another. The better approach is to identify sanctions risks early on, analyse them and engage stakeholders in decision-making about how to conduct business in a manner that respects applicable rules as well as the tolerances of counterparties. A legal memorandum explaining the issues is often helpful in this regard.

A common situation encountered in APAC involves capital markets or lending transactions in which banks insist that issuers or borrowers ring-fence proceeds from their activities with sanctioned territories or persons, once those activities have been identified through due diligence prior to the transaction. The meaning of the term 'ring-fence' in this context is vague, and it is typically taken to mean segregation of the proceeds from general operating accounts or the adoption of accounting controls to record how the proceeds are used in compliance with use-of-proceeds clauses. (A similar approach is often taken with respect to goods originating in the United States or other territories, which may be subject to export controls.)

Often, parties are satisfied with a simple use-of-proceeds contractual provision, particularly when funds are raised for specific purposes that are unrelated to a sanctioned territory or person. It is rare in capital markets transactions for underwriters to demand the termination of that business, unless it is particularly problematic. However, lenders appear to be more willing to demand that their borrowers cease activities with sanctioned territories or persons as a condition of financing. This is especially true after the reimposition of US secondary sanctions against Iran, beginning in August 2018. It is also common for depository institutions to refuse to open or maintain accounts for individuals or corporates with tangential exposure to sanctioned territories (e.g., nationals of sanctioned territories), although the legal basis for these policies is unclear. From a regulatory perspective, financial institutions' enforcement risk is low if they are not directly or indirectly financing prohibited activities.

Drafting mutually acceptable contractual terms and common issues

It is no secret that lawyers in the region spend a good amount of time negotiating sanctions clauses (sometimes for transactions with no apparent sanctions nexus). Given the fragmented legal picture, it is difficult to accommodate every party's demands and yet retain succinct and clear contractual language. (Despite best efforts, many agreements are capacious, at best.) The following are some of the common issues to bear in mind.

Scope of representations and warranties

Because parties in the region are subject to differing sanctions and export controls, contract clauses should clearly define which countries or programmes are intended to be covered by the language in the agreement. This includes identifying the authorities issuing sanctions and the targets of those sanctions. Lawyers in the region spend endless hours finessing sanctions clauses to assuage the concerns of clients on both sides of a deal, often with watered-down results. As demonstrated in cases concerning the EU Blocking Regulation, and at least one case in Hong Kong involving frozen assets of a customer of a Hong Kong bank, courts may be called on to interpret imprecise language, to the detriment of one party or the other. As a minimum, drafters should be reasonably familiar with sanctions so as to precisely render the parties' intentions.

Prohibited business

In our experience, there are three approaches to defining prohibited business in sanctions clauses: (1) a total prohibition against dealings with sanctioned territories or persons, irrespective of their relevance to the transaction; (2) a prohibition against using the transactions' proceeds for dealings with sanctioned territories or persons; or (3) a prohibition against violating sanctions with respect to a transaction (which may be read to permit proceeds to be used for this activity, provided it is done in compliance with applicable laws and regulations). Broadly speaking, it is now rare to find the first type of prohibition in APAC contracts. The second type is the most common and the least burdensome. The third type is increasingly common and often arises when parties that enter into a transaction are fully aware of the potential risks, and one party has agreed to assume that risk and to implement the appropriate compliance measures. It goes without saying that the party accepting these undertakings should have a reasonable basis for relying on them.

Changes in sanctions

While specificity is a virtue in contract drafting, language can become outmoded if sanctions change during the life of the contract. This problem is most often solved by indicating that references to particular sanctioned territories, persons or lists are 'without limitation' or are defined 'at the time of the transaction' to which they apply. Problems arise, however, when a party to a transaction becomes sanctioned after the adoption of an agreement. Companies are increasingly attempting to account for this possibility with the inclusion of termination provisions triggered by changes in the sanctions status of any party, and they may even define a mechanism for unwinding the transaction in compliance with applicable regulations.

Conclusion

For sanctions practitioners, advising clients in APAC can be both intellectually challenging and professionally rewarding. Whereas in some places the answer to most questions about sanctions is a hard 'no', the answer in this region is often 'maybe', subject to the circumstances. Clients expect their advisers to understand the ins and outs of international sanctions rules and be prepared to justify the advice given. Situational awareness is paramount. With enforcement and geopolitical risks rising, practitioners require both operational and decision-making skills – due diligence, legal analysis, risk assessment, strategic guidance – to lead their clients through uncharted, sometimes perilous, legal terrain.

CHAPTER 12

Developments in the Chinese Mainland and Hong Kong

Qing Ren, Deming Zhao and Ningxin Huo[1]

Introduction

This chapter provides an overview of the export control regime, the technology export administration regime and the sanctions and countermeasures regimes in the Chinese mainland, with a particular focus on developments in 2022. It also surveys export controls and sanctions in the Hong Kong Special Administrative Region (HKSAR).

Export controls in the Chinese mainland

On 29 December 2021, the State Council Information Office released the 'China's Export Controls' white paper,[2] which sets out China's basic positions upholding multilateral, fair and non-discriminatory export controls. The main purpose of China's export control regime is to safeguard the country's national security and to fulfil its non-proliferation and other international obligations. China endeavours to maintain a balance between development and opening up to the international economy, on the one hand, and security, on the other hand, and stands firmly against the proliferation of all forms of weapons of mass destruction (WMD) and their delivery systems. Further, China advocates increased representation for emerging markets and developing countries in international coordination on export controls, opposes the abuse of export control measures

1 Qing Ren and Deming Zhao are partners, and Ningxin Huo is an associate, at Global Law Office. The authors acknowledge the contributions of Yiqi Du and Calvin Jin to this chapter.

2 'Full Text: China's Export Controls', at https://english.www.gov.cn/archive/whitepaper/202112/29/content_WS61cc01b8c6d09c94e48a2df0.html.

and maintains the stand that export controls should not undermine the legitimate right of other countries to the peaceful use of controlled items, obstruct normal international science and technology exchanges and economic and trade cooperation, or disrupt the secure and smooth operation of global industrial and supply chains.

Based on these positions, China currently maintains a relatively modest export control regime. As for the scope of controlled items, items on the multilateral non-proliferation control list constitute the main body of China's dual-use export control list. Many of the dual-use items covered by the Wassenaar Arrangement are not currently controlled in China. China's Export Control Law (ECL)[3] also limits its reach of extraterritorial jurisdiction, and it is expected that, unlike the abuse of export control measures by other countries against China, the Chinese government would show self-constraint in enforcing those provisions with extraterritorial effect.

Nevertheless, the ECL, drawing upon the experiences of the United States and other countries, enhances China's export control regime. For instance, the ECL:

- expands the scope of controlled items in general;
- covers re-exports and deemed exports in addition to exports;
- strengthens the controls on end users and end use (e.g., establishing a restricted names list);
- grants broad enforcement and investigative powers to the export control authority; and
- significantly increases the penalties on export control violations.

To address the exposures under the ECL, export business operators (EBOs) in China (including Chinese subsidiaries of foreign companies), as well as overseas importers, end users and re-exporters, need to establish and implement an internal compliance programme (ICP) pursuant to the ICP guidelines from the export control authority.

On 12 February 2023, the Ministry of Commerce (MOFCOM), the leading export control authority in China, issued a circular entitled 'Notice of the General Office of the Ministry of Commerce on Further Improving the Export Controls

3 The Export Control Law of the People's Republic of China (adopted at the 22nd Meeting of the Standing Committee of the Thirteenth National People's Congress of the People's Republic of China on 17 October 2020, and entered into force on 1 December 2020). See the English version of the Export Control Law (ECL) at www.npc.gov.cn/englishnpc/c23934/202112/63aff482fece44a591b45810fa2c25c4.shtml.

of Dual-Use Items',[4] which specifies the duties of commercial departments at the provincial level. The provincial commercial departments are expected to promote publicity of, and training in, export control laws and regulations, encourage EBOs to establish ICPs, guide EBOs in complying with licensing procedures and intensify ECL enforcement and investigation. The Notice demonstrates MOFCOM's intentions to enforce the ECL against violations. The EBOs and foreign parties dealing with items imported from China are advised to conduct a risk assessment to establish whether they would survive an investigation by MOFCOM or China Customs.

Laws and regulations

Since its enforcement on 1 December 2020, the ECL has unified the previous fragmented export control regime in China with a comprehensive new framework for regulating exports of goods, technologies and services.

Under the ECL, six existing administrative regulations, issued by the State Council, and their implementing rules currently remain effective:

1 Regulations on the Administration of Controlled Chemicals;
2 Regulations on the Control of Nuclear Export;
3 Regulations on Administration of Arms Export;[5]
4 Regulations on the Control of Nuclear Dual-use Items and Related Technologies Export;
5 Regulations on Export Control of Missiles and Missile-related Items and Technologies; and
6 Regulations on Export Control of Dual-use Biological Agents and Related Equipment and Technologies.

On 22 April 2022, MOFCOM released the Regulations on Export Control of Dual-Use Items (Draft for Public Comments) (the Draft Regulations),[6] which will apply to all dual-use items (except for controlled chemicals) and will replace the regulations in points (4) to (6), above.

---

4 The Ministry of Commerce (MOFCOM), 'Notice of the General Office of the Ministry of Commerce on Further Improving the Export Controls of Dual-Use Items' (Chinese), at www.mofcom.gov.cn/article/zwgk/gkzcfb/202302/20230203384654.shtml.

5 The Regulations on Administration of Arms Export was promulgated by the Central Military Commission as well as the State Council.

6 MOFCOM, 'Notice of Public Consultation on the Regulations on Export Control of Dual-Use Items (Draft for Public Comments)' (the Draft Regulations). Unless otherwise stated, the provisions of the Draft Regulations are not reflected in this chapter.

According to the Draft Regulations, China may:

- adopt an export control classification numbering system for controlled items;
- abolish the registration requirement for the export business of dual-use items (except for controlled chemicals); and
- establish a multi-type licensing system, including licences for a single transaction, general licences and licensing exceptions.

The Draft Regulations may further clarify the obligations of EBOs in terms of item classification, record-keeping and establishment of ICPs.

Furthermore, China's Foreign Trade Law, National Security Law, Data Security Law, Nuclear Safety Law, Customs Law, Administrative Licensing Law, Administrative Punishment Law and Criminal Law also provide legal bases for the enforcement of export control measures.

Competent authorities

According to the ECL, the departments of the State Council and the Central Military Commission (CMC) that perform the export control functions (collectively, the State Export Control Administrative Departments (SECADs)) are responsible for tasks relating to export control according to their assigned duties.[7] The respective responsibilities of the SECADs are set forth below.

Items	Administrative departments for export control
Nuclear dual-use items	Ministry of Commerce (MOFCOM) jointly with the China Atomic Energy Authority (CAEA)
Dual-use biological items	MOFCOM jointly with the Ministry of Agriculture and Rural Affairs and the National Health Commission, among others, as required
Dual-use items related to certain chemical	MOFCOM
Dual-use missile-related items	MOFCOM jointly with the State Administration of Science, Technology and Industry for National Defence (SASTIND) and the Central Military Commission's (CMC) Equipment Development Department (EDD), and others, as required
Commercial cryptography	MOFCOM jointly with the State Cryptography Administration
Controlled chemicals	The Ministry of Industry and Information Technology regulates exporter accreditation jointly with MOFCOM, and is responsible for undertaking the specific export review

7 Article 5 of the ECL.

Items	Administrative departments for export control
Military products	SASTIND and CMC's EDD
Nuclear materials	CAEA and MOFCOM, in cooperation with other departments

Controlled items

The ECL applies to the following 'controlled items':

- dual-use items, which refers to goods, technologies, services and other items that have both civil and military uses or contribute to the enhancement of military potential, including, particularly, those that can be used to design, develop, produce or deploy WMD and their means of delivery;
- military items, which refers to equipment, special production facilities and other relevant goods, technologies and services used for military purposes;
- nuclear items, which refers to nuclear materials, nuclear equipment, non-nuclear materials for reactors and related technologies and services; and
- other goods, technologies, services and other items related to safeguarding national security and interests and fulfilling international obligations such as non-proliferation.[8]

An item is not automatically subject to control measures merely because it falls within the above general definition of 'controlled items'; it depends on whether the item is:

- included in an export control list;[9]
- subject to temporary controls;[10]
- prohibited from exportation;[11] or
- subject to the catch-all control.[12]

The control lists are formulated and promulgated by the SECADs jointly with other relevant departments following prescribed procedures.[13] Control lists that are currently in force include the following:

- Arms Export Control List (2002);
- Nuclear Export Control List (2018);
- Nuclear Dual-use Items and Related Technologies Export Control List (2017);

8 id., at Article 2.
9 id., at Article 9.
10 ibid.
11 id., at Article 10.
12 id., at Article 12(3).
13 id., at Article 9.

- Biological Dual-Use Items and Related Equipment and Technologies Export Control List (2006);
- List of Schedules of Controlled Chemicals (2020);
- Certain Chemicals and Related Equipment and Technologies Export Control List (2002);
- Missiles and Missile-related Items and Technologies Export Control List (2002); and
- Commercial Cryptography Export Control List (2020).

Upon approval of the State Council, or both the State Council and the CMC, SECADs may impose temporary controls or prohibitions by means of announcements. Temporary controls over potassium perchlorate (HS code 2829900020)[14] and certain high-pressure water cannons (and the main components and ancillary equipment specially designed for those cannons) (HS code 8424899920) entered into force in 2022.[15] In addition, the export of certain dual-use items and technologies to North Korea has been prohibited since 2013 for the purpose of implementing United Nations Security Council (UNSC) resolutions.[16]

In general, all the above-mentioned control lists (except for the Arms Export Control List) and temporary controls are consolidated into the Catalogue of Dual-use Items and Technologies Subject to Export Licence Management, the latest version of which was promulgated by MOFCOM and the General Administration of Customs on 30 December 2022.[17]

14 Announcement [2021] No. 46 of MOFCOM and the General Administration of Customs: Announcement on Export Controls of Potassium Perchlorate (entered into force on 1 April 2022).

15 Announcement [2022] No. 31 of MOFCOM, the General Administration of Customs and the State Administration of Science, Technology and Industry for National Defence: Announcement on Export Controls of Products related to High Pressure Water Cannons (entered into force on 1 December 2022).

16 Announcement [2013] No. 59 of MOFCOM, the Ministry of Industry and Information Technology and the General Administration of Customs: Announcement of the List of Dual-use Items and Technologies Prohibited from Export to North Korea (entered into force on 23 September 2013).

17 Announcement [2022] No. 42 of MOFCOM and the General Administration of Customs: Catalogue of Dual-use Items and Technologies Subject to Export Licence Management (entered into force on 1 January 2023).

The 2023 Catalogue includes the following 11 categories of items.

No.	Category of controlled items	Numbers of controlled items
1	Items and technologies in the Nuclear Export Control List	159
2	Items and technologies in the Nuclear Dual-use Items and Related Technologies Export Control List	204
3	Items and technologies in the Biological Dual-use Items and Related Equipment and Technologies Export Control List	144
4	Items in the List of Schedules of Controlled Chemicals	74
5	Items and technologies in the Certain Chemicals and Related Equipment and Technologies Export Control List	38
6	Items and technologies in the Missiles and Missile-related Items and Technologies Export Control List	186
7	Precursor chemical (I)	54
8	Precursor chemical (II)	17
9	Certain dual-use items and technologies	6
10	Special civil items and technologies	11
11	Items in the Commercial Cryptography Export Control List	11

Like other countries, China adopts catch-all controls. Specifically, any items that are neither included in the control lists nor subject to temporary controls will be subject to the export control licensing requirement where an EBO is, or should be, aware or is notified by the SECADs that the item may pose any of the following risks:

- endangering national security and interests;
- being used to design, develop, produce or use WMD and their means of delivery; and
- being used for the purposes of terrorism.[18]

Covered activities

The ECL applies to the following activities:

- transfer of controlled items from within the territory of China to outside China ('cross-border transfer');[19]
- provision of controlled items to foreign natural persons or entities by Chinese citizens or entities ('providing controlled items to foreigners');[20]

18 Article 12(3) of the ECL.

19 id., at Article 2.

20 ibid.

- transit, transshipment and through-shipment of controlled items;[21]
- re-export of controlled items;[22] and
- facilitation of export control violations.[23]

'Cross-border transfers' are not limited to exports in trade; they also include transfers that occur in overseas investments, exhibitions abroad, international scientific and technological cooperation and foreign aid.[24] In addition to physical border crossings, technology and data may cross the border by email, instant messaging, uploading to offshore websites, etc.

The scope of 'providing controlled items to foreigners' seems to be broader than that of 'deemed export' under the US export control law, because on its face: (1) it applies to goods and services, in addition to technologies and software; and (2) it could take place either within or outside China. It is particularly relevant to technology companies and may cause difficulties in respect of inter-company research and development where employees of different nationalities work together. The precise coverage of 'providing controlled items to foreigners' is expected to be clarified in the implementing regulations that are yet to be promulgated.[25]

Re-export under Article 45 seems to only cover export of Chinese-origin controlled items (as opposed to any foreign products that contain a certain percentage of Chinese-origin controlled items) from one foreign country or region to another, subject to future clarification in the implementing regulations that are yet to be promulgated.[26]

Article 20 prohibits any organisations or persons from facilitating violations of export controls by acting as an agent or providing freight, delivery, customs declarations, third-party e-commerce trading platforms, financial services or other services. Article 36 further provides corresponding legal liabilities.

---

21 id., at Article 45.

22 ibid.

23 id., at Article 20.

24 e.g., Article 2 of the Regulations on the Control of Nuclear Dual-use Items and Related Technologies Export; Article 2 of the Regulations on Export Control of Missiles and Missile-related Items and Technologies.

25 The Draft Regulations have not clarified the meaning of 'providing controlled items to foreigners'.

26 The Draft Regulations have not clarified the definition of 're-export'.

Control measures

The ECL establishes a range of control measures, including qualification, licensing requirement, 'end users and end uses' control and a restricted names list.

Qualification

Military items must be exclusively exported by EBOs with export monopoly qualifications for military items[27] (i.e., arms trading companies approved by the Ministry of Industry and Information Technology (MIIT) and the CMC's Equipment Development Department).[28] The qualifications of EBOs for dual-use items, nuclear items and other controlled items are subject to requirements of other laws and regulations.[29] Currently, EBOs wishing to engage in the export of all dual-use items are required to be registered with MOFCOM;[30] the export of certain controlled chemicals can only be undertaken by entities designated by both MIIT and MOFCOM.[31] The export of nuclear items can only be undertaken by entities designated by the State Council.[32]

Licensing

Article 12 imposes a licensing requirement for the export of controlled items that are on a control list, subject to temporary controls or within the scope of the catch-all control. Transit, transshipment, through-shipment and re-export of these items may also require a licence.[33] A licence application will be examined by MOFCOM[34] or other competent SECADs. For certain significant exports, approval by the State Council or the CMC, or both, is also required.

The SECADs may consider the following factors when determining whether to grant licences:

- national security and interests;
- international obligations and commitments;
- type of export;

---

27 Article 23 of the ECL.

28 Articles 7, 8 and 20 of the Regulations on Administration of Arms Export.

29 Article 11 of the ECL.

30 Articles 2 and 3 of the Administrative Measures for the Registration of the Export Operation of Sensitive Items and Technologies. According to the Draft Regulations, the registration requirements for the export of dual-use items will be abolished.

31 Article 14 of the Regulations on Administration of Controlled Chemicals.

32 Article 6 of the Regulations on Nuclear Export Control.

33 Article 45 of the ECL.

34 MOFCOM receives applications and informs the applicants of its decisions via an online platform (https://ecomp.mofcom.gov.cn/loginCorp.html).

- sensitivity of controlled items;
- destination country or region of export;
- end users and end uses;
- the exporter's relevant credit record; and
- other factors as prescribed by laws and administrative regulations.[35]

In addition to licences authorising individual export transactions, SECADs may issue general licences to EBOs that have established internal export compliance programmes,[36] authorising multiple export transactions within a period of three years.[37]

End users and end uses

The ECL attaches great importance to the management of 'end users and end uses'. In particular:

- EBOs are required to submit end-user and end-use statements to the SECADs;[38]
- end users must undertake not to alter the end use of the controlled items concerned or assign the items to any third party without the approval of the SECADs;[39]
- EBOs and importers are required to immediately report to the SECADs when they become aware of any possible change of the end user or end use;[40] and
- the SECADs should establish a risk management system to assess and verify the end users and end uses,[41] which implies that the SECADs may conduct on-site verification when necessary.

---

35 Article 13 of the ECL.

36 Additional requirements for the application of general licences (Article 7 of the Administrative Measures for General Licence of Exports of Dual-use Items and Technologies).

37 A Class A general licence authorises an export business operator (EBO) to export one or more specified items and technologies to one or more end users in one or more countries or regions within the valid period, while a Class B general licence authorises an EBO to export the same items and technologies to the same end user in the same country or region multiple times (Administrative Measures for General Licence of Exports of Dual-use Items and Technologies (Chinese), at http://exportcontrol.mofcom.gov.cn/article/zcfg/gnzcfg/zcfggzqd/202111/505.html).

38 Article 15 of the ECL.

39 id., at Article 16.

40 ibid.

41 id., at Article 17.

Restricted names list

SECADs are authorised under Article 18 to establish a restricted names list, listing foreign importers and end users that are found to be involved in any of the following:

- violating the requirements regarding the management of end users or end uses;
- potentially endangering national security or interests; and
- using controlled items for any terrorism purpose.

The SECADs may, among other things, prohibit or restrict the listed parties from engaging in transactions relating to relevant controlled items, or order the suspension of the export of controlled items. The term 'transactions' seems to cover more than export. However, given that the scope of controlled items is narrower than the items subject to the US Export Administration Regulations, the consequence of being listed in the restricted names list seems less severe, compared with that of being listed in the US Commerce Department's Bureau of Industry and Security (BIS) Entity List.

Enforcement and investigation

According to Article 28 of the ECL, the SECADs may take the following measures when conducting an investigation of suspected violations of the ECL:

- enter the business premises of the investigation subject or other relevant premises for inspection;
- make enquires of the investigation subject, interested parties and other relevant organisations or individuals, and request that they explain matters related to the event under investigation;
- consult and copy relevant documents, agreements, accounting books, business correspondence and other documents and materials of the investigation subject, interested parties and other relevant organisations or individuals;
- inspect the means of transport used for export, stop the loading of suspicious export items and order the return of illegally exported items;
- seal up and seize relevant items involved in the case; and
- examine the investigation subject's bank accounts.

Article 19 of the ECL further requires that:

- relevant departments of the State Council and local governments should assist the SECADs in carrying out their duties in accordance with the law; and
- relevant organisations and persons should cooperate and should not reject or impede the supervision and administration work of the SECADs.

Penalties

Articles 33 to 38 of the ECL provide seven types of administrative penalties for nine types of violations, respectively, including warnings, orders to stop illegal activities, confiscation of illegal gains, fines, orders to suspend business for rectification, revocation of licences and revocation of the qualification for exporting relevant controlled items.

Notably, fines apply to all nine types of violations and the amount of the fines prescribed is relatively high. For example, an EBO that exports controlled items without obtaining the required qualification, without a licence or beyond the scope of the licence will be subject to a fine of not less than five times and not more than 10 times the amount of the EBO's illegal turnover.[42] Consequently, assuming that the illegal turnover is 100 million yuan, the fine could be up to 1 billion yuan. Any person facilitating export control violations may be fined three to five times the illegal turnover, while an EBO entering into a transaction with an importer or end user on the restricted names list may face a fine of 10 to 20 times the illegal turnover.

Apart from the above administrative penalties, the SECADs may refuse to accept a licence application submitted by an EBO that has been penalised for export control violations for up to five years, while persons in charge of the EBO and other persons who are directly responsible for the violations may be prohibited from engaging in the relevant export business activities for five years, or even for life for those who have been charged with criminal offences.[43]

Additionally, persons who export items prohibited from exportation, or export controlled items without approval, could be found criminally liable in accordance with the law.[44] 'Criminal liability' in this context may refer to, inter alia, smuggling or illegal business operations under China's Criminal Law 1997 (last revised in 2020).

42 id., at Article 34.

43 id., at Article 39(1).

44 id., at Article 43(2).

In 2022, there were several instances in which EBOs violated the ECL by exporting controlled items (such as graphite cored wire)[45] without licences, and Chinese customs authorities imposed fines in accordance with Article 34 of the ECL.[46] To date, neither MOFCOM nor other SECADs have imposed fines or other penalties under the ECL.

With respect to criminal liability, in 2022 Chinese courts sentenced defendants to imprisonment in at least two cases for exporting ammonium chloride to Myanmar without the licences required.[47]

Internal compliance programme

In 2021, MOFCOM issued the Guiding Opinions on the Establishment of Internal Compliance Mechanisms for Export Control by Exporters of Dual-use Items,[48] with a detailed 37-page Guide to Internal Compliance with Export Controls of Dual-use Items as an appendix thereto.[49]

EBOs are advised to establish an ICP with the following nine elements:

- compliance policy;
- compliance governance structure;
- comprehensive risk assessment;
- transaction review procedure;
- emergency response measures (i.e., handling violations and taking corrective measures);
- education and training;
- audits;
- record-keeping; and
- building and maintaining an export compliance manual.

45 Tianjin Customs, Administrative Penalty Decision [2022] Jin Xin Gang Guan Ji Cha/Wei Zi No. 0063.

46 In some cases, Chinese customs authorities impose fines for the export of controlled items without licences in accordance with the Customs Law and its implementing regulations. For example, Guangdong Customs, Administrative Penalty Decision [2022] Nan Guan Ji Wei Zi No. 0185.

47 Intermediate People's Court of Xishuangbanna Dai Autonomous Prefecture, Yunnan Province (2022) Yun 28 Xing Chu No. 2; Intermediate People's Court of Dalian City, Liaoning Province (2022) Liao 02 Xing Chu No. 37.

48 www.mofcom.gov.cn/article/zwgk/zcfb/202104/20210403056267.shtml (Chinese).

49 http://images.mofcom.gov.cn/aqygzj/202104/20210428182950304.pdf (Chinese).

These elements are largely identical or similar to those in other jurisdictions such as the United States and the European Union, although they differ in the detail. Therefore, Chinese subsidiaries of multinational companies that have established ICPs based on requirements or guidelines of other jurisdictions would normally not find it difficult to adapt their existing ICPs to MOFCOM's Guiding Opinions in terms of general methodologies and structure, while most of the adaption or adjustment would focus on the substantive requirements of China's export control regime, as noted above.

Administration of technology export in the Chinese mainland

In addition to the above-mentioned export control regime, China maintains a separate administration regime for technology export under the Regulations on the Administration of Technology Import and Export (TIER).[50]

The TIER applies to the transfer of technologies from inside the territory of China to outside the territory of China by way of trade, investment or economic and technological cooperation, including the transfer of patent rights, patent application rights, patent licensing, know-how and technology services.[51] However, export of nuclear technologies, dual-use nuclear technologies, technologies concerning the production of controlled chemicals, military technologies and other export control technologies is subject to the ECL and its implementing regulations.[52]

Under the TIER, technologies are divided into three categories: permitted (i.e., no restriction), restricted and prohibited. Contracts of permitted technology export shall be reported to the competent authority for record-filing; restricted technology shall not be exported without an export licence; and technologies within the prohibited category are forbidden from export.[53] The Catalogue of Technologies Prohibited and Restricted from Export (the Catalogue) was promulgated by MOFCOM and the Ministry of Science and Technology in 2001, and amended in 2008 and 2020, respectively. The 2020 version of the Catalogue, while removing certain technologies from the prohibited and restricted categories, added a number of technologies to the restricted category, including

50 The Regulations of the People's Republic of China on the Administration of Technology Import and Export (promulgated on 10 December 2001 and most recently revised on 29 November 2020 by the State Council). See the Chinese version of the Regulations at www.gov.cn/gongbao/content/2019/content_5468926.htm.

51 id., at Article 2.

52 id., at Article 43.

53 id., at Articles 37, 31 and 30.

some emerging technologies such as 3D printing technology, unmanned aerial vehicle technology, information defence technology, artificial intelligence interactive interface technology and personalised push service technology based on data analysis.[54]

On 30 December 2022, MOFCOM published an announcement to solicit comments on a new revision of the Catalogue (the 2022 Draft Catalogue).[55] Compared with the 2020 version, the 2022 Draft Catalogue proposes to:

- remove 32 technologies (five prohibited and 27 restricted) within several industries, such as raw materials and chemical products manufacturing, general equipment manufacturing, special equipment manufacturing, agriculture, forestry, animal husbandry and fishery;
- revise the control points or parameters of 36 technologies (seven prohibited and 29 restricted), including core computer hardware manufacturing technology, drone technology and information processing technology; and
- add seven new technologies (one prohibited and six restricted), including human cell cloning and gene editing technology, photovoltaic silicon chip manufacturing technology, lidar systems and synthetic biology technology.

Since 2007, MOFCOM has delegated the authority for reviewing and approving the export of restricted technologies to commercial departments at the provincial level.[56] Upon receipt of an application for technology export, the competent commercial department shall, within 30 working days, review the application in conjunction with the competent science and technology department, make a decision on approval or non-approval, and, in the case of approval, issue a letter of intent for technology export licence. An applicant may engage in substantive negotiations and sign a technology export contract with foreign parties only after having obtained the aforesaid letter of intent. After having signed a technology export contract, the applicant shall apply for the technology export licence. The competent commercial department shall examine the authenticity of the technology export contract and decide whether to grant the technology export licence

54 Announcement [2020] No. 38 of MOFCOM and the Ministry of Science and Technology: Announcement on the Amendment and Release of China's Catalogue of Technologies Prohibited and Restricted from Export (entered into force on 28 August 2020).

55 MOFCOM, 'Notice of Public Consultation on the Revision of China's Catalogue of Technologies Prohibited and Restricted from Export'.

56 Article 4 of the Administrative Measures on Prohibition and Restriction of Exported Technologies.

within 15 working days of receipt of the application. The relevant technology export contract shall come into effect as of the date of issuance of the technology export licence.[57]

Sanctions and countermeasures in the Chinese mainland

China's economic sanctions regime is defensive rather than offensive in nature. Apart from following the multilateral sanctions adopted by the UNSC, it primarily aims at countering sanctions perceived as abusive by foreign countries against China. In terms of countermeasures, MOFCOM has issued two departmental rules, namely, (1) the Provisions on the Unreliable Entity List (the UEL Provisions), which target certain foreign entities that impose discriminatory measures against Chinese entities,[58] and (2) the Rules on Counteracting Unjustified Extraterritorial Application of Foreign Legislation and Other Measures (the Counteracting Rules),[59] which block certain foreign legislation or measures that prohibit or restrict normal economic activities between Chinese entities and third-state parties. Furthermore, under the Anti-Foreign Sanctions Law (AFSL),[60] individuals and entities advancing discriminatory restrictive measures that interfere in China's internal affairs (intrusive measures) may be sanctioned by China. Most recently, two provisions have been proposed in the Foreign Relations Law (Draft)[61] (published on 30 December 2022) to provide additional legal bases for the enforcement of UNSC sanctions and the implementation of countermeasures, respectively.

As a compliance measure, entities in China are recommended to screen their counterparties against the UNSC sanctions lists and China's AFSL List and Unreliable Entity List (UEL) and avoid transactions with parties designated on

---

57 id., at Articles 6, 10, 11, 13, 14 and 15.

58 The Provisions on the Unreliable Entity List (the UEL Provisions) (MOFCOM Order No. 4 [2020], promulgated and entered into force on 19 September 2020). See the English version at http://english.mofcom.gov.cn/article/policyrelease/questions/202009/20200903002580.shtml.

59 The Rules on Counteracting Unjustified Extraterritorial Application of Foreign Legislation and Other Measures (MOFCOM Order No. 1 [2021], promulgated and entered into force on 9 January 2021). See the English version at http://english.mofcom.gov.cn/article/policyrelease/announcement/202101/20210103029708.shtml.

60 The Anti-Foreign Sanctions Law of the People's Republic of China (AFSL) (adopted at the 29th Meeting of the Standing Committee of the Thirteenth National People's Congress of the People's Republic of China and entered into force on 10 June 2021). See the Chinese version at www.npc.gov.cn/npc/c30834/202106/d4a714d5813c4ad2ac54a5f0f78a5270.shtml.

61 The Foreign Relations Law (Draft) published on 30 December 2022. See the Chinese version at www.npc.gov.cn/flcaw/flca/ff808181844232f70185611f164d4045/attachment.pdf.

these lists. Both Chinese and foreign entities also need to proactively identify, assess and prevent the risk of being sued in China by implementing intrusive measures.

Anti-Foreign Sanctions Law

The AFSL mainly targets intrusive measures that are adopted by foreign countries against Chinese citizens or organisations in violation of international law and the basic norms of international relations and that interfere in China's internal affairs to contain or suppress China.[62] In practice, those sanctions imposed by countries against state organs, organisations and individuals (including public servants) of China in respect of Xinjiang, Tibet, Taiwan and Hong Kong-related issues are most likely to fall within the scope of intrusive measures. Additionally, the AFSL is also applicable to actions that endanger the national sovereignty, security and development interests of China.[63]

To counter intrusive measures, the AFSL authorises the relevant departments of the State Council to designate individuals and organisations directly or indirectly involved in the formulation, decision and enforcement of intrusive measures (listed persons) into the AFSL List,[64] and imposes the following countermeasures:

- denial of issuance of visas, denial of entry, cancellation of visas or deportation;
- sealing up, distraining and freezing movable and immovable property and other types of property within the territory of China;
- prohibiting or restricting organisations and individuals within the territory of China from conducting relevant transactions, cooperating or carrying out other activities with them; and
- other necessary measures.[65]

Article 5 of the AFSL further authorises relevant departments of the State Council to take countermeasures against persons that have certain connections with listed persons, including:

- the spouse and direct lineal family members of the individuals included in the AFSL List;
- the senior managers or actual controllers of the organisations included in the AFSL List;

62 Article 3 of the AFSL.

63 id., at Articles 13 and 15.

64 id., at Article 4.

65 id., at Article 6.

- the organisations in which the individuals included in the AFSL List serve as senior managers; and
- the organisation in which the individuals or organisations included in the AFSL List actually control or participate in the establishment and operation.

Article 12 of the AFSL has been widely discussed for its 'blocking law' nature. Under Article 12(1), any organisation or individual shall not implement or assist in the implementation of intrusive measures. Article 12(2) provides that where any organisation or individual violates Article 12(1) and thus infringes the legitimate rights and interests of any Chinese citizen or organisation, the Chinese citizen or organisation may, in accordance with the law, file a lawsuit with a Chinese court to request the cessation of infringement and compensation for any loss. How the Chinese courts will apply this provision remains to be seen.

Prior to the adoption of the AFSL, the Ministry of Foreign Affairs (MFA) had announced several countermeasures in response to foreign sanctions and interference.[66] After the AFSL entered into force, the MFA expressly invoked it as the legal basis for its actions in several announcements. Notably, on 23 December 2022, the MFA issued its first decision in the form of a ministerial order that explicitly invoked Articles 4, 5 and 6 of the AFSL, specified the content and the effective date of the countermeasures, and attached the AFSL List as an annex to the order.[67] This indicates a more standardised implementation of the AFSL.

66 For example, on 21 January 2021, China imposed sanctions on 28 US persons who had seriously violated China's sovereignty and who it believes have been mainly responsible for the anti-China movement of the US. These individuals and their immediate family members are prohibited from entering the Chinese mainland, Hong Kong and Macau. They, and companies and institutions associated with them, are also restricted from doing business with China. See the Foreign Ministry Spokesperson's Announcement, at www.fmprc.gov.cn/web/fyrbt_673021/t1847570.shtml.

67 Ministry of Foreign Affairs, Order No. 4, Decision on Countermeasures against Miles Maochun Yu and Todd Stein.

Unreliable Entity List

Under the UEL Provisions, a foreign entity or individual may be added to the UEL by the Chinese government if it: (1) endangers the national sovereignty, security or development interests of China; or (2) stops, in violation of normal market transaction principles, supplying to, or discriminates against, a Chinese company that suffers serious damage as a result.[68]

If included on the UEL, a foreign entity or individual may, among other things, not be able to trade with or invest in China if the Chinese government so determines at its own discretion.[69] Accordingly, the UEL listing may have a far-reaching impact, if compared with inclusion on the restricted names list under the ECL. The restricted names list only impacts the export of controlled items.

On 16 February 2023, on behalf of the UEL Working Mechanism, MOFCOM issued the first decision under the UEL Provisions, designating two companies (Lockheed Martin Corporation and Raytheon Missiles & Defense) engaged in arms sales to the Taiwan region to the UEL and taking the following measures:

- prohibiting them from engaging in China-related import and export activities;
- prohibiting them from increasing or expanding investment in China;
- prohibiting the senior management personnel of the two companies from entering China;
- denying and revoking the work permit, the status of stay or residence of senior management personnel of the two companies in China; and
- imposing fines on the two companies in the amount of twice the value of their arms sales contracts with the Taiwan region since the implementation of the UEL Provisions.[70]

68 Article 2 of the UEL Provisions. It is not entirely clear from the text whether conditions (1) and (2) are accumulative or alternative. However, from the first designation decision on 16 February 2023, it seems that condition (1) is a necessary condition but condition (2) is not.

69 id., at Article 10.

70 Notice of the Unreliable Entity List Working Mechanism on the Listing of Lockheed Martin Corporation and Raytheon Missiles & Defense on the Unreliable Entities List [2023] No. 1, at www.mofcom.gov.cn/article/zwgk/gkzcfb/202302/20230203391289.shtml.

Counteracting Rules

The Counteracting Rules apply to situations in which the extraterritorial application of foreign legislation and other measures, in violation of international law and the basic principles of international relations, unjustifiably prohibits or restricts Chinese entities or individuals from engaging in normal economic, trade and related activities with a third state (or region) or its entities or individuals.[71]

Unlike the approach of the EU Blocking Statute, the Counteracting Rules do not identify which foreign legislation or other measures are blocked, but provide a working mechanism led by MOFCOM to determine which foreign legislation or other measures shall be blocked.[72] It has thus led to different readings as to the scope of its application. It is commonly held that the Counteracting Rules apply to US 'secondary sanctions' as these sanctions prohibit or restrict Chinese parties from entering into certain transactions with third-state or third-region parties. However, it is unclear whether the Counteracting Rules may also apply to other circumstances. For example, it remains to be seen whether the Counteracting Rules apply to: (1) certain US primary sanctions to the extent they prohibit or restrict Chinese parties' transactions with third-state or third-region parties with a 'US-nexus' (e.g., US dollar payment or transfer through the US financial system); or (2) certain US export control rules to the extent that they prohibit or restrict Chinese parties from re-exporting Chinese-origin products with US content (e.g., *de minimis* rule and foreign direct product rule). Further, there are discussions regarding whether Chinese companies designated on the US Treasury Department's Office of Foreign Assets Control's (OFAC) Specially Designated Nationals and Blocked Persons List (the SDN List) or the BIS Entity List may also invoke the Counteracting Rules.

The Counteracting Rules establish a reporting requirement; namely, any Chinese party that encounters the above-mentioned prohibition or restriction by foreign legislation and other measures must truthfully report these matters to MOFCOM within 30 days.[73]

The Counteracting Rules establish the working mechanism to determine whether the above-mentioned prohibition or restriction constitutes unjustified extraterritorial application,[74] and, if so, to issue a prohibition order to the effect that the relevant foreign legislation and other measures shall not be recognised,

71 Article 2 of the Counteracting Rules.

72 id., at Article 4.

73 id., at Article 5.

74 id., at Article 6.

executed or complied with.[75] Chinese parties are required to comply with these prohibition orders; that is, they are prohibited from complying with the foreign law or measure within the scope of the prohibition order, unless they obtain an exemption from MOFCOM.[76] Otherwise, a penalty and suit for damages may follow.[77]

A foreign party may also risk facing a lawsuit in China to redress any benefits gained from a foreign suit derived from the foreign legislation blocked by China.[78]

To date, no prohibition orders have been issued.

Implementation of UN sanctions

China does not have specific laws or regulations on how to implement UNSC sanctions. Generally, after a UN sanctions-related resolution is adopted or a UN sanctions list is updated, the MFA will issue a notice publicising the resolution or list. For example, the Notice on the Implementation of the Sanctions List of the UNSC ISIL (Da'esh) and Al-Qaida Sanctions Committee[79] was issued by the MFA to notify relevant parties that the sanctions list had been updated, and all relevant authorities and entities were requested to take corresponding measures to implement the updated list. In 2022, the MFA issued a total of 21 notices on the implementation of UNSC sanctions-related resolutions regarding the adoption of sanctions resolutions, updates to sanctions lists, extensions of sanctions measures, humanitarian assistance exemptions and other relevant issues under a number of sanctions programmes, such as those concerning Afghanistan, ISIL and Al-Qaida, Yemen, Iraq, the Democratic Republic of the Congo, South Sudan, Libya, Mali, Haiti, Central Africa and Somalia.

After the MFA issues its notices, relevant authorities may, within their own jurisdiction, issue further notices or take other measures to implement UN sanctions. For instance, to implement UN sanctions against North Korea, MOFCOM, along with other authorities, has promulgated the following announcements since 2017:

- Announcements Nos. 9 [2017], 17 [2018] and 36 [2018], prohibiting exports of certain dual-use items and technologies to North Korea;

75 id., at Article 7.
76 id., at Article 8.
77 id., at Article 13.
78 id., at Article 9.
79 Notice No. 11 [2022].

- Announcements Nos. 47 [2017] and 55 [2017], prohibiting new investment from North Korea to China, or vice versa, and requiring the closure of existing North Korean-invested enterprises in China and overseas joint ventures established by and between Chinese enterprises and North Korean entities or individuals; and
- Announcements Nos. 40 [2017] and 52 [2017], prohibiting imports of coal, iron, iron ore, lead, lead ore, water, seafood and textile products from North Korea, prohibiting exports of condensate and liquefied natural gas to North Korea and restricting exports of refined petroleum products to North Korea.

Notably, there is a general requirement for the banking sector to implement UN sanctions.[80]

To improve China's implementation of UNSC sanctions, a dedicated article has been proposed to be included in China's upcoming Foreign Relations Law. Article 35 of the Foreign Relations Law (Draft) first states a general policy that China will take measures to implement the binding sanctions adopted by the UNSC under Chapter VII of the UN Charter. It also authorises the MFA to publicise UNSC sanctions and relevant ministries and provincial governments to take measures to implement UNSC sanctions within their respective competence. Finally, Article 35 requires that individuals and organisations shall comply with the measures implementing the UNSC sanctions and shall not engage in activities in violation of the UNSC sanctions.

HKSAR: Gateway to the East and West

HKSAR implements strategic trade control in accordance with the Import and Export Ordinance (Cap 60) and its subsidiary legislation, the Import and Export (Strategic Commodities) Regulations (Cap 60G), Schedule 1 of which sets out the lists of strategic commodities, namely, the Strategic Commodities Control List.[81]

---

80 Article 20 of the Measures for the Administration of Combating Money Laundering and Financing of Terrorism by Banking Financial Institutions (Order No. 1 [2019] of China Banking and Insurance Regulatory Commission).

81 Hong Kong maintains its Strategic Commodities Control List based on the Australia Group, Chemical Weapons Convention, Missile Technology Control Regime, Nuclear Suppliers Group and Wassenaar Arrangement. The Strategic Commodities Control List comprises two sub-lists: the Munitions List and the Dual-use Goods List. The Munitions List covers 22 munition-related items; the Dual-use Goods List covers a wide variety of industrial dual-use goods under 10 categories: Nuclear Materials, Facilities & Equipment; Special Materials and Related Equipment; Materials Processing; Electronics; Computers; Telecommunications and Information Security; Sensors and Lasers; Navigation and

HKSAR also implements UN sanctions in accordance with the United Nations Sanctions Ordinance (UNSO) (Cap 537), which, by its terms, excludes sanctions targeting China.

Competent authorities

The strategic trade control system in HKSAR is made up of a licensing system and an enforcement system. The Trade and Industry Department is responsible for issuing licences covering the import, export, re-export and transshipment of strategic commodities as well as the transit of 'sensitive' items. Other government departments with an interest may be consulted as and when necessary. The Customs and Excise Department (C&ED) is responsible for the enforcement of strategic trade controls in HKSAR.

With respect to sanctions, the Commerce and Economic Development Bureau (CEDB) is responsible for maintaining lists of designated individuals and entities under the UNSO. The Hong Kong Monetary Authority (HKMA) is the competent authority for supervisory and enforcement measures over authorised institutions (AIs), such as banks, for the implementation of UN sanctions as well as to combat money laundering and terrorism financing under the Hong Kong Anti-Money Laundering Ordinance and related statutes. The HKMA issues statutory and regulatory guidance to provide specific requirements for compliance with UN sanctions by AIs. It is also empowered to take administrative and prudential measures, ranging from warnings to the imposition of restrictions on the business of AIs, and financial penalties.[82] The Securities and Futures Commission is responsible for anti-money laundering and counterterrorism financing in the securities and futures sector. It has the power to issue public reprimands or impose fines on regulated entities that violate relevant rules and requirements.[83] Finally, the Hong Kong Police Force (HKPF) and the C&ED are the law enforcement agencies for the purposes of the UNSO. Generally speaking,

---

Avionics; Marine; and Aerospace and Propulsion. For further information, See Hong Kong Strategic Commodities Control System, at www.stc.tid.gov.hk/english/hksarsys/Scope_Control_List.html.

82 Hong Kong Monetary Authority, 'Supervisory Policy Manual', at www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SPM-AML-1.pdf.

83 Securities and Futures Commission, 'Anti-money laundering and counter-financing of terrorism', at www.sfc.hk/en/Rules-and-standards/Anti-money-laundering-and-counter-financing-of-terrorism.

the HKPF is responsible for investigating financial matters, while the C&ED is mainly responsible for enforcement concerning the supply, sale or transfer of arms and other controlled items.[84]

China's control over HKSAR policy

As part of China, HKSAR implements UNSC sanctions as well as unilateral sanctions under the instructions of the Chinese government.

With respect to UNSC sanctions, the MFA may give an instruction to the chief executive (CE) of HKSAR to implement the sanctions specified in the instruction, or when sanctions have been implemented, to cease or modify the implementation of those sanctions or replace the sanctions specified in the instruction. Upon receipt of these instructions, the CE shall make regulations to give effect to the relevant instructions, including by prescribing penalties thereunder.[85]

The CE and relevant agencies have issued regulations under the UNSO to implement UN sanctions or restrictions against each of the UN targets, respectively. CEDB maintains lists of designated individuals and entities under the UNSO.[86]

The AFSL has not yet been included in Annex III of the HKSAR Basic Law.[87] Nevertheless, certain countermeasures taken by the Chinese government under the AFSL have already had implications for HKSAR. For example, on 30 December 2021, the MFA announced countermeasures against five US individuals, prohibiting them from entering China, 'including Hong Kong and Macao of China'.[88]

---

84 Press Release, Hong Kong government (23 January 2019), at www.info.gov.hk/gia/general/201901/23/P2019012300436.htm.

85 Articles 2 and 3 of the United Nations Sanctions Ordinance (UNSO) (Cap 537).

86 United Nations Security Council Sanctions page on the Commerce and Economic Development Bureau's website, at www.cedb.gov.hk/en/policies/united-nations-security-council-sanctions.html.

87 The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China (adopted at the Third Session of the Seventh National People's Congress on 4 April 1990 and entered into force on 1 July 1997). See the English version of the Basic Law at www.basiclaw.gov.hk/en/basiclaw/index.html.

88 Foreign Ministry Spokesperson's Announcement, at www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202112/t20211230_10477568.html.

Although certain countries may impose unilateral sanctions that apply to their nationals in HKSAR, the government has clarified that 'HKSAR does not have the responsibility nor the authority to enforce these unilateral sanctions or investigate related cases'.[89]

Non-China influences over HKSAR sanctions and export controls

After the promulgation and implementation of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (the HK National Security Law) on 30 June 2020, the United States and certain other foreign governments changed their policies towards Hong Kong in relation to export controls and sanctions.

In respect of export control, HKSAR was once treated as a separate territory under US law. In certain situations, items that require a licence for export to the Chinese mainland did not require a licence for export to HKSAR. After the HK National Security Law came into force, the US government, through the Executive Order on Hong Kong Normalization (EO 13936) of 14 July 2020 and related measures, revoked this treatment of Hong Kong. Hong Kong is now subject to the same licence requirements, licensing exceptions and provisions as the Chinese mainland under the US export control regime.

As for sanctions, according to its 2023 Hong Kong Policy Act Report, the United States communicated regularly 'with Hong Kong authorities through demarches and notifications on issues involving sanctions implementation, including on actions taken by the Department of the Treasury against several Hong Kong-registered entities under sanctions authorities related to China and counterterrorism'.[90]

US sanctions over HKSAR

Since the promulgation of the HK National Security Law, the US government has imposed a series of sanctions on the Chinese mainland and Hong Kong.

On 14 July 2020, President Trump issued EO 13936 and signed the Hong Kong Autonomy Act of 2020 (HKAA) into law. EO 13936 authorises the Treasury and State departments to impose blocking sanctions on property of foreign persons in relation to certain events in HKSAR, while the HKAA authorises (and in certain

89 Press Release, Hong Kong government (23 January 2019), at www.info.gov.hk/gia/general/201901/23/P2019012300436.htm.

90 2023 Hong Kong Policy Act Report issued by the US Department of State, Bureau of East Asian and Pacific Affairs (31 March 2023), at https://hk.usconsulate.gov/n-2023033102/.

circumstances, requires) the Executive Branch to impose sanctions on any foreign person identified in a report submitted by the State Department to Congress and to impose at least five of 10 enumerated sanctions on any foreign financial institution included in a report submitted by the Treasury Department to Congress. On 15 January 2021, the US Treasury issued Hong Kong-related sanctions regulations to implement EO 13936.[91]

To date, 42 HKSAR and Chinese mainland officials have been designated to the OFAC SDN List, and 39 of these have been identified by the State Department under the HKAA. No foreign financial institution has yet been identified under the HKAA.

91 US Treasury (15 January 2021), at https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210115_33.

CHAPTER 13

Practical Applications of International Sanctions and Export Controls in France

Stéphane de Navacelle, Julie Zorrilla and Juliette Musso[1]

Sources, definition and scope of restrictive measures on trade in France

Sources of trade sanctions in France

In France, international economic sanctions, defined as institutionalised mechanisms aimed at modifying reprehensible behaviour in the international sphere by means of partial or complete restrictions in trade and financial matters,[2] are mainly an application of international instruments adopted by the United Nations (UN) and the European Union.[3] It is important to note that European Union regulations are directly applicable in France. However, France has also adopted similar national retaliatory mechanisms in its own legislation.[4]

---

1 Stéphane de Navacelle is managing partner, Julie Zorrilla is a partner and Juliette Musso is an associate at Navacelle.

2 Emmanuel Lebrun-Damiens and Patrick Allard, 'Les sanctions internationales sont-elles efficaces?', in *Les Carnets du CAP: notes de réflexion et de prospective du Centre d'analyse et de prévision du Ministère des affaires étrangères*, April 2012, p. 107, refers to the different types of sanctions according to their nature, scope and effects.

3 David Hotte, Didier Morlet, Stéphane Sauteret and Vincent Soulignac, *Les sanctions financières internationales* (RB Editions, 2012), p. 91.

4 Régis Chemain and Juin Dalloz, *Répertoire de droit international –Sanctions économiques* (Dalloz, 2021), Section 13; EU Best Practices for the effective implementation of restrictive measures, Foreign Relations Counsellors Working Party, Council of Europe, 2018 recommends adopting autonomous mechanisms of economic sanctions to complement the prevention of terrorism funding.

These international sanctions can be of a commercial nature, aimed at restricting trading, import and export activities with a given country or entity,[5] or of a financial nature, corresponding to those restrictions linked to the access and continuation of financial, banking or stock market activities.[6]

Sanctions can also target a specific individual, territory or country or can be limited to a specific economic sector. When a sanction targets an individual, it generally involves the blocking of the target's accounts or financial products, which are included in sanctions lists. Sectoral sanctions are restrictions of trade or the rendering of certain services. For instance, recent EU sanctions against entities from the Russian Federation were imposed to restrict trade related to energy production, the aviation sector, the mining and quarrying sector, and the defence and security sector.[7] Similarly, the European sectoral sanctions concern access to the provision of credit and investment services on the European market for certain Russian banks.[8]

Economic sanctions applicable in France can take three forms:

- economic sanctions adopted by resolutions of the UN Security Council, which can be adopted by both the European Union and by the French state through transposition;
- economic sanctions dictated by Common Foreign and Security Policy (CFSP) decisions of the European Union and the corresponding regulations, which are immediately applicable in the French state; and
- measures adopted by means of national legislation or administrative acts on monetary and financial matters, customs or even national defence.

This chapter focuses on national provisions and France's approach to international sanctions.

5 Hotte, Morlet, Sauteret and Soulignac (footnote 3), p. 27.

6 ibid.

7 See Council Regulation (EU) No. 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

8 See Council Decision (CFSP) 2022/264 of 23 February 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine; Council Regulation (EU) 2022/263 of 23 February 2022 concerning restrictive measures in response to the recognition of the non-government controlled areas of the Donetsk and Luhansk oblasts of Ukraine and the ordering of Russian armed forces into those areas.

French authorities' roles in sanctions implementation

Different French authorities are involved in the implementation of international sanctions, depending on the context of the export, the nature of the goods or the applicable legislation.

For instance, the Directorate General of the Treasury Department within the Ministry of the Economy is responsible for approving certain transactions through its 'Sanctions financières internationales' platform.[9]

The French Export Control Office on Dual-Use Goods (SBDU), also linked to the Ministry of the Economy, is responsible for authorising the export of dual-use goods and other categories of goods for which exportation and importation is limited by European Union regulations.[10] The National Cybersecurity Agency (ANSSI), established in 2009 and related to the Ministry of Defence, is responsible for authorising the importation and exportation of dual-use items that contain encryption.

French customs authorities also generally control the importation and exportation of all goods to ensure compliance with import and export laws.

Sanctions applied in France on a domestic basis

Under French law, the French government may put in place different asset freezing mechanisms at the national level.

Article L151-2 of the Monetary and Financial Code allows the French government to restrict French investments and financial relations in foreign countries to protect national interests.[11] Historically, this was the main legal process used to apply sanctions before they were enacted through the EU CFSP and other international instruments.[12]

Article L562-2 of the Monetary and Financial Code also provides that, through the minister in charge of the economy, the French government can order the freezing of assets of persons related to terrorist cases. This measure can also be extended to legal persons or entities detained, controlled or managed by the targeted person.[13]

---

9 www.tresor.economie.gouv.fr/services-aux-entreprises/sanctions-economiques/teleservice-sanctions.

10 www.entreprises.gouv.fr/fr/echanges-commerciaux-et-reglementation/service-des-biens-double-usage/service-des-biens-double-usage.

11 Article L151-2 of the French Monetary and Financial Code.

12 Treasury Department Guidelines/frequently asked questions (FAQs) on the implementation of economic and financial sanctions, Department of Treasury, 2016, p. 8.

13 Article L562-2 of the French Monetary and Financial Code.

Article L562-3 of the Monetary and Financial Code provides that the French government may, for a renewable term of six months, decree the freezing of assets of entities or persons sanctioned by the UN and the European Union. In addition, this measure can be extended to legal persons or entities detained, controlled or managed by a sanctioned person.[14] This system reinforces the effectiveness of internationally adopted measures in the event of any delays that may occur in implementation.[15]

It is possible to file an appeal or litigation against a decision to freeze the assets of a person.[16] French law also provides the possibility for a partial release of sums of money intended to cover, within the limits of the available funds, basic living expenses and required legal costs, justified in advance.[17]

Consequences for non-sanctioned actors under French law

Sanctions also involve challenges for non-sanctioned economic actors, which must ensure that they do not violate the sanctions rules as an asset freeze prohibits making available economic resources to listed entities or persons.[18]

For ease of access, the implementation of these sanctions mechanisms is based on the use of lists of entities subject to an asset freeze, made available to the public by the Directorate General of the Treasury. Via the publicly available National Registry of Frozen Assets, it is possible to determine whether a person is subject to both domestic and international sanctions, without prejudice to the lists adopted at a European level.[19]

Furthermore, financial institutions are required to have a detection system that allows the filtering of persons and entities included in the asset freeze list.[20] Financial institutions must refuse to provide any services or authorise any transactions as soon as the sanction comes into force.[21]

---

14 id., Article L562-3.

15 Hotte, Morlet, Sauteret and Soulignac (footnote 3), p. 95.

16 Treasury Department Guidelines/FAQs (footnote 12), questions 10 and 11.

17 Article L562-11 of the French Monetary and Financial Code.

18 Joint guidelines of the French Treasury and the Authority of Prudential Control of Resolution (ACPR) on the implementation of asset freezing measures, 2016, p. 6.

19 https://gels-avoirs.dgtresor.gouv.fr/.

20 Joint guidelines of the ACPR (footnote 18), p. 20; Article 11 of Order dated 16 January 2021 on the system and internal controls relating to the fight against money laundering and terrorist financing and to the freezing of assets and the prohibition on making available or using funds or economic resources.

21 Joint guidelines of the ACPR (footnote 18), p. 32.

Violations of the asset freeze regime by financial institutions may result in disciplinary sanctions imposed by the French regulator of the financial, banking and financial sector, the Authority of Prudential Control of Resolution (ACPR), as well as criminal liability.[22] Other common challenges when an asset freeze is ordered may include cases of non-sanctioned persons who are affected even if they are not the subject of the asset freeze[23] as well as cases of homonymy.[24] Complying with export regulations is an additional challenge.

Export of dual-use items and licence export applications in France

France enforces Regulation (EU) 2021/821, which provides for an EU regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. Dual-use items are those that, while produced and marketed for civilian purposes, may also benefit military activities in contravention of international material control or restriction provisions.[25]

As such, an exporter must obtain a licence prior to exporting a dual-use item. A licence granted after the export is made does not render it lawful a posteriori.[26] Likewise, the state exercises control over dual-use goods via a series of obligations related to the end user and the ultimate destination of the items.[27]

Although dual-use goods and licences are mainly determined by the aforementioned European regulation, the French government, through the SBDU, can grant, suspend, modify, withdraw or revoke licences under national regulations.[28]

---

22 id., p. 46; ACPR is defined as competent to monitor and enforce regulations on national and international asset freezes by institutions under its supervision; see Articles L612-1 and L561-36-1 of the French Monetary and Financial Code on the ACPR's power to impose disciplinary sanctions; Article L574-3 of the French Monetary and Financial Code on criminal penalties for violation of an asset freeze measure; and Article 459 of the Customs Code on criminal sanctions regarding the violations of legislation and regulations relating to financial sanctions.

23 Treasury Department Guidelines/FAQs (footnote 12), Question 12.

24 id., Question 36.

25 Article 2.1 of Council Regulation (EU) 2021/821 of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.

26 id., Article 3.

27 id., Article 27 et seq.

28 Article 1 of Decree No. 2001-1192 of 13 December 2001 on the control of export, import and transfer of dual use goods and technologies; Article 1 of Decree No. 2020-74 of 31 January 2020 on the national service called 'Export Control Office on Dual-Use Goods', a department with nationwide competence.

The SBDU also elaborates on governmental positions regarding dual-use item exports and participates in the corresponding European-level negotiations.[29]

More importantly, through the use of off-licence requests, exporters may request guidance from the SBDU regarding whether the item intended for export is a dual-use item and to which category it belongs pursuant to the Annexes of EU Regulation 2021/821.[30]

Licences delivered in France by the SBDU may take the following different forms, depending on their scope and specific application:

- individual licences: these are granted for one or several identified dual-use goods of the same nature, intended for a particular person within a given limit and value.[31] Exporters should attach an end-user certificate to facilitate the licence application process;[32]
- global licences: these allow exporters to export dual-use items and may refer to one or several end users as well as to one or several countries.[33] To obtain a global licence, an exporter that carries out activity through a regular flow of supply abroad of dual-use goods as defined by the applicable regulations[34] is required to have a monitoring programme in place to control the end users to whom it is exporting on a regular basis. The exporter must be able to indicate the internal procedures adopted for the purpose of internally verifying the nature of the goods, the list of internal persons in charge of monitoring compliance, and the development of an audit programme. The exporter is also required to implement a due diligence procedure to identify clients that may not comply with export controls, to implement a training programme for employees and to set up a registration and archiving system;[35]
- national general licences: these cover agreed licences for export without limit in quantity or value for certain categories of dual-use items to certain specified destinations;[36] and

29 Article 3 of Decree No. 2020-74.

30 www.entreprises.gouv.fr/fr/echanges-commerciaux-et-reglementation/service-des-biens-double-usage/deposer-dossier-hors-licence.

31 Article 3 of Decree No. 2001-1192.

32 www.entreprises.gouv.fr/fr/echanges-commerciaux-et-reglementation/service-des-biens-double-usage/documents-fournir-et-modalites-par-type-d-autorisation.

33 Article 3 of Decree No. 2001-1192.

34 Article 8 of the Order of 13 December 2001 on the control of exports to third countries and transfers to Member States of the European Community of dual-use items and technologies.

35 id., Article 10.

36 Article 3 of Decree No. 2001-1192.

- European general authorisations: EU Regulation 2021/821 provides general authorisations for exporters that fulfil specific monitoring and traceability conditions of their exports.[37]

The SBDU can also issue international import certificates and delivery verification certificates to allow the importer to justify the final destination of the dual-use goods concerned to a foreign supplier or foreign national authorities, which may need to approve the export of the item.[38]

Applications are generally made digitally through the SBDU website.[39] From a practical standpoint, the SBDU encourages companies to adopt review methods and internal controls to ensure the accuracy of the information provided and mitigate the risks associated with exports of dual-use items. For example, to obtain a licence and to avoid customs delays, the service draws attention to the need to have the latest version of the relevant forms, particularly the end-user certificate.[40]

Attention is also drawn to the declared value of the goods, nomenclature codes and other specifications requested in the application form.[41] Finally, the SBDU advises exporters to include a contextual letter to enable it to fully understand the scope of the export operation contemplated.[42]

Although the SBDU grants licences for the export of dual-use items, some products may require further authorisations for the export to be legal; for example, dual-use software that integrates cryptography or cryptological functions[43] and that is classified as a dual-use item requires an authorisation from the French National Agency of Security and Information Systems, which is attached to the Ministry of the Interior.[44]

37 ibid.

38 id., Article 8.

39 Articles 2, 11 and 12 of the Order of 13 December 2001.

40 'Documents obligatoires', www.entreprises.gouv.fr/files/files/entreprises/biens-a-double-usage/demarches/modalites-demande-licence-individuelle.pdf, p. 15.

41 ibid.

42 ibid.

43 Article 29 of Law No. 2004-575 of 21 June 2004 on confidence in the digital economy, which defines the means of cryptology as any device designed or modified to transform data using secret characters to guarantee security.

44 Article 3 of Decree No. 2007-663 of 2 May 2007 taken for the application of Articles 30, 31 and 36 of Law No. 2004-575.

Non-compliance with these formalities may lead to the failure of the export and may also lead to penalties, as discussed below. It is therefore essential for exporters to be equipped with effective verification and compliance systems. This will allow them to gain a full understanding of regulations and to adapt their activities accordingly.

Main export licence of military equipment in France

France has adopted a political doctrine in which the export of military equipment is seen as a key component of its sovereignty and security. The general principle is thus that the export of military equipment and weapons is prohibited by law.[45] However, there are some exceptions, and exports of military equipment must be expressly authorised through the granting of a licence. While dual-use items are regulated at the EU level through Regulation 2021/821, the export of military items is regulated at the national level mainly by the French Ministry of Defence as the French rules applicable to the export of military items are found in the Defence Code. In that regard, the logic is similar to the licence application process for dual-use items.

Military equipment licences are granted by the Defence Ministry through the General Directorate of the Army (DGA) and the General Secretariat of Defence and National Security.[46] They are granted for either exports to non-Member States of the European Union[47] or for 'transfers' within the European Union.[48]

There are three main types of military equipment licence:

- individual licences: these refer to a given operation, limited in price and quantity, with an identified recipient,[49] and are valid for three years;[50]
- global licences: these are granted to an applicant for one or several operations with no price or quantity limit. They are valid for a specific period and can be automatically renewed;[51] and

45 French Defence Code, Article L2335-2 for exports to non-Member States of the European Union.

46 id., Article R2335-9.

47 id., Article L2335-2 for exports to non-Member States of the European Union.

48 id., Article L2335-9.

49 id., Article L2335-3 for exports to non-Member States of the European Union; Article L2335-10 for transfers to EU Member States.

50 id., Article R2335-34.

51 id., Article L2335-3 for exports to non-Member States of the European Union; Article L2335-10 for transfers to European Union Member States.

- general licences: these are defined by an administrative decision published in the Official Gazette and allow exports without price or quantity limits to one or several categories of recipients.[52]

In the case of individual or global licences, the application may be made electronically through the online export licence information, management and administration system.[53] Exporters may be required to produce certificates of non-re-exportation of the goods, issued by the holders of the goods, which guarantee that it is not a triangular operation or a form of circumvention of the regulations.[54]

There is also an obligation to submit a semi-annual accountability report on licensed operations. This report must include the orders and shipments made and the certificates of non-re-exportation, among other technical specifications of the operations.[55]

In the post-licensing stage, the exporter must keep a record of all the necessary justifications to establish that there was no misuse of the material exported during the operation.[56] In the case of inconsistencies found during a verification by the DGA, a report and the established verbal proceedings may be sent to a ministerial committee for follow up.[57] In addition, if a criminal offence is suspected, the DGA may inform the French prosecutors, after informing the French Ministry of Defence.

Trade sanctions violations and enforcement defence in France

The international economic sanctions regime at the EU or UN level does not have a direct sanction mechanism in the event of a violation. It is the responsibility of each state, in its enforcement mission, to define the penalties applicable for violation of the various international regimes and to sanction the corresponding infractions.

52 ibid.

53 id., Article R2335-10.

54 Article 2 of the Order of 30 November 2011 establishing the organisation of documentary and on-site inspections carried out by the Ministry of Defence pursuant to Article L2339-1 of the Defence Code.

55 ibid.

56 ibid.

57 id., Article 11.

However, it was decided in November 2022 that violation of restrictive measures adopted by the EU was to be added to the list of 'EU crimes', meaning that the EU will adopt a 'directive containing minimum rules concerning the definition of criminal offences and penalties for the violation of restrictive measures', which must be transposed in every Member State.[58] This process is ongoing at the time of writing.

French provisions on violations of restrictive measures on trade

The violation of an economic sanctions regime can also be a key element in determining criminal liability in cases where the commission of more complex offences is alleged.

Article 459 of the Customs Code states that it is a criminal offence for a person to breach international economic restrictive measures adopted by the European Union or through an international treaty. The infringement, circumvention or fraud of these sanctions carries a maximum sentence of five years' imprisonment and a fine of double the proceeds of the offence. Exporting dual-use items or military equipment without a licence carries a similar sentence.[59]

Article L574-3 of the Monetary and Financial Code provides for the same penalties for violation of sanctions adopted by the French government at national level.[60]

As far as asset freezes are concerned, the ACPR exercises its control through the imposition of civil sanctions in the financial, banking and insurance sectors.[61] For instance, a €50 million penalty was imposed on French bank La Banque Postale in 2018 because of the absence of an adequate detection system to identify whether beneficiaries of bank transactions are subject to an asset freeze.[62] The French Supreme Court for administrative matters later confirmed the sanction.[63]

58 Press Release, European Council, 28 November 2022: 'Sanctions: Council adds the violation of restrictive measures to the list of EU crimes', www.consilium.europa.eu/en/press/press-releases/2022/11/28/sanctions-council-adds-the-violation-of-restrictive-measures-to-the-list-of-eu-crimes/.

59 Article 414 of the French Customs Code.

60 Article L574-3 of the French Monetary and Financial Code.

61 Joint guidelines of the French Treasury and the ACPR on the implementation of asset freezing measures, 2016, p. 46.

62 Decision of the ACPR Enforcement Committee of 21 December 2018, No. 2018-01.

63 French Council of State, 15 November 2019, No. 428.292.

Similarly, on 30 November 2021, the ACPR imposed a €4 million penalty on MMA IARD, a French insurance company, holding that it had shortcomings in the implementation of asset freeze obligations.[64]

In addition, Article L2339-2 of the French Defence Code provides for a maximum sentence of seven years of imprisonment and a fine of €100,000 for any person who produces and markets war materials, arms and ammunition without complying with the corresponding licensing and authorisation obligations.[65] Pursuant to Article L2339-14 of the Code, the penalty is set at 15 years of imprisonment and a fine of €1.5 million if the materials are biological weapons or weapons of mass destruction.

International sanctions-related criminal seizure of property in France

In October 2022, French authorities seized a villa at Saint-Jean-Cap-Ferrat in the South of France, representing the first criminal seizure of real property of a sanctioned Russian individual. Viktor Rachnikov, majority holder of one of the biggest steel producers in Russia, was suspected to be its owner. He was sanctioned in March 2022 under Regulation (EU) No. 269/2014. When the National Financial Intelligence Unit learned that he was the owner of the villa via a complex arrangement to hide his ownership, it blocked the payment for the sale of the villa before going to court, and the villa was seized.[66] The seizure was made because it was linked to potential money laundering offences. The judicial proceedings are ongoing at the time of writing.

Criminal seizure of property is available under French criminal law until a decision of a court regarding the forfeiture of the property.[67] Forfeiture is available if the property was used to commit a crime or if the property was intended for the perpetration of an offence,[68] as well as under Article 459 of the Customs Code for violation of sanctions regimes.

Sanctions or restrictive measures violations linked to other crimes

In addition to the offences described above, recent events illustrate that violation of the sanctions regime may also be used as evidence of other violations.

64 Decision of the ACPR Enforcement Committee of 30 November 2021, No. 2020-09.

65 Article L2339-2 of the French Defence Code.

66 'Une villa saisie et dix-neuf enquêtes ouvertes: les sanctions contre les oligarques russes commencent à porter leurs fruits en France', *Le Monde*, 1 March 2023.

67 Article 706-121 et seq. of the French Code of Criminal Procedure.

68 Article 131-21 of the French Penal Code.

For instance, the French-Swiss company Lafarge is currently being prosecuted in France for various offences, including for funding terrorism in Syria.[69] The company is alleged to have decided to continue its activities in territories controlled by the Islamic State.[70] Not only did inherent economic sanctions risks in Syria materialise, but French authorities are currently seeking[71] criminal liability for the company.[72] In May 2022, the Paris Court of Appeal confirmed the indictment of Lafarge for complicity for crimes against humanity.[73]

Another relevant case in France concerns the link between the violation of international economic sanctions and the characterisation of the crime of corruption. This case relates to the criminal liability of Total, in the framework of the UN oil-for-food programme, which entailed a considerable diversion of funds.[74] Total, as a company participating in the programme, was sanctioned for its participation in fraudulent schemes that not only allowed a violation of the embargoes but constituted acts of corruption.[75]

Exporters are also at risk of liability in cases of misuse of equipment. This is especially relevant in terms of dual-use items and military equipment. These exports carry a significant legal risk for companies that operate on a global scale. In that regard, under French law, not only can companies be criminally liable, but the French Supreme Court recently confirmed that in the case of a merger or acquisition, an absorbing company can, under certain conditions, be convicted for offences committed by the absorbed company prior to the merger.[76]

---

69 European Council Press Release, 27 May 2021: 'Syria: Council extends sanctions against the regime for another year'.

70 'How the cement company Lafarge worked with the Islamic State in Syria', *Le Monde*, 21 June 2016.

71 'Lafarge in Syria: the Court of Cassation invalidates the cancellation of proceedings for complicity in crimes against humanity', *Le Monde*, 7 September 2021.

72 'Syria: Lafarge indicted for complicity in crimes against humanity', *Le Monde*, 28 June 2021.

73 'Lafarge case in Syria: indictment for "complicity in crimes against humanity" confirmed', *Le Monde*, 18 May 2022.

74 'Q&A: Oil-for-food scandal', BBC One-Minute World News, 7 September 2005.

75 'Total fined by French court in Iraq oil-for-food case', Reuters, 26 February 2016.

76 Supreme Court, Criminal Division, 25 November 2020, No. 18-86.955.

Examples of challenges for entities operating in France facing allegations of international sanction violations

Aside from regulatory and legal risks, sanctions violations expose corporations to reputational issues, market consequences[77] and scrutiny from non-governmental organisations (NGOs) and civil society.[78]

This may be illustrated by public criticism of the decision of certain French companies to continue activities in sanctioned countries.

Such is the case, for example, of the French energy group TotalEnergies, which decided to continue operations in Myanmar despite the impositions of economic sanctions following the military coup that took place on 1 February 2021.[79] The same issue applied to Total in the context of the Russian sanctions.[80] Regarding the Myanmar operations, while the media and NGOs questioned the presence of TotalEnergies in the country because the company would be financing the state structures responsible for the repression,[81] TotalEnergies claimed that it did not contribute either directly or indirectly to the violation of human rights in Myanmar and that its motives for maintaining its operations were humanitarian in nature.[82] Despite the decision to continue operations, pressure by NGOs and the threat of judiciary actions against the company led to its decision to withdraw in 2022.[83]

The reasoning behind this case is particularly useful, as it reveals the complexities of the regulations and the risk of sanctions, as well as the seriousness of the violation, resulting in the intensification of the risks, even at a preparatory stage. Effectively, it illustrates the balancing act involved in complying with international sanctions regimes and the challenges for companies in doing so.

77 Pauline Grosset-Grange, 'French NGOs and corporate funding from companies: the stakes of a convergence', Dumas Institute of Political Science, Paris, 2014, p. 30.

78 id., p. 14.

79 'The oil company Total remains in Burma despite the repression', FranceTv Info, 4 April 2021.

80 'TotalEnergies in Russia: We must stop turning a blind eye', *Le Monde*, 24 August 2022.

81 Joint Press Release, NGOs, 19 March 2021, 'Burma: Total Must Stop Funding the Junta'.

82 Patrick Pouyanné, 'Total facing Human Rights tragedy in Myanmar', Tribune CEO, 4 April 2021.

83 'TotalEnergies and Chevron withdraw from Myanmar, almost a year after the coup', *Le Monde*, 21 January 2022.

Exporters have also increasingly been held liable for the misuse of their products. For instance, reports show that French companies and their executives have recently been prosecuted as accomplices for providing mass surveillance technology to repressive regimes in Libya and Egypt.[84]

Regarding the export of military equipment, the latest French parliamentary report on export licences of weapons underlines that an increasing number of NGOs have started filing criminal complaints against private weapons manufacturer and exporters in France.[85]

Despite compliance with the requirements for this type of export, the responsibility of the producer and exporter after the export may involve complex elements in terms of penalties. In that regard, it should be noted that the granting of a licence by France does not shield exporters from liability arising from misuse of their products.

This is explained by the fact that, although French export regulations may require exporters to maintain control and surveillance of the final use of certain goods marketed by their customers, it is difficult to assess the scope of this obligation once the export transaction has been concluded.

Managing the risk of violations of international sanctions

Compliance with regulations or licences granted by the state is necessary to protect company interests but would most likely not be sufficient to mount an effective enforcement defence in the case of judicial and administrative prosecution for alleged violation of the provisions regarding EU or UN regulations that are applied by the French state.

An effective compliance system may enable the anticipation, and overcome the legal challenges posed by enforcement, of international restrictive measures on trade.

It is therefore necessary to establish risk management mechanisms and compliance policies in this area. Companies should have teams trained in these issues and, if necessary, seek external assistance in forecasting and reacting to the adoption of international restrictions regardless of their origins. Support in decision-making is essential to manage the risks of sanctions and prosecution in this area and to adopt a global view on these matters.

84 'Sale of surveillance equipment to Libya', *Le Monde*, 22 June 2021.

85 Report on export control of weapons No. 3581, 18 November 2020.

There is no 'standard' compliance system applicable to all types of companies or a central authority issuing general recommendations. It is therefore necessary to consider the specificities of the activity and the geographical location to define adequate procedures and rules.

It is also necessary to consider the regulations on international economic sanctions in commercial relations with third parties. In this sense, guarantee clauses in accordance with the regulations (mandatory, for example, in the matter of prohibition of re-export) should be generalised in entities that have specific exposure. Likewise, an analysis of beneficial owners should be made to verify whether the structure of suppliers, customers or contractors includes or may benefit persons subject to international sanctions.

Another important aspect, in addition to prevention, concerns the definition of procedures for detecting violations of international sanctions regimes, audits and controls. Although French authorities do not check for the existence of sanctions compliance systems, when it comes to enforcement action, active cooperation may result in less severe treatment.

Part II

Compliance Programmes

CHAPTER 14

Principled Guide to Sanctions Compliance Programmes

Zia Ullah and Victoria Turner[1]

The past decade has seen sanctions move up the risk agenda, becoming one of the most significant risks for businesses operating across multiple jurisdictions. This has been emphasised throughout 2022 and 2023 by the expansive and complex sanctions imposed against Russia, which saw businesses across all sectors evaluating sanctions risk and compliance. Once only a real concern for regulated financial institutions, the proliferation of enforcement action against unregulated business outside of the financial services sector has forced all businesses, irrespective of the sectors in which they operate, to consider the adequacy of their sanctions compliance programmes. In addition, companies face pressure from their own business partners to ensure and demonstrate sanctions compliance downstream, particularly within supply chains. As a result of this scrutiny, never has an effective sanctions programme been more important. This chapter considers the key areas of focus that businesses and their teams should consider when developing sanctions compliance programmes.

Proportionate and risk-based programmes

Sanctions compliance programmes should be risk-based and proportionate. What is applicable for one organisation will not be appropriate for another, and enforcement agencies have noted that an adequate compliance programme will very much depend upon factors unique to each organisation (including their products, customers, geographical exposures and nature of their business).

1 Zia Ullah is a partner and Victoria Turner is a principal associate at Eversheds Sutherland.

The concept of proportionality is very important. Although on one measure, sanctions compliance may be considered as a binary 'comply or breach' issue, the practical reality is that a one-size-fits-all approach is not necessary or indeed cost-effective. The large-scale sanctions mitigation strategies, which regulated businesses develop to ensure they are able to effectively screen millions of customers and transactions every day, will not (nor should they) be the same strategies that are employed by smaller businesses with only a fraction of the number of customers or potential sanctions touchpoints across their business life cycles. As we outline below, assessing the sanctions risks applicable to any particular business will ensure that the most proportionate sanctions compliance programme is implemented for that enterprise, taking into account the levels of resources that are available, or indeed appropriate.

Preventive measures

Prevention is key in terms of sanctions compliance. Regulators across the world take a dim view of those institutions that fail to identify risks and seek to implement preventative measures to mitigate those risks. In this regard, sanctions compliance is no different from other financial crime compliance. However, sanctions compliance has a number of unique and specific challenges, including the constantly evolving regimes (sometimes daily) and the difficult position conflicting global regimes can create for global institutions. Being aware of the challenges that sanctions compliance poses, staying on top of worldwide developments and anticipating future changes are all key issues when identifying the preventative measures that should be put in place and to ensure that they continue to operate in an effective manner.

The development of policies and procedures, customer screening systems, the provision of training, due diligence, transaction monitoring and transaction screening are all key preventative measures that organisations should consider putting in place. As there is no one-size-fits-all when it comes to sanctions compliance, a risk assessment should be at the heart of all sanctions compliance programmes.

Recent events have also shown that those with more sophisticated and effective sanctions compliance programmes are also able to:

- utilise learnings from the root causes of apparent violations within publicised enforcement actions to identify and strengthen preventative measures. Understanding where others have failed is a key component of determining whether your own sanctions compliance programme will be effective; and
- react to significant geopolitical and legal changes quickly, as was shown with the rapid deployment of sanctions against Russia in 2022.

What constitutes a good sanctions compliance programme?

Sanctions are, quite rightly, a high compliance priority for many businesses, and, in recent times, regulators and enforcement agencies have provided guidance on what to consider when assessing a sanctions compliance programme. Key guidance to note includes:

- FAQs published by the Office of Foreign Assets Control (OFAC) in respect of sanctions compliance;[2]
- 'A Framework for OFAC Compliance Commitments' (dated 2 May 2019);[3]
- the Department of Justice's (DOJ) 'Evaluation of Corporate Compliance Programs' (issued in 2019 and updated in June 2020 and March 2023);[4]
- the Office of Financial Sanctions Implementation's (OFSI) general guidance on financial sanctions;[5]
- OFSI's monetary penalty guidance;[6]
- the Financial Conduct Authority's (FCA) 'Financial Crime Guide';[7] and
- EU guidance on internal compliance programmes.[8]

Sanctions authorities around the world broadly agree that the general core components of an effective sanctions compliance programme are:

- senior management commitment;
- risk assessment;
- policies, procedures and internal controls;

---

2 See https://ofac.treasury.gov/faqs.

3 See https://ofac.treasury.gov/media/16331/download?inline.

4 See US Department of Justice's guidance on 'Evaluation of Corporate Compliance Programs' (issued in 2019 and updated in June 2020 and March 2023), at www.justice.gov/criminal-fraud/page/file/937501/download. Although this is not specific to sanctions, it is helpful in understanding the approach enforcement agencies may take when assessing whether or not a compliance framework was adequate.

5 See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1144893/General_Guidance_-_UK_Financial_Sanctions__Aug_2022_.pdf; in particular, Chapter 7 regarding compliance.

6 See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1143219/March_2023_Monetary_Penalty_and_Enforcement_Guidance.pdf.

7 See www.handbook.fca.org.uk/handbook/FCG/7/; in particular, Chapter 7, which provides examples of good practice for sanctions systems and controls.

8 Commission Recommendation (EU) 2019/1318; although this focuses on compliance programmes for dual-use trade controls, the overarching principles are arguably relevant to any sanctions compliance programme. See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318.

- training; and
- audit.

We examine each of these five components in more detail.

Senior management commitment

Senior management commitment is at the forefront of all guidance on sanctions compliance programmes. Compliance should not operate in a vacuum, and senior management should understand the compliance programme's purpose, the key risks faced by the organisation (both inherent and residual) and how the programme is designed to work. Senior management should demonstrate, at board level where appropriate, support for the compliance programme and those within the business who are responsible for its development and operation.

Both regulators and sanctions enforcement agencies expect senior management to review and approve an organisation's sanctions compliance programme. This must not be just a tick-box process, and regulators will look to senior management to provide support for the compliance programme within their organisation and demonstrate compliance themselves, as well as a general culture that fosters positive and effective sanctions compliance. Senior management should set the tone for the business, undertake sanctions compliance training and regularly review sanctions risks faced by the business, providing effective challenge to the risk and compliance function where appropriate.

Senior management should not stifle or prevent risk and compliance teams from implementing and operating an effective sanctions compliance programme. Regulators and enforcement agencies are keen to see adequate resources being provided to compliance teams and that compliance and risk teams have a sufficient level of autonomy to implement policies and procedures designed to mitigate the sanctions risk identified within an organisation. However, overall responsibility for sanctions compliance should lie with a chief compliance officer, general counsel or some other appropriate member of an organisation's executive committee.

It should be noted that where issues arise as a result of potential failings in sanctions compliance frameworks, senior management are often at the heart of any potential investigation into any failings, and as such they should ensure that they fully understand the potential sanctions risks their businesses face and be able to articulate the steps they took to ensure compliance. With the current scrutiny on sanctions compliance, it has never been more important for senior management to have sufficient understanding and oversight of sanctions compliance within their business.

Risk assessment

Internal controls, policies and procedures and training cannot be done in an appropriate manner unless a risk assessment has been conducted and the output is used to inform those elements of the compliance programme. It is only when an organisation has considered and laid out its inherent sanctions risk that it can truly start identifying controls and residual risk factors. A sanctions risk assessment will vary significantly across different business types and sectors; however, OFAC notes that a risk assessment 'should generally consist of a holistic review of the organization from top-to-bottom and assess its touchpoints to the outside world'.[9] Equally, from a legal point of view, different legal requirements (including cross-border requirements) pose different challenges and risks to different businesses. Understanding the complexity of sanctions and the effects on your own individual business is vital when implementing and managing an effective compliance programme.

In the United Kingdom, the FCA is clear that 'a thorough understanding of its financial crime risks [including sanctions] is key if a firm is to apply proportionate and effective systems and controls'.[10] Corporate resources are not infinite and one of the key benefits in conducting a risk assessment is that it enables an organisation to target resource on the areas of greatest sanctions risk (alongside other financial crime-related areas).

Risk assessments should have a broad scope and should include assessment of:

- customer risk;
- product risk;
- geography risk;
- transaction risk; and
- delivery risk.

It is important to identify all potential sanctions risk and, in particular, where it is in the operation of your business that potential sanctions exposure may lie. As noted in 'A Framework for OFAC Compliance Commitments', sanctions risk not only exists in the day-to-day operations of a business but also in mergers and acquisitions, particularly where these introduce cross-border considerations. As such, assessing the applicability of various sanctions regimes to different parts

9 Office of Foreign Assets Control (OFAC), 'A Framework for OFAC Compliance Commitments' (dated 2 May 2019), at https://ofac.treasury.gov/media/16331/download?inline.

10 Financial Conduct Authority, 'Financial Crime Guide', 2.2.4. See www.handbook.fca.org.uk/handbook/FCG/2/2.html.

of your business, customers, intermediaries, the supply chain, counterparties and the geography of each of these is important. Understanding the root causes of apparent sanctions violations (both those identified internally and those seen in enforcement cases) and how international sanctions may develop as a result of geopolitical events will also result in a more effective risk assessment.

OFAC has helpfully provided a suggested risk matrix that may be used when assessing compliance programmes.[11]

Policies, procedures and internal controls

Internal controls are the measures put in place by an organisation to mitigate the risks it has identified. Examples of internal controls that may be appropriate in the context of sanctions include:

- policies and procedures;
- customer and third-party screening;
- transaction screening;
- due diligence requirements;
- contractual provisions; and
- training.

Sanctions compliance programmes typically include, at their most basic, a sanctions policy and, in some cases, a compliance manual (which may cover more than one area of financial crime risk) that sets out the processes underpinning the internal controls in place, along with an appropriate internal reporting and governance structure and exceptions process.

Internal controls for any financial crime compliance programme must be able to adapt to ongoing changes and developments. This is particularly important in the context of sanctions where changes to legal regimes occur frequently (as has been seen throughout 2022 and 2023), where new entities and individuals are designated by one or more regulators and where geopolitics frequently result in changes in focus by different governments across the world. An effective sanctions compliance programme must be able to adapt to these evolutions and this should be built into the framework of the internal controls.

11 Annex to Appendix A to 31 Code of Federal Regulations Part 501, OFAC's Economic Sanctions Enforcement Guidelines. See www.ecfr.gov/current/title-31/subtitle-B/chapter-V/part-501/appendix-Appendix%20A%20to%20Part%20501.

Although there is generally no legal obligation within primary sanctions legislation to conduct sanctions screening,[12] it is often the only practical way an organisation can ensure that it does not engage in conduct that would give rise to violations of sanctions. There are multiple screening tools available to organisations, some of which will no doubt be better suited to certain industries. However, what is important is that those responsible for the screening solution within an organisation understand why the tool was selected, how it operates, how it is calibrated to meet the needs of the organisation and its risk assessment, and how the underlying logic works. The effectiveness of sanctions screening tools, at both the customer and transaction levels, should be regularly tested to ensure it is operating within the parameters the organisation needs and expects.

Having a screening tool working in isolation is unlikely to be effective, and the importance of ensuring it is aligned to a risk assessment and due diligence requirements cannot be understated. An organisation's risk assessment should inform how a screening solution is utilised and what is screened and when.

The importance of internal controls is not a new concept and has been a significant area of focus for regulated entities for many years. Both civil monetary penalties issued by sanctions authorities, and regulatory penalties issued by those regulating the financial sector, have heavily focused on internal controls to combat sanctions risk, and this scrutiny has been emphasised throughout 2022 and 2023 as a result of the sanctions imposed against Russia. Regulators, such as the FCA, have stressed that sanctions compliance and the testing of internal controls within organisations is a key priority area of focus and is not reliant on there being a sanctions violation. The aim of regulators across many jurisdictions is to take action proactively in assessing the adequacy of controls to ensure the risk of sanctions violations occurring is mitigated. This message is emphasised by actions taken by regulators across the world against organisations not only for actual violations of sanctions but also because of the lack of adequate internal controls in preventing violations from occurring.

Training

An organisation could design the best sanctions compliance programme ever seen, but failing to train employees adequately, not only on the programme itself but on the rationale for having it (including legal and regulatory obligations), is

12 In the UK, the EU or the US, although the authors acknowledge that certain regulated entities may have regulatory obligations imposed on them by specific regulators, such as the New York State Department of Financial Services in the US.

a sure-fire way of ensuring the compliance programme fails. While technology no doubt plays a significant role in any compliance programme, the complexity of international sanctions and the need for various controls to work alongside and in conjunction with each other means that, often, a sanctions compliance programme is only as good as the people who implement it.

Training can take many forms and what is appropriate for one organisation will not necessarily be appropriate for another. Organisations that operate across multiple jurisdictions will no doubt need a more detailed training plan than a small organisation based only in the UK, for instance. Again, the training requirements needed should flow from the outcome of an organisation's risk assessment and we would stress that it is important to consider the root causes of sanctions violations to ensure that these are, where appropriate, addressed within the training provided.

Training may include:

- clear communication of internal controls, policies and procedures to relevant employees;
- internal face-to-face or webinar-based training in respect of sanctions obligations (of the organisation and individual employees), legal and regulatory requirements, internal controls and reporting obligations (both internally and externally). Many enforcement authorities and regulators expect to see training being given regularly (at least once a year) to relevant employees; and
- external specialist training for those operating in vital roles within the risk and compliance functions and high-risk areas within a business.

Training content should be developed so that it is relevant to the particular organisation. Relevant sanctions regimes should be detailed, and, where appropriate, the conflict between regimes should be explained alongside the organisation's stance in respect of that conflict. Role-specific knowledge should be provided, and the obligations on individual employees and on the organisation and its senior management should be made clear. Within regulated firms, it is not unusual to see sanctions training programmes developed across the 'three lines of defence' model (with the first line being relevant business operations or units, the second line being risk and compliance functions, and the third line being internal audit), such that training is delivered to teams operating in each of the first, second and third lines to ensure that the specific risks and issues faced by those teams are considered specifically. This also enables these firms to demonstrate to regulators that they have considered the risks of breaching sanctions holistically.

Audit

Once a sanctions compliance programme is implemented, it is important to ensure that it is regularly tested and evaluated to not only ensure it remains effective, but also to ensure that the programme is being implemented consistently throughout the organisation. Both internal and external audits are useful in this regard, and audits can be carried out on specific aspects of a compliance programme or on the programme as a whole.

Audits, whether internal or external, should be independent and should aim to identify any deficiencies in the compliance programme, make recommendations for improvement and follow up on action items to ensure audit points are closed off and remediated where necessary. Linking back to the subject of senior management commitment, it is also recommended that audit functions are held accountable by senior management and that updates and reports on findings are presented to, and considered by, senior management.

Audit functions should provide a level of challenge to the risk and compliance function and the sanctions compliance framework. The DOJ has indicated that when assessing compliance programmes generally, in the context of criminal proceedings, the following three key questions should be asked:

- Is the corporation's compliance programme well designed?
- Is the programme being applied earnestly and in good faith?
- Does the corporation's compliance programme work in practice?[13]

These questions are equally relevant to the work of an independent audit function.

The events of 2022, with respect to the imposition of sanctions against Russia, also highlighted the importance of evaluating lessons learned in relation to how businesses cope with the increased number and complexity of sanctions. This is undoubtedly an area where auditing can provide additional value to a business, looking not only at the effectiveness of a compliance programme but also at its ability to efficiently adapt to rapid and complex changes.

Why is a sanctions compliance programme important?

Regulators and enforcement agencies across the world have made it clear, through their enforcement action, that failure to have an adequate sanctions compliance programme in place will only be to the detriment of the entity and be seen as an aggravating factor when sanctions violations are identified. In recent years, we

13 US Dep't of Justice's guidance on 'Evaluation of Corporate Compliance Programs'. See www.justice.gov/criminal-fraud/page/file/937501/download.

have seen substantial fines being imposed, particularly in the United States, as a result of sanctions compliance failures. Organisations operating only within the United Kingdom, however, should not seek comfort from the fact that most of the significant enforcement in recent years has historically taken place in the United States, as the UK enforcement agency, OFSI, has demonstrated that it is also willing and able to take substantive action. In 2022, OFSI and OFAC announced their enhanced partnership to, among other things, 'support OFSI's move to a larger and more proactive organisation'.[14]

Actions taken by enforcement agencies in the past few years have highlighted the importance of sanctions compliance programmes. If one is not in place or is not effective, enforcement agencies will not hesitate in requiring one to be put in place as a condition of a settlement. Being forced by a regulator or enforcement agency to strengthen a sanctions compliance programme comes with a number of difficulties, including reputational damage and, in serious cases, ongoing costs associated with future monitorship by enforcement agencies. It is far better for an organisation to take the initiative and develop and implement a sanctions compliance programme on its own terms to protect the business.

Some key UK and US enforcement cases in the past few years that highlight the importance of sanctions compliance programmes and the features of these programmes as detailed in this chapter include the following.

British American Tobacco Plc

British American Tobacco Plc (BAT) agreed to pay over US$500 million for violations of US sanctions against North Korea and weapons of mass destruction proliferators.[15] The enforcement action demonstrated the importance of senior management in sanctions compliance with the actions of senior management described as having been taken to 'purposefully obscure' BAT's ongoing ownership and control over a joint venture company in North Korea. OFAC determined that it was an aggravating factor that senior management had actual knowledge of a conspiracy to evade sanctions from its inception through to its ultimate termination. The size and sophisticated nature of the company was also determined to be an aggravating factor. OFAC stated that 'without a culture of compliance driven by senior management and attendant policies and controls, firms increase the risk that they may engage in apparently violative conduct'.[16]

14 See https://ofsi.blog.gov.uk/2022/10/17/ofac-ofsi-enhanced-partnership/.

15 See https://ofac.treasury.gov/media/931666/download?inline.

16 ibid.

Microsoft Corporation

When imposing a fine of just under US$3 million on Microsoft Corporation, OFAC stated that it had taken the extensive enhancements made by the company to its sanctions compliance programme into account as mitigating factors when determining the penalty to impose.[17] As part of its general comments, OFAC noted a number of key compliance messages, including: (1) the importance of companies having sufficient visibility into end users when conducting business through foreign-based subsidiaries and distributors, thereby highlighting the importance of due diligence controls; (2) that companies with global customer bases and sophisticated technology operations should ensure their sanctions compliance programme remains commensurate with the risk posed and that appropriate technological compliance solutions are leveraged where possible; and (3) the importance of ensuring and testing adherence to the sanctions compliance programme in place.

Uphold HQ Inc

While it involved a relatively small penalty (US$72,230.32), this enforcement action is worthy of note as it highlights the importance of financial institutions 'maintaining robust controls to screen information provided by customers to identify sanctions risk'.[18] OFAC noted the importance of ensuring that information provided at account opening and as part of ongoing due diligence should be considered for screening, particularly in relation to location information. This was also highlighted in other enforcement cases such as Bittrex, Inc where OFAC highlighted the importance of sanctions compliance controls when onboarding customers.[19] In this case, Bittrex failed to conduct screening that would have enabled internet protocol blocking controls to be put in place to prevent customers from accessing products and services when in prohibited jurisdictions.

Danfoss A/S

In this case, OFAC highlighted, among other things, the importance of maintaining effective, risk-based sanctions compliance programmes and the particular need to ensure adequate training is given to staff (including senior management),

17 See https://ofac.treasury.gov/media/931591/download?inline.

18 See https://ofac.treasury.gov/media/931556/download?inline.

19 See https://ofac.treasury.gov/media/928746/download?inline.

as well as the importance of considering guidance that may be issued periodically by OFAC on relevant issues.[20] Similarly, in *American Express National Bank*, OFAC highlighted the importance of employee training.[21]

Hong Kong International Wine and Spirits Competition Ltd

In this case, OFSI stated that companies need to consider sanctions risk broadly to include intangible economic resources and emphasised that those operating outside of the financial sector cannot seek to rely on the compliance programmes of those in the financial industry.[22] The enforcement action was an important reminder that sanctions apply to all businesses and that it is not the sole responsibility of the finance industry to ensure compliance.

Adequate procedures

When faced with potential enforcement action, one of the key questions organisations should be asking themselves is whether they had adequate procedures in place to prevent sanctions violations. 'Adequate procedures' are not defined in any guidance but generally speaking they are the measures an organisation has in place to mitigate the risk of sanctions violations. They are the components of a sanctions compliance programme that have been dealt with in this chapter.

It is entirely possible for an organisation to have adequate procedures in place and still experience sanctions violations; no system is perfect. However, being in a position to demonstrate to an enforcement agency such as OFAC or OFSI that your organisation had adequate procedures in place may be the difference between a breach being found to be egregious or not[23] and will undoubtedly influence enforcement agencies when they consider whether the violation has arisen from wilful or reckless conduct by the organisation and its employees. Being able to demonstrate that adequate procedures were in place, albeit a violation still occurred, could be significant in ensuring lower penalties.

In this regard, the approach to a sanctions compliance programme is similar to that which an organisation would take under the UK Bribery Act 2010 (UKBA). The UKBA provides a defence[24] to organisations if they are able to show that

---

20 See https://ofac.treasury.gov/media/930196/download?inline.

21 See https://ofac.treasury.gov/media/924406/download?inline.

22 See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1106745/Notice_of_Imposition_of_MP_-_HKIWSC.pdf.

23 Which is relevant when OFAC determines base penalties; see www.ecfr.gov/cgi-bin/text-idx?SID=ccac94aaa0387efe2a9c3fca2dc5a4ab&mc=true&node=ap31.3.501_1901.a&rgn=div9.

24 UK Bribery Act 2010, Section 7; see www.legislation.gov.uk/ukpga/2010/23/section/7.

they had adequate procedures in place designed to prevent an offence of bribery occurring. Where the approach differs is that although having adequate procedures provides a defence against prosecution under the UKBA, the same cannot necessarily be said for sanctions violations given the use of strict liability in some jurisdictions.[25] Notwithstanding this, having adequate procedures in place is a very significant form of mitigation in the context of sanctions violations.

Consolidated compliance programmes

Sanctions compliance does not operate in isolation. It is one component of a business's financial crime compliance framework, albeit a sometimes tricky one to design and manage. Sanctions due diligence closely aligns with that undertaken for the purposes of anti-money laundering (AML) and anti-bribery compliance and it is often the case that these are undertaken concurrently. Aligning relevant financial crime compliance programmes makes sense not only from a practical point of view, but it also has financial advantages and enables a business to mitigate its financial crime risk more effectively. Pulling together AML due diligence, screening for politically exposed persons, anti-bribery due diligence and adverse media checks means that an organisation is more likely to have a holistic view of the financial crime risks it faces and those its customers pose. The importance of due diligence across financial crime programmes and specifically to address sanctions risk has been at the heart of compliance messages over recent times, particularly as a result of the sanctions imposed against Russia, where due diligence has been key in identifying the extent of restrictions such as asset freezes.

Moreover, an organisation's ability to articulate the potential risks a particular customer or business partner poses across the whole financial crime risk matrix gives that organisation a commercial advantage – it truly understands where its customers and business partners are, where their main places of business are and, as a consequence, where they are likely to need products and services that the organisation can provide or products and services that must be declined because of the potential increase in risk. Either way, the organisation is able to properly assess the risks. When considering this risk assessment in the context of sanctions

25 For example, in the UK, strict liability was imposed for financial sanctions violations occurring on or after 15 June 2022, meaning that it is not a defence for a person to say that they had no knowledge or reasonable cause to suspect that the action in question was in violation of sanctions.

compliance, organisations that have a mature consolidated approach to compliance will be at a distinct advantage over those that approach risk management in a siloed manner.

In an increasingly complex geopolitical environment, the most successful businesses will not only be those that know when to offer their products and services to clients, but also those that know when to say no.

CHAPTER 15

Sanctions Screening: Challenges and Control Considerations

Charlie Steele, Gerben Schreurs, Weng Yee Ng and Jona Boscolo Cappon[1]

Background

Economic sanctions have evolved dramatically over the past few years, and especially after Russia's February 2022 invasion of Ukraine. The resulting sanctions are unprecedented in number, scope, complexity and type. While governments are increasingly turning to highly specific measures that prohibit particular types of transactions, list-based sanctions, which broadly prohibit business dealings with specific persons and entities rather than entire countries or geographic regions, remain the most frequently deployed type of sanctions. The best-known list-based sanctions are those maintained by the US Office of Foreign Assets Control (OFAC) and published on its Specially Designated Nationals and Blocked Persons (SDN) List.[2] These finely targeted sanctions generally result in fewer unintended collateral consequences than do country-based measures, but they

---

1 Charlie Steele, Gerben Schreurs and Weng Yee Ng are partners, and Jona Boscolo Cappon is a director, at Forensic Risk Alliance.

2 https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists. Because this chapter focuses on sanctions screening in particular – as opposed to, for example, export control rules and other requirements – it focuses on Office of Foreign Assets Control (OFAC) and other sanctions screening lists. However, readers should also be aware of the Consolidated Screening List maintained by the US Department of Commerce (www.trade.gov/data-visualization/csl-search). This List helpfully consolidates a number of US government lists of interest to those engaged in international business. It includes parties on which the US maintains restrictions on certain exports, re-exports or transfers of items, and it includes the Specially Designated Nationals and Blocked Persons List and other OFAC lists.

can often be more difficult to comply with. In 2022, further additions have been made to SDN lists, by jurisdictions such as the EU and UK, which has added to the complexity of maintaining current lists. Screening against targeted sanctions lists presents considerable challenges, given the complex corporate structures used to obscure underlying sanctioned parties, the inherent difficulties in name matching and the difficulties in screening for entities that are, directly or indirectly, 50 per cent or more owned in the aggregate by sanctioned parties, under OFAC's 50 Percent Rule.

An example of this increasing complexity are sanctions that address both entities and their underlying activities. Following Russia's invasion of Ukraine in 2022, additional sanctions to the 2014 sectoral sanctions were imposed, which limit specific investment activities, among other things, with Russian entities.[3] This new type of sanction added another level of complexity to compliance. Existing challenges in correctly identifying sanctioned parties were compounded by the requirement to also understand the nature of the proposed transaction by the customer.

Sanctions screening failures have figured prominently in a number of OFAC penalty settlements with both financial institutions and non-financial entities. To this end, we discuss current regulatory guidance for a successful sanctions screening programme, how screening relates to the core elements of the overall sanctions compliance programme, examples of enforcement actions focusing on screening failures, and screening in the context of a sanctions investigation.

Regulatory expectations for sanctions screening

In the US, OFAC has not published detailed guidance regarding expectations for sanctions screening programmes. The 2019 'Framework for OFAC Compliance Commitments' (the Framework),[4] after addressing five high-level elements for a sound sanctions compliance programme, identifies 10 common root causes of sanctions compliance failures. The sixth root cause addresses some of the failures that occur due to poor configuration of sanctions screening software.[5] The guid-

3 https://ofac.treasury.gov/system/files/126/new_debt_and_equity_directive_3.pdf.

4 https://ofac.treasury.gov/system/files/126/framework_ofac_cc.pdf.

5 'VI. Sanctions Screening Software or Filter Faults: Many organisations conduct screening of their customers, supply chain, intermediaries, counterparties, commercial and financial documents, and transactions in order to identify OFAC-prohibited locations, parties, or dealings. At times, organizations have failed to update their sanctions screening software to incorporate updates to the [Specially Designated Nationals and Blocked Persons] List or [Sectoral Sanctions Identifications] List, failed to include pertinent identifiers such as SWIFT

ance mentions some specific failings, including using outdated screening lists, incomplete data screening and not accounting for alternative spellings of names. These are a few of the potential points of failure when screening for possible sanctions targets, and we discuss several others in this chapter.

In 2015, OFAC published a one-page guidance document regarding the management of 'false hits' lists.[6] Pursuant to that guidance, where companies have determined that potential match alerts can be disregarded as false positives and suppressed going forward, compliance personnel should be involved in oversight and administration of the lists, and, among other things, the lists should be modified promptly and as necessary to account for changes to sanctions lists.

In contrast to the limited guidance from OFAC, the New York Department of Financial Services (NYDFS), which regulates financial institutions licensed within the state of New York, has taken a more prescriptive stance as to sanctions screening programmes. NYDFS has identified weaknesses in transaction monitoring and sanctions screening programmes within regulated institutions, and attributed them to insufficient governance and accountability at senior levels. As a result, NYDFS set out specific requirements for these programmes[7] that require boards of directors or senior officers to certify compliance on an annual basis.[8]

The first compliance findings were due in April 2018 and required regulated institutions to:

- *Undertake comprehensive and holistic assessments of their transaction monitoring and sanctions filtering programs;*
- *Provide appropriate supporting evidence to demonstrate the effectiveness of the programs;*
- *Execute remedial efforts, material improvements, or redesigns to keep the programs in compliance; and*
- *Implement governance processes for the annual certification.*[9]

Business Identifier Codes for designated, blocked, or sanctioned financial institutions, or did not account for alternative spellings of prohibited countries or parties – particularly in instances in which the organisation is domiciled or conducts business in geographies that frequently utilize such alternative spellings (i.e., Habana instead of Havana, Kuba instead of Cuba, Soudan instead of Sudan, etc.).'

6 https://ofac.treasury.gov/system/files/126/false_hit.pdf.

7 Part 504 of the New York State Banking Regulations in 2017.

8 www.dfs.ny.gov/industry_guidance/transaction_monitoring.

9 New York State Banking Regulations.

At a more detailed level, each regulated institution must maintain a sanctions screening programme that is reasonably designed to interdict transactions prohibited by OFAC and that includes the following attributes:

- *Be based on the risk assessment of the institution;*
- *Be based on technology, processes or tools for matching names and accounts, in each case based on the institution's particular risks, and transaction and product profiles;*
- *End-to-end, pre- and post-implementation testing of the Filtering Program, including, as relevant, a review of data matching, an evaluation of whether the OFAC sanctions list and threshold settings map to the risks of the institution, the logic of matching technology or tools, model validation, and data input and program output;*
- *Be subject to on-going analysis to assess the logic and performance of the technology or tools for matching names and accounts, as well as the OFAC sanctions list and the threshold settings to see if they continue to map to the risks of the institution; and*
- *Include documentation that articulates the intent and design of the Filtering Program tools, processes or technology.*[10]

In addition, the sanctions screening programme must include:

- *Identification of all data sources that contain relevant data;*
- *Validation of the integrity, accuracy and quality of data to ensure that accurate and complete data flows through the Transaction Monitoring and Filtering Program;*
- *Data extraction and loading processes to ensure a complete and accurate transfer of data from its source to automated monitoring and filtering systems, if automated systems are used;*
- *Governance and management oversight, including policies and procedures governing changes to the Transaction Monitoring and Filtering Program to ensure that changes are defined, managed, controlled, reported, and audited;*
- *Vendor selection process if a third party vendor is used to acquire, install, implement, or test the Transaction Monitoring and Filtering Program or any aspect of it;*
- *Funding to design, implement and maintain a Transaction Monitoring and Filtering Program that complies with the requirements of this Part;*

10 ibid.

- *Qualified personnel or outside consultant(s) responsible for the design, planning, implementation, operation, testing, validation, and on-going analysis of the Transaction Monitoring and Filtering Program, including automated systems if applicable, as well as case management, review and decision making with respect to generated alerts and potential filings; and*
- *Periodic training of all stakeholders with respect to the Transaction Monitoring and Filtering Program.*[11]

Although not all financial institutions are subject to these rules (and non-financial entities are not within their scope), they provide a useful benchmark in evaluating whether a sanctions screening programme has been designed well and is operating effectively.

In the UK, the Financial Conduct Authority's (FCA) Financial Crime Guide addresses compliance with sanctions and asset freezes.[12] In the context of a risk assessment, a firm should understand where sanctions risks reside, considering different business lines, sales channels, customer types and geographical locations, and should keep the risk assessment current. Examples of good practices related to sanctions screening include:

- *where a firm uses automated systems, these can make 'fuzzy matches' (be able to identify similar or variant spellings of names, name reversal, digit rotation, character manipulation, etc.);*
- *the firm should screen customers' directors and known beneficial owners on a risk-sensitive basis;*
- *where the firm maintains an account for a listed individual, the status of this account is clearly flagged to staff; and*
- *a firm should only place faith in other firms' screening (such as outsourcers or intermediaries) after taking steps to satisfy themselves that this is appropriate.*[13]

In addition to these examples of best practices, the Guide cites a £5.6 million fine by the FCA's predecessor against Royal Bank of Scotland (RBS) in 2010, where RBS failed to adequately screen its customers and payments against the sanctions list, did not ensure its 'fuzzy matching' remained effective, and, in many cases, did

11 ibid.

12 www.handbook.fca.org.uk/handbook/FCG.pdf.

13 id., at Section 7.2.3.

not screen the names of directors and beneficial owners of customer companies. Regulators have continued to cite lack of sufficient fuzzy matching in enforcement cases since then.[14]

In addition to the OFAC, NYDFS and FCA guidance, the Wolfsberg Group, an association of 13 global banks, published 'Wolfsberg Guidance on Sanctions Screening' in 2019.[15] The Guidance indicates that sanctions screening should be supported by key enabling functions, such as policies and procedures, a responsible person, a risk assessment, internal controls and testing. These areas roughly correspond to the high-level elements within OFAC's Framework. In addition to Wolfsberg's key enabling functions, the Guidance also discusses principles for generating productive sanctions alerts, the need for metrics and reporting, independent testing and validation, data integrity and criteria used to develop screening technology in-house or to select a vendor to provide these services.

How sanctions screening fits into the sanctions compliance programme

Sanctions screening does not operate in a vacuum; it is an integrated piece of the compliance programme. In this section, we describe some of the key elements of an effective sanctions screening programme in relation to the five high-level areas of compliance articulated in OFAC's Framework.

Governance and risk assessment

When an entity implements proper governance and oversight and performs a sound sanctions risk assessment, there should be clear alignment between identified sanctions risks and the screening programme configuration. If the sanctions risk assessment determines that certain geographies, customers or products present significant sanctions risk, regulators would expect to see that the relevant sanctions lists are utilised for screening and that there are more stringent screening criteria applied in higher-risk areas.

For example, NYDFS requires that sanctions screening attributes address links between the risk assessment and the screening programme configuration. Specifically, screening tools must be based on the risk assessment, configured in a risk-based manner and tested to ensure they provide results in accordance with the identified risks; in addition, the entity must document links between risks

14 See, for example, the cases cited in 'Internal controls – screening'.

15 www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf.

identified and the configuration of the sanctions screening. This is an important reminder that entities should not just implement software to address general sanctions risks; rather, they should identify specific sanctions risks and then develop or procure software that sufficiently addresses those identified risks.

Internal controls – due diligence

To properly screen for potential sanctions violations, sufficient due diligence must be performed. During customer onboarding, the entity must obtain and verify key information to identify the customer, including, but not limited to, name, alternate names, address, date of birth, registration number and country of incorporation, residence or nationality. These attributes are useful during subsequent sanctions screening as they help determine if a potential sanctions match is valid. The entity should also understand ultimate beneficial ownership (UBO) information, key trading partners and supply chain information, where relevant. UBO information, in particular, is relevant in determining if a person or company falls within the sanctions restrictions due to their beneficial ownership of a sanctioned entity. Before processing transactions, the company may need to understand the counterparty UBO, supply chain information, shipping information and mergers and acquisitions (M&A) due diligence information, including UBOs, controllers, goods and services and origin of goods. UBO issues have taken on greater priority in recent years, including, for example, in the landmark US Anti-Money Laundering Act of 2020, which requires (among many other things) that the Financial Crimes Enforcement Network establish a registry of beneficial ownership information. At the time of writing, those efforts are underway. If insufficient due diligence is performed during onboarding and before transactions occur, it is difficult to put an effective sanctions screening programme in place later, when necessary and relevant information with which to identify potential sanctions violations is not present.

Internal controls – screening

Proper sanctions screening processes involve many controls. At a high level, we can consider three distinct phases: (1) inclusion of complete and accurate information; (2) the logic behind how matching occurs; and (3) how potential sanctions violations are evaluated.

The first consideration in sanctions screening is to determine whether you have gathered all of the relevant information. This often involves collating siloed data across different business or product lines. It can also entail ensuring that all

relevant information within those systems is included in the population of data for screening. In several recent OFAC enforcement actions, the agency noted absence of, or failure to properly utilise, relevant data in the sanctions screening process.

- November 2022: Payward, Inc (doing business as Kraken) settled with OFAC for US$362,158.70 for exporting services to users in Iran. OFAC found the violations resulted from Kraken's failure to timely implement appropriate geolocation tools, including an automated internet protocol (IP) address blocking system.[16]
- October 2022: Bittrex, Inc settled with OFAC for US$24,280,829 for processing virtual currency exchanges for over three years, where they possessed IP data, physical address and passport information that indicated that the customer was located in a sanctioned jurisdiction, but did not utilise that information for sanctions screening.[17] As a result, customers with IP addresses or other details indicating origination in Crimea, Cuba, Iran, Sudan and Syria were able to transact with parties in the US and elsewhere using digital currency on Bittrex's platform.
- September 2022: Tango Card, Inc settled with OFAC for US$116,048.60 for transmitting over 27,000 stored value products ('electronic rewards') to individuals with IP and email addresses associated with countries subject to OFAC sanctions (Cuba, Iran, Syria, North Korea and Crimea). OFAC found that although Tango Card used geolocation tools to identify transactions in which its customer – the sender of rewards – was from a sanctioned jurisdiction, it did not use those tools to identify whether award recipients were located in these jurisdictions.[18]
- January 2022: Airbnb Payments Inc settled with OFAC for US$91,172 for processing payments for Cuba-related travel that was outside the approved categories. OFAC noted that neither the guest country of residence and payment instrument information nor IP addresses were gathered for sanctions screening.[19]

16 https://ofac.treasury.gov/system/files/126/20221128_kraken.pdf.
17 https://ofac.treasury.gov/system/files/126/20221011_bittrex.pdf.
18 https://ofac.treasury.gov/system/files/126/20220930_tango_card.pdf.
19 https://ofac.treasury.gov/system/files/126/20220103_abnb.pdf.

- April 2021: SAP SE, the global software provider, settled with OFAC for US$2,132,174 for providing software licences and related services to Iran. Internal audits conducted by SAP between 2006 and 2014 found that it did not screen customers' IP addresses, which limited its ability to determine the location where software was downloaded. OFAC identified the lag in addressing the lack of geolocation IP blocking as an aggravating factor in determining the settlement amount.[20]
- December 2020: BitGo Inc settled with OFAC for US$98,830 for processing digital currency transactions for customers with IP addresses in numerous sanctioned jurisdictions.[21]

Of particular note, between July 2020 and January 2022, of the 30 settlements or 'Findings of Violation' against companies, OFAC mentioned the lack of screening IP addresses in seven.[22] Although there is no regulation that requires IP address screening, it is clear from the regulatory feedback, including recent guidance,[23] that this is expected as part of a successful sanctions screening programme.

Once all relevant information is gathered, the quality of the data must also be addressed. For example, typing errors, non-standard inputs, blank values and inconsistent structure can all impede effective sanctions screening.

The second consideration is the configuration of the sanctions screening. There are many areas to consider when defining the configuration, but we focus on the importance of an effective name-screening process.

Sanctions screening can be performed against standing data within an entity or against transactions. The most common type of sanctions matching is based on name screening, determining whether there is a match between the sanctions list entry and a company's internal information. This is performed, for example, during due diligence on new customers, when due diligence is periodically refreshed, when transactions occur and during M&A activity. Name screening can generate both false-negative and false-positive matches.

False positives occur when names of non-sanctioned entities or individuals are incorrectly matched and flagged as sanctioned. Sanctions screening can reduce false positives and validate matches by leveraging the many attributes included in sanctions lists for individuals, companies, ships, aeroplanes and financial

20 https://ofac.treasury.gov/system/files/126/20210429_sap.pdf.

21 https://ofac.treasury.gov/system/files/126/20201230_bitgo.pdf.

22 Airbnb Payments, NewTek, Payoneer, SAP, BitPay, BitGo and Amazon.

23 https://ofac.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.

institutions. Sanctions lists typically contain several different pieces of identifying information, such as aliases, street addresses, dates of birth, nationalities, passport numbers, tax identification numbers, email addresses, corporate registration numbers, aircraft tail numbers, vessel registration identification numbers, website addresses and digital currency addresses.

However, the risk of false negatives – that is, failure to identify a true match to a sanctioned party – is often much higher than the risk of false positives. A common problem occurs when screening looks only for exact matches, and therefore misses a potential match due to a slight variation in the name. Name variations can occur for a number of reasons, such as the presence of hyphens, use of titles, punctuation, spelling errors, use of initials, acronyms, name reversals, phonetic spellings, abbreviations and shortened names.

Language differences, phonetic transcriptions and transliteration from one alphabet or writing system to another further complicate the landscape of name matching. For example, a lack of standards for the spelling of Cyrillic names in Roman script introduces at least a dozen name variations for the former Russian leader Boris Yeltsin, ranging from Jelzin to Eltsine.

'Fuzzy matching' introduces flexibility in how the screening system matches names and terms. For example, 'Jon' and 'John' might be considered equivalent in a fuzzy matching system, particularly where the last name or date of birth is an exact match. However, the more expansive the fuzzy match criteria become, the greater the risk that the company will become inundated with false positives, which affects the effectiveness and efficiency of the screening process as a whole.

Configuration of fuzzy matching is both art and science. There are many data analytic methods to employ in fuzzy matching, such as sound methods (which use algorithms to turn similar sounding names into the same key to identify similar names), distance methods (which measure the difference in characters between two names), statistical similarity methods (which look at large data sets to train the model to find similar names) and hybrids of these methods. A detailed analysis of the various methods is outside the scope of this chapter, but the more important point is that there is a regulatory expectation that fuzzy matching techniques will be employed and continually fine-tuned to address each company's unique environment and sanctions risk.

In recent years, several OFAC enforcement actions have noted fuzzy match inadequacies, including the following.

- July 2021: Payoneer Inc's US$1,385,901 settlement with OFAC noted several screening failures, including 'weak algorithms that allowed close matches to SDN List entries not to be flagged by its filter'.[24]
- April 2021: MoneyGram Payment Systems, Inc's US$34,328 settlement with OFAC cited, among other things, the company's 'fuzzy logic failures'.[25]
- September 2020: Deutsche Bank Trust Company Americas' September 2020 settlement with OFAC cited, among other things, the company's complete lack of fuzzy matching for names.[26]
- July 2020: Amazon.com Inc settled with OFAC for US$134,523 for Amazon's screening processes, which did not flag orders with address fields containing an address in 'Yalta, Krimea' for the term 'Yalta', a city in Crimea, nor for the variation of the spelling of Crimea.[27] It also failed to interdict or otherwise flag orders shipped to the Embassy of Iran located in third countries. Moreover, in several hundred instances, Amazon's automated sanctions screening processes failed to flag the correctly spelled names and addresses of persons on OFAC's SDN List.
- November 2019: Apple settled with OFAC for US$466,912 for failing to identify that SIS, an App Store developer, was added to the SDN List and was therefore blocked.[28] Apple later attributed this failure to its sanctions screening tool's failure to match the upper-case name 'SIS DOO' in Apple's system with the lower-case name 'SIS d.o.o.' as written on the SDN List. The term 'd.o.o.' is a standard corporate suffix in Slovenia identifying a limited liability company.
- October 2019: General Electric Company (GE) settled with OFAC for US$2,718,581 for accepting payments from an entity on the SDN List.[29] The sanctioned entity was Cobalt Refinery Company, or Corefco. The payments contained Cobalt's full legal entity name as it appears on OFAC's SDN List as well as an acronym for Cobalt (Corefco), but GE's sanctions screening software, which screened only the abbreviation of the SDN's name, never generated an alert on Cobalt's name.

---

24 https://ofac.treasury.gov/system/files/126/20210723_payoneer_inc.pdf.
25 https://ofac.treasury.gov/system/files/126/20210429_moneygram.pdf.
26 https://ofac.treasury.gov/system/files/126/20200909_DBTCA.pdf.
27 https://ofac.treasury.gov/system/files/126/20200708_amazon.pdf.
28 https://ofac.treasury.gov/system/files/126/20191125_apple.pdf.
29 https://ofac.treasury.gov/system/files/126/20191001_ge.pdf.

All of the enforcement examples described above show that failures as to completeness of data and fuzzy matching can lead to ineffective sanctions screening and enforcement actions.

On a related note, one of OFAC's and the UK's Office of Financial Sanctions Implementation's (OFSI) 'mitigating factors' used to determine the final civil penalty amount is the strength of an entity's sanctions compliance programme, including the screening component. More recently, OFAC has increasingly given mitigation credit for meaningful and effective remedial measures, including in the following cases.

- Godfrey Phillips India Limited's March 2023 settlement with OFAC included mitigation for implementing an enhanced compliance policy, including screening, know-your-customer and record-keeping elements, post-violation.[30]
- Kraken's November 2022 settlement included mitigation for several significant remedial measures, including additional geolocation blocking and blockchain analysis tools, and enhancements to compliance training and staffing.[31]
- Toll Holdings Limited's April 2022 settlement included mitigation for the company's extensive remedial measures, including enhanced screening, training and auditing.[32]
- Sojitz (Hong Kong) Limited's January 2022 settlement with OFAC noted that the company revised its screening procedures to require all counterparties in all business transactions be subject to screening.[33]
- NewTek Inc's September 2021 settlement with OFAC noted that it implemented bulk name screening of product registrants and both current and pending distributors against the SDN List. In addition, it noted that the company implemented geo-IP blocking measures to prevent downloading or registering products from blocked locations.[34]
- First Bank SA's August 2021 settlement with OFAC noted that its remediation measures included updating its sanctions screening tool.[35]

30 https://ofac.treasury.gov/system/files/126/20230301_gpi.pdf.
31 https://ofac.treasury.gov/system/files/126/20221128_kraken.pdf.
32 https://ofac.treasury.gov/system/files/126/20220425_toll.pdf.
33 https://ofac.treasury.gov/system/files/126/20220111_sojitz.pdf.
34 https://ofac.treasury.gov/system/files/126/20210909_newtek.pdf.
35 https://ofac.treasury.gov/system/files/126/20210827_firstbank_flowers.pdf.

- In a January 2021 settlement, OFAC noted that Union de Banques Arabes et Françaises now utilises the sanctions screening software used by its largest shareholder, which includes screening the client database, an anti-stripping module, negative news research, risk database research, vessel screening and country screening.[36]
- BitGo, Inc's December 2020 settlement with OFAC noted that the company now performs IP address blocking, as well as email-related restrictions for sanctioned jurisdictions, and performs periodic batch screening, reviews of screening configuration criteria, screening all 'hot wallets'[37] against the SDN List, including cryptocurrency wallet addresses identified by OFAC and a retroactive batch screen of all users.[38]

Finally, it is important to note that the examples thus far have focused on identifying matches for list-based sanctions targets. As noted above, there are other types of sanctions that are more targeted and complex; for example, OFAC's sectoral sanctions, which focus on entities and activities.[39] In 2019, Haverly Systems, Inc settled an OFAC enforcement action for US$75,375 after it invoiced JSC Rosneft, a Russian oil company, for payment within 90 days.[40] The invoices were not paid within that time frame and this violated Directive 2 under the Russia sectoral sanctions, which, at the time of the transaction, prohibited dealing in new debt of greater than 90 days' maturity. Similarly, Standard Chartered Bank was fined over £20 million by the UK's OFSI for loans with maturity of over 30 days to specific entities as part of the Ukraine sanctions.[41]

Another example is the recent ban on US person investment in identified Chinese Military-Industrial Complex Companies (CMICs) on public exchanges; this involves identification of both the investor (are they a US person?) and the activity (does this transaction involve investment in or derivative of, or provide investment exposure to, securities in the specified CMICs?). As sanctions include more complex, targeted criteria, the methods needed to ensure compliance

36 https://ofac.treasury.gov/system/files/126/01042021_UBAF.pdf.
37 Cryptocurrency wallets that are online and connected in some way to the internet.
38 https://ofac.treasury.gov/system/files/126/20201230_bitgo.pdf.
39 https://ofac.treasury.gov/system/files/126/ukraine_eo3.pdf.
40 https://ofac.treasury.gov/system/files/126/20190425_haverly.pdf.
41 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/876971/200331_-_SCB_Penalty_Report.pdf.

likewise become more complex, in some cases requiring companies to flag both the entity and the activity to determine whether potential sanctions violations have occurred.

OFAC's 50 Percent Rule adds an additional element to screening complexity. Under this Rule, any entity owned in the aggregate, directly or indirectly, 50 per cent or more by one or more blocked persons is itself considered blocked, and therefore subject to the same sanctions as the owners.[42] This Rule means that screening may require tools that review and assess an entity's ownership structure, and do not just stop at a review against designated parties' lists. The difficulty in applying the 50 Percent Rule is evident in the recent designation of numerous Russian oligarchs with large, complex business holdings. As in 2014, when some Russian oligarchs were added to sanctions lists after the annexation of Crimea, they have employed various methods such as signing over assets to close relatives, registering entities in secrecy havens and creating nominee shareholders to evade detection through the 50 Percent Rule.

The Wolfsberg Group's sanctions screening guidance contains a discussion regarding the assessment of which data elements to screen.[43] Specifically, the guidance states:

> *Names of parties involved in the transaction are relevant for list based sanctions programmes, whereas addresses are more relevant to screening against geographical sanctions programmes and can be used as identifying information to help distinguish a true match from a false match. Other data elements, such as bank identification codes, may be relevant for both list and geographically based sanctions programmes.*
>
> *In a sanctions context, some data elements are more relevant when found in combination with other attributes or references. For example, detection of sectoral sanctions risk typically requires detection of multiple factors, such as those where both the targeted parties and the prohibited activities are involved. Many controls may not be capable of detecting both factors simultaneously and, therefore, may not be effective.*

42 https://ofac.treasury.gov/system/files/126/licensing_guidance.pdf.

43 www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf.

Internal controls – virtual currency screening

There is incentive for heavily sanctioned countries, such as North Korea, Iran and Russia, to use cryptocurrency to evade sanctions. Recent analysis indicates that cryptocurrency transactions indicating sanctions evasion increased in 2022 to 43 per cent of transactions received by illicit addresses, compared to a relatively small portion in 2021.[44]

OFAC's SDN List includes cryptocurrency addresses that should be blocked.[45] In practice, enforcement of the block relies on compliant cryptocurrency exchanges. If cryptocurrency is transferred with a non-compliant exchange or peer-to-peer, it likely will not be blocked.

Blockchain analysis has indicated that the majority of cryptocurrency transactions related to sanctions evasion were subsequently transferred to centralised exchanges.[46] OFAC sanctioned Russia-based Garantex in 2022, which accounted for the majority of the sanctions-related transaction volume.

The methods used to identity sanctions evasion via cryptocurrency include screening for: the cryptocurrency addresses on the SDN List; addresses associated with those same blocked addresses; addresses associated with known exchange hacks; and addresses associated with ransomware payments, which are often associated with efforts to evade sanctions.

Internal controls – investigation

The third consideration is the evaluation process for potential sanctions violations. After the potential violations are identified through the screening process, manual investigation is required to determine whether there is a true match. If repeated alert closures due to non-matches are obvious during the manual review, these repetitive false matches should be incorporated into whitelists, to ensure that the names generating the false matches will not trigger alerts going forward. However, it is important to note that those whitelists should be reviewed each time changes are made to relevant sanctions lists. Relevant key controls within this area include: sufficient personnel to review sanctions alerts; policies and procedures specifying how alerts are adjudicated and the relevant information that must be included; and procedures for approval and communication of potential sanctions breaches to relevant authorities.

---

44 'The 2023 Crypto Crime Report', Chainalysis, February 2023.

45 OFAC FAQ 563.

46 ibid.

Auditing

Evaluating the auditing component of the sanctions compliance programme involves three key areas of focus with respect to screening. The first is determining if the configuration of automated screening tools is explicitly tied to the sanctions risk assessment. The second is performing an independent evaluation of the software configuration and results. This can be accomplished through an independent party that re-scans existing customers or transactions to determine if they receive similar results. Finally, it is important to determine how the company gains comfort over the outsourcing of any elements of the screening process. Where the entity relies on external parties to provide timely updated sanctions lists, or to screen against the lists and provide alerts, the company needs to confirm for itself whether or not those results match the configuration. As an example of where this can go wrong, in December 2021 TD Bank settled with OFAC for US$115,005 for violations of the North Korea and Drug Kingpin sanctions regimes. Within the North Korea violations, five employees at the North Korean Mission to the United Nations were able to open accounts with North Korean passports because the bank relied on a vendor-supplied politically exposed persons list, which did not include government employees of sanctioned countries.[47]

Training

There are two key aspects to evaluating the training component of the sanctions compliance programme as it relates to screening. The first is determining if those charged with managing the sanctions screening process received specialised training that may include sanctions evasion techniques, data analytic methods related to fuzzy matching, and language or cultural training for understanding how names and punctuation differ between countries. The second is incorporating information learned during the potential sanctions matching process into the sanctions training that is provided to the wider company. For example, after GE discovered the alleged sanctions violations noted above, during testing and auditing of its compliance programme it implemented remedial measures, including developing a training video for employees using the violations as a case study.[48]

47 https://ofac.treasury.gov/system/files/126/20211223_TDBNA.pdf.

48 See footnote 29.

Sanctions screening in an investigation

A sanctions investigation can be initiated for a number of reasons, including an independent evaluation of a company's sanctions compliance programme, a tip from a whistle-blower, an adverse audit or compliance finding, or a regulatory inquiry. As part of any sanctions compliance investigation, the sanctions screening process and tools will require review. The investigation should include:

- review of the due diligence performed and included in the screening process;
- review of the specific data subject to screening and its field mapping;
- independent evaluation of the current screening configuration, such as fuzzy matching, in a test environment to see if it is comparable to what the screening tool is supposed to determine; and
- comparative analysis of search terms run through the existing screening tool against a sanctions search engine to determine if any likely matches were missed over time.

Conclusion

Complete and accurate sanctions screening is a critical component of any successful compliance programme. Many companies utilise automated screening tools to flag potential matches for review. Regulators expect proper oversight and effective use of these tools, which is illustrated in the recent settlement agreements for both financial and non-financial entities. In addition, regulators (and prosecutors) typically credit companies for having sound and effective compliance programmes (including screening controls), even when there are violations, by mitigating the penalties they pursue.[49] While many entities focus on their technical screening capabilities, successful programmes equally require proper oversight, clear mapping between screening configuration and relevant sanctions risks, and regular review to ensure results are complete, accurate and efficient. And while there has so far been little in the way of sanctions guidance and enforcement from the UK and other governments as compared to the US, that appears to be changing, with those other jurisdictions beginning to emulate the US approach (as was the case previously with anti-corruption and anti-money laundering). Companies should therefore consider looking to US compliance best practices (including for sanctions screening) and building from there.

---

49 The US Department of Justice has stated, for example: 'Prosecutors may credit the quality and effectiveness of a risk-based compliance program that devotes appropriate attention and resources to high-risk transactions, even if it fails to prevent an infraction.' www.justice.gov/opa/speech/file/1571911/download.

Part III

Sanctions in Practice

CHAPTER 16

Sanctions Issues Arising in Corporate Transactions

Barbara D Linney and Orga Cadet[1]

Sanctions risk in corporate transactions has increased steadily as sanctions have become more complex and more intertwined with other areas of regulatory compliance. To further complicate the diligence required in these transactions, the footprints of transacting parties have expanded around the globe, and expectations of various stakeholders (such as investors, lenders, insurers and regulators) have heightened. Today, a simple representation of compliance with applicable law no longer adequately addresses sanctions risk. Whether the transaction involves an acquisition, establishment of a joint venture, appointment of an agent, onboarding of a customer or even a divestiture or financing, a full understanding and review of all applicable sanctions, anti-boycott and export control requirements is necessary if enforcement risks are to be minimised.

While this chapter attempts to present diligence principles and methodologies that can be applied irrespective of the jurisdictions of the parties and businesses involved, it will not escape the reader's notice that principles of US law are featured prominently. Examination of potential US law exposure is a necessary element of almost all transaction diligence owing to the broad extraterritorial reach of US primary sanctions[2] and related laws and regulations affecting international business, the robust enforcement of these laws, and the wide-ranging deployment of secondary sanctions designed to advance US national security and foreign policy

---

1 Barbara D Linney is a partner and Orga Cadet is an associate at Baker & Hostetler LLP.

2 US 'primary' sanctions are those that proscribe behaviour of US persons (and, in the case of Cuba and Iran sanctions, non-US entities owned or controlled by them). 'Secondary' sanctions are those that do not proscribe conduct but rather impose consequences on persons engaging in activities identified as contrary to US national security or foreign policy.

goals. That said, diligence must, of course, cover all potentially applicable laws and regulations. A comprehensive multi-jurisdictional review is beyond the scope of this chapter, but examples of commonly encountered issues posed by EU, UK and national laws are addressed, including the challenges presented by broad multilateral imposition of sanctions against Russia as a result of the war in Ukraine.

Scope of sanctions diligence

The establishment of new business relationships poses a myriad of risks when it comes to compliance with sanctions. This is especially so given the substantial overlap of sanctions regulation and enforcement with other regulatory areas, such as anti-boycott and export control laws and regulations. In the United States, both the Office of Foreign Assets Control (OFAC) and the export control agencies have jurisdiction over trade in goods subject to comprehensive embargoes. In addition, some sanctions programmes – notably, the Ukraine/Russia-related sanctions and the Russian Harmful Foreign Activities Sanctions – were implemented simultaneously with export control measures targeting many of the same actors, first in 2014 and then increasingly after Russia invaded Ukraine in February 2022. Furthermore, there is often a high correlation between sanctions evasion, diversion of export-controlled items and corruption. Anti-boycott regulations are viewed in some jurisdictions as sanctions subject to blocking laws. In the financial sector, sanctions compliance measures often double as a means of detecting money laundering and other financial crimes, and vice versa. The result is that sanctions diligence cannot be effective if approached in isolation – rather, prospective parties to transactions should deploy a holistic methodology to ensure that all relevant aspects of transactions are reviewed. Happily, this approach is also less time-consuming and more cost-effective.

Why diligence is important

Global businesses must comply with sanctions and other legal requirements in all jurisdictions in which they do business. This has become vastly more complicated for companies with global footprints, given the volume and scope – yet nuanced differences – of sanctions and export controls adopted by numerous jurisdictions over the past year in response to the invasion of Ukraine. This explosion of new regulation has been accompanied by a steady increase in cooperation and collaboration among the United States and its allies on both implementation and enforcement of sanctions. For example, the Russian Elites, Proxies and Oligarchs Task Force, formed by Australia, Canada, France, Germany, Italy, Japan, the UK,

the US and the European Commission shortly after the invasion, has focused multilateral 'information sharing and coordination to isolate and exert unprecedented pressure on sanctioned Russian individuals and entities'.[3]

In turn, the US agencies have turned to closer collaboration to further US policy goals regarding implementation and enforcement of sanctions and export controls. As part of these joint efforts, on 2 March 2023, the US departments of the Treasury, Justice and Commerce published a 'Tri-Seal Compliance Note' urging multinational companies to be 'vigilant in their compliance efforts and be on the lookout for possible attempts to evade U.S. laws' and reminding the public of the US government's 'unprecedented enforcement efforts to aggressively prosecute those who violate U.S. sanctions and export control laws'.[4]

However, notwithstanding this trend towards more multilateral and interagency cooperation, even small companies that do international business face a risk of both civil and criminal penalties for violating US sanctions due to their activities abroad.[5] Often, requirements of one jurisdiction conflict with those of another (as, for example, when efforts to impose compliance with US primary sanctions run up against EU or national blocking statutes) or apply alongside those of another (such as when US export control rules applicable to items manufactured outside the United States apply in addition to the export control rules of the country of manufacture). In addition, the increasing application of US secondary sanctions creates sanctions risks for companies even if they are in compliance with applicable local laws and not subject to US primary sanctions.

---

3 See 'Global Advisory on Russian Sanctions Evasion Issued Jointly by the Multilateral REPO Task Force' (March 2023) at https://finance.ec.europa.eu/system/files/2023-03/230309-repo-global-advisory_en.pdf (last visited 17 April 2023).

4 Office of Foreign Assets Control (OFAC), 'Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note: Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls' (March 2023).

5 OFAC, 'OFAC Settles with Chisu International Corporation for $45,908 Related to Apparent Violations of the Cuban Assets Control Regulations' (April 2022) (apparent violations against a 'small company largely overseen by a single individual [that] failed to understand U.S. prohibitions on dealings in Cuban property or engaging in transactions related to merchandise of Cuban origin outside the United States').

Another source of risk is the expansion 'by operation of law' of the list-based sanctions of several jurisdictions to entities owned or controlled by listed parties, which requires not only name screening of potential business partners but also an examination of their ownership and control.[6]

Moreover, owing to the 'long-arm' reach of US export control regulations outside the United States to encompass re-exports (from one country to another) and transfers (within another country), non-US companies have not been immune from enforcement action for violations of US export controls[7] and related sanctions.[8] Recent examples include the imposition of fines against a Lebanese company for re-exporting engines of US origin to Syria and OFAC's action against a dental supply company for exporting dental products of US origin to third-country distributors with knowledge that the exports were destined for Iran.[9] Non-US companies also face the risk of being targets of enforcement for evading US sanctions or helping others to evade US sanctions, penalties for causing US persons to violate sanctions, and secondary sanctions for providing material assistance to sanctioned persons. For instance, OFAC penalised a Hong Kong company in January 2022 for omitting references to underlying transactions involving Iran in its US dollar-denominated wire payments, thereby causing the US financial institutions that processed the payments to violate US sanctions.[10] The company settled with OFAC for over US$5 million, despite the fact that the company's employees had acted contrary to company-wide policies and

---

6 See OFAC, 'Revised Guidance on Entities Owned by Persons Whose Property and Interest in Property Are Blocked' (2014); European Commission Opinion of 19 June 2020 on Article 2 of Council Regulation (EU) No. 269/2014; Office of Financial Sanctions Implementation, 'UK Financial Sanctions: General guidance for financial sanctions under the Sanctions and Anti-Money Laundering Act 2018' (December 2020), at 17. While OFAC prohibits certain dealings with non-listed entities based on ownership considerations (generally, 50 per cent or more ownership by one or more blocked persons), it merely cautions against dealings with non-listed entities that are only controlled – but not 50 per cent or more owned – by one or more blocked persons. In contrast, the United Kingdom prohibits dealings both with non-designated entities owned by one or more designated persons and with non-designated entities that are only controlled by one or more designated persons.

7 See, e.g., Bureau of Political Military Affairs, US Dep't of State, BAE Systems plc Consent Agreement (2011); Bureau of Political Military Affairs, US Dep't of State, Qioptiq S.a.r.l. Consent Agreement (2008). See also Bureau of Industry and Security, US Dep't of Commerce (BIS), Order Relating to Ghaddar Machinery Co., SAL (2019) (*Ghaddar*).

8 OFAC, 'DENTSPLY SIRONA Inc. Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations' (2019) (*Dentsply*).

9 See *Ghaddar* (footnote 7); *Dentsply* (footnote 8).

10 OFAC, 'OFAC Settles with Sojitz (Hong Kong) Limited for $5,228,298 Related to Apparent Violations of the Iranian Transactions and Sanctions Regulations' (January 2022).

procedures, thereby demonstrating the importance of actively ensuring compliance rather than passively relying on employees to follow policies and procedures.[11] As Deputy Attorney General Lisa O Monaco stated in her keynote remarks at the '2022 GIR Live: Women in Investigations' conference in June 2022:

> *Every company needs to be pressure-testing its sanctions compliance program, for instance through risk assessments, technology upgrades and industry benchmarking. Every board of directors of such a company should be inquiring whether it is conducting necessary oversight of the company's sanctions controls. Every corporate officer should be committed to ensuring they have the programs, culture, personnel and counsel to identify problem areas and navigate the rapidly changing landscape. And for anyone who seeks to evade sanctions, the warning is simple: the Justice Department is coming for you.*[12]

Long-arm reach is further extended by the broad definition of items subject to the Export Administration Regulations (EAR),[13] which include not only US-origin items and items in the United States, but also foreign-produced items that are subject to the *de minimis* or foreign-direct product rules. The EAR *de minimis* exemption excludes from EAR jurisdiction certain foreign-made items that incorporate not more than a *de minimis* level of US 'controlled content' (itself broadly defined), which ranges from zero to 25 per cent, depending upon the nature of the item and the location of the customer to which the item is sold. The foreign-direct product rules expand EAR jurisdiction to reach certain items produced outside the United States with specified US-origin technology or software or by plants that are a direct product of specified US-origin technology. In certain cases, depending upon the end user or destination of the item, a broader scope of products would be caught by the applicable foreign-direct product rule (e.g., products destined for customers on the Entity List, military end users in Russia or Belarus, or certain end uses in China).

In the merger and acquisition (M&A) context, due diligence is a must if the risk of successor liability for sanctions and export control violations and other offences is to be assessed. Transactions structured as mergers generally pass liability for the pre-transaction activities of the acquired entity to the buyer by operation of law, but successor liability can also arise from stock purchases, as

11 ibid.

12 US Department of Justice, 'Deputy Attorney General Lisa O. Monaco Delivers Keynote Remarks at 2022 GIR Live: Women in Investigations' (June 2022).

13 15 C.F.R. §§ 730–774.

well as transactions structured as asset purchases. Of course, stock purchases that maintain the separate status of the target entity do not create successor liability for the buyer in the strictest sense of the term, but enforcement costs incurred by the target entity in connection with pre-completion violations, with the associated reputational costs, will diminish the value of the buyer's investment in the target entity. Even in jurisdictions without successor liability, difficulties may arise when company assets may include the proceeds of previous sanctions and export control violations.

As for asset purchases, in a string of US cases, beginning with *Sigma-Aldrich* in 2002,[14] the Bureau of Industry and Security of the US Department of Commerce (BIS) has interpreted the International Emergency Economic Powers Act (IEEPA)[15] and the EAR[16] to impose successor liability for export violations on purchasers of assets when 'substantial continuity' of the business results from the transaction.[17] Notably, IEEPA is also the statutory underpinning for all US sanctions programmes except the Cuban embargo. The Trading with the Enemy Act,[18] which authorises the Cuban embargo, contains provisions similar to the IEEPA provisions interpreted in *Sigma-Aldrich*, and goes a step further by purporting to impose obligations on non-US entities owned or controlled by US persons. *Sigma-Aldrich* thus laid the groundwork for both BIS and OFAC to impose successor liability on purchasers of assets when the purchased assets constitute a business that continues under the new owner. As outlined in *Sigma-Aldrich*, a finding of 'substantial continuity' will be supported when:

> *the successor: (1) retains the same employees, supervisory personnel and the same production facilities in the same location; (2) continues production of the same products; (3) retains the same business name; (4) maintains the same assets and general business operations; and (5) holds itself out to the public as a continuation of the previous corporation.*[19]

---

14 *Sigma-Aldrich Business Holdings, Inc.*, Case No. 01-BXA-06, US Dep't of Commerce (29 August 2002) (*Sigma-Aldrich*).

15 International Emergency Economic Powers Act (codified at 50 U.S.C. § 1701).

16 ibid. The Export Administration Regulations also include the US anti-boycott rules. See 15 C.F.R. Part 760.

17 See *Sigma-Aldrich* (footnote 14), at 6, 7 and 12.

18 Trading with the Enemy Act (codified at 50 U.S.C. § 4301).

19 *Sigma-Aldrich* (footnote 14), at 9.

The decision in *Sigma-Aldrich* was not appealed and the parties entered into a settlement agreement, following which the BIS position on successor liability was applied in subsequent settlement agreements with both BIS and OFAC.[20]

The Directorate of Defense Trade Controls (DDTC), which administers the International Traffic in Arms Regulations[21] pursuant to the Arms Export Control Act,[22] likewise has a long history of imposing successor liability dating back to 2003, when the DDTC entered into a consent agreement with Hughes Electronics Corporation and Boeing Satellite Systems, Inc (formerly Hughes Space and Communications). The consent agreement imposed penalties for violations that occurred several years prior to Boeing's acquisition of the Hughes space and communications division in 2000.[23] Since 2003, the DDTC has made regular use of consent agreements to assert enforcement jurisdiction over businesses sold by companies subject to consent agreements, whether in stock or asset transactions. The most recent agreements feature an expanded version of the standard consent agreement clause utilised for this purpose.[24] In addition, the DDTC's position on successor liability is further bolstered by its policy of requiring registered defence companies to agree in writing to assume responsibility for pre-acquisition export licences issued to the acquired business.[25]

Although the US position on successor liability has been criticised by legal scholars, as a practical matter, given OFAC's sweeping discretionary powers and the ability of US export agencies to deny export privileges, parties have tended to settle enforcement actions rather than embark on time-consuming and expensive challenges to agency authority. As a result, the risk of enforcement actions based on the successor liability concept remains an important focus of sanctions and export control diligence.

---

20 See, e.g., BIS, Order Relating to Sirchie Acquisition Company, LLC (2010), and related Settlement Agreement (2009); *Dentsply* (footnote 8).

21 22 C.F.R. §§ 120–130.

22 Arms Export Control Act (codified at 22 U.S.C. 2778 (2014)).

23 Bureau of Political Military Affairs, US Dep't of State, Order, *In the Matter of Hughes Electronics Corporation and Boeing Satellite Systems, Inc.*, and related Consent Agreement (2003).

24 See, e.g., Bureau of Political Military Affairs, US Dep't of State, Order, *In the Matter of 3D Systems Corporation*, and related Consent Agreement, § 5; and Bureau of Political Military Affairs, US Dep't of State, Order, *In the Matter of Honeywell International Inc.*, and related Consent Agreement, § 5.

25 See 'Sample 5-Day Notice' (for Buyer), 'Updating a Registration: Notification of Change for Mergers, Acquisitions, and Divestitures', Directorate of Defense Trade Controls, at www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=fc8aaa9adb74130044f9ff621f9619c3#tab-mad (last accessed 25 June 2020).

In addition to the role of due diligence in detecting potential successor liability, diligence in M&A transactions is essential if patterns of violative behaviour that may continue post-closing are to be discovered. OFAC has shown little patience for companies that have allowed violations to continue post-closing,[26] imposing penalties in a series of recent cases notwithstanding voluntary disclosures filed by the acquirers. Root causes of violations emphasised by OFAC included being 'slow to integrate the subsidiary into the . . . corporate family, including with respect to compliance with U.S. sanctions' (*Expedia*); failure to 'implement procedures to monitor or audit [the subsidiary's] operations to ensure that its Iran-related sales did not recur post-acquisition' (*Stanley Black & Decker*); and not undertaking 'a fuller internal investigation' upon receipt of helpline reports of continued sales to Cuba (*AppliChem*). On 30 March 2023, OFAC announced a US$30 million settlement with Wells Fargo Bank, NA, which, after acquiring Wachovia Bank in 2018, provided a former Wachovia Bank customer with software that enabled it to process trade finance transactions with US-sanctioned persons and jurisdictions.[27] In *Kollmorgen*, a penalty was imposed, notwithstanding the buyer's 'extensive efforts' to ensure its newly acquired subsidiary was complying with US sanctions, because that subsidiary's management engaged in 'egregious conduct' by actively obfuscating continued sales to Iran in an attempt to thwart the buyer's compliance efforts.[28] Similarly, in *Keysight*, a penalty was imposed despite the buyer's directive to its newly acquired subsidiary that continued sales to Iran should cease and the newly acquired subsidiary's assurance that they had – although, as in *Kollmorgen*, the newly acquired company continued sales that were actively concealed from the buyer.[29] However, OFAC and other agencies have made it clear that uncovering potential violations during the diligence process is not enough. OFAC's

26 See, e.g., OFAC, 'OFAC Settles with Keysight Technologies Inc., as Successor Entity to Anite Finland OY, with Respect to Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations' (2020) (*Keysight*); OFAC, 'Expedia Group, Inc. ("Expedia") Settles Potential Civil Liability for Apparent Violations of the Cuban Assets Control Regulations' (2019) (*Expedia*); OFAC, 'Stanley Black & Decker, Inc. Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations Committed by its Chinese-Based Subsidiary Jiangsu Guoqiang Tools Co. Ltd' (2019) (*Stanley Black & Decker*); OFAC, 'AppliChem GmbH Assessed a Penalty for Violating the Cuban Assets Control Regulations' (2019) (*AppliChem*); OFAC, 'Kollmorgen Corporation Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations' (2019) (*Kollmorgen*).

27 OFAC, 'OFAC Settles with Wells Fargo Bank, N.A. for $30,000,000 Related to Apparent Violations of Three Sanctions Programs' (2023).

28 *Kollmorgen* (footnote 26), at 3.

29 *Keysight* (footnote 26), at 1–2.

compliance framework, issued in 2019, notes that mergers and acquisitions 'appear to have presented numerous challenges with respect to OFAC sanctions' but that OFAC nevertheless expects that compliance functions 'be integrated into the merger, acquisition, and integration process' and that '[w]hether in an advisory capacity or as a participant, the [buyer] engages in appropriate due diligence to ensure that sanctions-related issues are identified, escalated to the relevant senior levels, addressed prior to the conclusion of any transaction, and incorporated into the organization's risk assessment process'.[30] The 2021 *SAP* case[31] serves as a stark reminder of the consequences of failure to address compliance gaps identified during M&A diligence and post-acquisition audits. In April 2021, OFAC, BIS and the US Department of Justice announced settlements with the German company concerning, among other things, violations of the EAR and the Iranian Transactions and Sanctions Regulations (ITSR),[32] resulting from failure to integrate various US cloud services providers acquired in transactions dating back to 2011 into its export controls and sanctions compliance programme.

Transactional due diligence will focus on many of the same compliance issues that should be reviewed in the context of M&A activity, but for different reasons. When vetting potential agents, distributors, joint venture partners or customers, a history of non-compliance with sanctions or export control laws can foreshadow a risk of becoming embroiled in violations and enforcement actions in the future. Companies contemplating entering into a transaction with a third party with a less than stellar compliance record should take a hard look at whether the risk that the party will commit violations in the future can be adequately addressed in the agreement governing the transaction and its implementation. If the contemplated transaction is a long-term arrangement, such as a joint venture, care should be taken to ensure that the governing agreement provides a clear exit strategy if violations occur or if changes in the law render continuation of the relationship unlawful.

---

30 OFAC, 'A Framework for Compliance Commitments' (May 2019), at 4–5.

31 OFAC, 'OFAC Settles with SAP SE for Its Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations' (2021) (*SAP*). See also, 'SAP Resolves Allegations of Export Control Law Violations with US$3.29 Million Administrative Settlement, Bureau of Industry and Security' (2021); US Department of Justice, 'SAP Admits to Thousands of Illegal Exports of its Software Products to Iran and Enters into Non-Prosecution Agreement with DOJ' (2021); Non-Prosecution Agreement between SAP and the US Department of Justice (2021), available at www.justice.gov/opa/press-release/file/1390531/download.

32 Iranian Transactions and Sanctions Regulations, 31 C.F.R. Part 560.

What your diligence review should include

Diligence in corporate transactions has both business and legal elements, and both come into play in the context of sanctions, anti-boycott and export control due diligence.

From a legal perspective, verifying compliance with legal requirements is a standard starting point. However, establishing that a target company or potential business partner is in compliance with all applicable legal requirements prior to entering into a transaction will not suffice, as new requirements and risks may take effect when the transaction is consummated, with both business and legal implications.

For example, non-US businesses that come under the ownership or control of US persons will become subject to US anti-boycott rules and certain US primary sanctions[33] requirements upon completion of the transaction. In the anti-boycott context, the rules apply to 'US persons', which is defined to include 'controlled in fact' foreign subsidiaries, affiliates or other permanent foreign establishments of US business entities, which are termed 'domestic concerns' in the rules.[34] 'Control in fact' is defined to consist of 'the authority or ability of a domestic concern to establish the general policies or to control day-to-day operations of its foreign subsidiary, partnership, affiliate, branch, office, or other permanent foreign establishment'.[35]

In the sanctions context, both the Iran and Cuba sanctions extend to non-US entities 'owned or controlled by' US persons.[36] The ITSR provide that:

> *an entity is 'owned or controlled' by a United States person if the United States person:*
> *(i) Holds a 50 percent or greater equity interest by vote or value in the entity;*
> *(ii) Holds a majority of seats on the board of directors of the entity; or*
> *(iii) Otherwise controls the actions, policies, or personnel decisions of the entity.*[37]

Although what constitutes ownership or control is undefined in the regulations governing the Cuba sanctions programme, the definition applicable to Iran reflects OFAC's long-standing interpretation of the reach of the Cuba sanctions as well.

---

33 Iranian Transactions and Sanctions Regulations, 31 C.F.R. Part 560; Cuban Assets Control Regulations, 31 C.F.R. Part 515.

34 15 C.F.R. § 760.1(b).

35 15 C.F.R. § 760.1(c).

36 31 C.F.R. §§ 515.329 and 560.215.

37 31 C.F.R. § 560.215(b)(1).

Diligence should be designed to both ferret out historical compliance lapses and identify activities that will not be permitted post-completion, as well as the effects of implementing prohibitions on the business outlook. Cessation of activities that will be unlawful under US ownership or control may have a material adverse effect on the financial outlook of the acquired business, while compliance failures post-completion will give rise to enforcement risk. Nevertheless, the parties may decide to proceed with the transaction, notwithstanding any detrimental effect on the business that would result from the need to cease certain operations post-completion. In these cases, further diligence should be conducted regarding the legal risks associated with cessation so that advice can be taken on how best to navigate any potential roadblocks, such as those posed by 'blocking' statutes. Several jurisdictions, as well as the European Union, have adopted blocking measures to counteract extraterritorial application of US sanctions against Cuba and Iran,[38] while Canada has restricted its blocking measures to the Cuba embargo[39] and German law targets foreign boycotts.[40] Thus, advice should be taken before completion so that an appropriate plan of action can be formulated, bearing in mind recent enforcement actions against US companies that failed to prevent their recently acquired non-US subsidiaries from continuing business with Cuba and Iran.[41] Litigation risk arising from breach of contract claims brought by parties to discontinued relationships may also be a factor.

Transactional diligence, like compliance programmes, should also be customised to fit the risks presented and the risk appetites of the parties. Some companies subject all potential agents or distributors to background checks; others only apply these requirements to relationships with third parties located in countries or regions considered high risk from a sanctions, corruption or export diversion

38 See, e.g., Council Regulation (EC) No. 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom (as amended by Commission Delegated Regulation (EU) 2018/1100 of 6 June 2018); and, for the position in the United Kingdom, see the European Union (Withdrawal) Act 2018 and the Protecting against the Effects of the Extraterritorial Application of Third Country Legislation (Amendment) (EU Exit) Regulations 2020 (in force 10 January 2021).

39 Foreign Extraterritorial Measures Act, R.S.C. ch. F-29 (1985), as amended by Bill C-54, proclaimed in force 1 January 1997; Foreign Extraterritorial Measures (United States) Order, 1992, as amended, SOR 96-84, 5 January 1996.

40 Foreign Trade and Payments Ordinance, § 7 (Boycott Declaration) (Germany).

41 OFAC, 'Acteon Group Ltd. and 2H Offshore Engineering Ltd. Settle Potential Civil Liability for Apparent Violations of the Cuban Assets Control Regulations' (2019); *AppliChem* (footnote 26); *Stanley Black & Decker* (footnote 26); *Kollmorgen* (footnote 26).

perspective. In the absence of red flags, third-party certification of matters such as ownership and control, as well as compliance, can be considered in place of more extensive diligence.

Diligence checklists must be the subject of continuous improvement. Laws and regulations in the sanctions and export control area change frequently, and these changes usually spawn new diligence requirements, as do new enforcement actions and agency guidance.

In each transaction, care should be taken to ensure that compliance with all applicable sanctions and export controls is reviewed, based on the jurisdiction of formation and places of business, as well as products and services of the target company.

When considering doing business with, or acquiring, a company with operations outside the United States, possible secondary sanctions risk based on the nature of the target's business must also be considered. US secondary sanctions target those doing business with numerous sectors of the Iranian economy, as well as Russia, Venezuela and North Korea, among other countries.

Relationships with customers, agents or distributors in countries or regions characterised by high risk for diversion or corruption should also be scrutinised carefully – several countries in Asia and the Middle East come to mind in this regard, although, perhaps surprisingly to some, US law enforcement officials also view Canada as a country of diversion risk. As OFAC's April 2022 enforcement action against Newmont Corporation indicates, strong controls on dealings with suppliers is critical, including with respect to a company's subsidiaries.[42] In that case, Newmont Corporation's wholly owned subsidiary, Newmont Suriname, failed to include in its purchase orders express statements that no items provided to it may originate from embargoed jurisdictions, and did not obtain country-of-origin information for the goods it acquired from its suppliers. As a result, Newmont Suriname unintentionally purchased Cuban-origin explosives and other prohibited items from a third-party vendor, in apparent violation of the Cuban Assets Control Regulations.

In light of the risk that financing of transactions can itself be the source of sanctions violations, buyers and other borrowers should screen any banks and other financial institutions providing loans and lines of credit and the like. Inversely, lenders should carefully consider the risk that any borrower would directly or indirectly use any proceeds from the lender for sanctions violations

42 OFAC, 'OFAC Settles with Newmont Corporation for $141,442 Related to Apparent Violations of the Cuban Assets Control Regulations' (April 2022).

or repay a loan using the proceeds of sanctions violations. OFAC also released compliance guidance in September 2022 regarding new payment technologies such as instant payment systems that allow near-instantaneous transmission and receipt of payments.[43] While OFAC acknowledged that 'there is no one-size-fits-all approach to managing sanctions risks with regard to instant payment systems', it also encouraged financial institutions to evaluate their risks based on their 'geographic locations and the extent of [their] international presence; the location, nature, and transactional history of [their] customers and their counterparties; the specific products and financial services [they] offer[]; and [their] size and sophistication'.[44]

Other often overlooked but important areas of potential liability when conducting due diligence on non-US companies include application of US sanctions and export control *de minimis* rules and compliance with US export controls applicable to foreign-produced items. Many non-US companies are unaware of the extent to which their products might be subject to US export controls and sanctions as a result of incorporating components of US origin or that have been manufactured using US technology or plant and equipment.

Due diligence should also be designed to uncover practices that have tended to circumvent compliance. For instance, in April 2022, OFAC settled with S&P Global, Inc for apparent violations of the Ukraine-Related Sanctions Regulations in connection with extension of credit to JSC Rosneft, a state-owned Russian oil company, in violation of the debt and equity restrictions imposed by Executive Order 13662.[45] The extensions of credit that caused the apparent violations occurred after Rosneft failed multiple times to timely make payments to S&P, and also failed to timely respond to S&P's requests for payment. S&P ultimately reissued and re-dated multiple invoices to continue to extend credit to Rosneft, leading OFAC to observe that '[t]his case underscores the importance of careful adherence to OFAC regulations, including in cases where counterparties may make compliance challenging'.

Though traditionally an exercise conducted primarily by the buyer, the increasing convergence of sanctions and export controls with other areas of law and regulation, including national security, anti-money laundering (AML) and anti-corruption, has given rise to diligence obligations for all parties to the transaction.

---

43 OFAC, 'Sanctions Compliance Guidance for Instant Payment Systems' (September 2022).

44 ibid.

45 OFAC, 'OFAC Settles with S&P Global, Inc. for $78,750 Related to Apparent Violations of the Ukraine-Related Sanctions Regulations in 2016 and 2017' (April 2022).

In transactions that may be reviewed by the Committee on Foreign Investment in the United States, both parties will need to assess the export controls applicable to the target US business to assess whether mandatory filing requirements apply,[46] and sellers will want to assess the sanctions and export control compliance history of potential non-US buyers, given new rules that ban companies with a history of violations of US sanctions and export controls from enjoying certain exceptions to the mandatory filing requirements.[47] Investors and bankers providing financing for a transaction will want to ensure sanctions and anti-financial crime compliance by all parties, as well as compliance with export controls and sanctions by the acquired company. Representation and warranty insurers likewise will be alert for compliance lapses so that material violations can be excluded from coverage.

Streamlining diligence

As much as possible without compromising compliance, diligence should be streamlined to avoid having to go over the same grounds multiple times. Particularly in the context of M&A activity, the target company's appetite and capacity for responding to diligence requests can wane in the face of competing queries from a myriad of business and legal teams. Furthermore, the rapid pace of change in US sanctions laws (particularly in the context of recent expansion of the Russia sanctions), including the increasingly multilateral approach to international sanctions, can pose compliance risks that require a fine-tuned approach to due diligence. For instance, in the year following Russia's invasion of Ukraine in February 2022, OFAC and BIS have each published over 50 regulatory actions involving Russia, including adding over 2,500 Russia-related targets to the Specially Designated Nationals and Blocked Persons List and over 100 Russia-related targets to the BIS Entity List, and related sanctions and export controls of other jurisdictions have likewise expanded substantially.

Efficiencies can be achieved in the M&A context by minimising the number of requests for the same information. For example, questions relating to sanctions risk assessment, internal controls, testing and auditing, compliance training and management's demonstrated commitment to comply with applicable sanctions and export control law can be grouped with similar questions about other relevant compliance matters. Further efficiencies can be achieved if the various subject matter experts reviewing the responses to diligence queries coordinate their efforts to avoid having multiple reviewers pore over the same document.

46 31 C.F.R. § 800.401.

47 31 C.F.R. §§ 800.219 and 802.215.

In addition, compliance efforts may be fine-tuned by being consolidated, where possible, across multiple sanctions jurisdictions and by proactively accounting for rules that have been announced but are not yet effective.

When onboarding business partners, deployment of multiple work streams should be avoided. Questions relating to sanctions, anti-corruption, AML and export compliance should be consolidated into one online or paper form rather than sprinkled throughout a variety of documents and certification. OFAC has signalled approval of this holistic approach. In a release regarding its 2019 enforcement action against Apollo Aviation Group, LLC, OFAC emphasised the importance of know-your-customer (KYC) diligence – traditionally the purview of export and AML compliance guidelines – in the context of sanctions compliance, noting 'the importance of companies operating internationally to implement Know You [sic] Customer screening procedures and implement compliance measures that extend beyond the point-of-sale and function throughout the entire business or lease period'.[48]

What to do if historical breaches are uncovered

If the diligence process uncovers historical breaches, the parties must decide how to proceed.

If compliance issues are discovered while conducting a background check of a potential customer or distributor, the way forward will depend on whether a relationship is off-limits as a result of the discovery (for example, if the party is on an asset freezing or other applicable sanctions list) or whether a trustworthy relationship can nevertheless be achieved in spite of historical issues (perhaps by imposing and monitoring adherence to various compliance terms and conditions).

In the M&A context, in many cases the seller will learn of the historical breaches first while preparing responses to the buyer's diligence queries. At this point, it will be important to consider whether a disclosure should or must be filed. In the United States, most disclosure processes are voluntary rather than mandatory. However, given the substantial reduction in potential fines for sanctions and export control violations that are voluntarily disclosed, many companies will decide to make a disclosure so as to reduce potential exposure. In some

48 OFAC, 'Apollo Aviation Group, LLC ("Apollo," now d/b/a Carlyle Aviation Partners Ltd.1) Settles Potential Civil Liability for Apparent Violations of the Sudanese Sanctions Regulations', 31 C.F.R. Part 538, 3 (2019) (*Apollo*).

instances, the violation may be deemed not to warrant disclosure (such as a minor record-keeping violation), in which case the seller may elect to implement corrective action and disclose the matter to the buyer but not to the relevant agency.

That said, recent changes in the BIS policy regarding voluntary self-disclosures to that agency have complicated the decision-making process. Voluntary self-disclosure has traditionally been applied as a mitigating factor when assessing civil penalties in enforcement actions. However, in April 2023, the Assistant Secretary for Export Enforcement announced that, going forward, BIS will consistently consider failure to disclose a 'significant possible violation' as an aggravating factor.[49] As a result, companies are now on notice that self-disclosure will result in a 'sharply reduced penalty', while by failing to disclose a significant possible violation, 'they risk a sharply increased one'.[50] The new policy was not accompanied by guidance on how the agency intends to define 'significant' for these purposes, thereby making it difficult to make the necessary assessment. Some have argued that the new policy disincentivises self-disclosure. On the other hand, the Assistant Secretary's announcement also emphasised various benefits of disclosing apparent misconduct by others, such as exceptional cooperation credit in both pending and future enforcement actions and monetary awards available to whistle-blowers. Given the likelihood that both the seller's and the buyer's employees will be aware of potential violations discovered during the due diligence process, the risk that enforcement agencies will become aware of possible violations that are not voluntarily disclosed will be heightened – and this factor, in turn, will have to be weighed by parties that may be inclined not to disclose.

Neither OFAC (which has substantially similar guidelines for assessment of civil penalties) nor the DDTC has publicly adopted a similar new approach to penalty assessment. Likewise, the Department of Justice has not announced any change in its approach to assessment of criminal penalties. Of course, a decision on whether to disclose potential criminal conduct is not to be taken lightly in any context, but the decision in the *SAP* case, announced in late 2019 and described by the Department of Justice as the 'first-ever resolution pursuant to the Department's Export Control and Sanctions Enforcement Policy for Business

49 BIS, 'Clarifying Our Policy Regarding Voluntary Self-Disclosure and Disclosures Concerning Others' (18 April 2023), available at www.bis.doc.gov/index.php/documents/enforcement/3262-vsd-policy-memo-04-18-2023/file.

50 ibid.

Organizations',[51] does illustrate the benefits of disclosure in appropriate circumstances, in the form of substantially reduced penalties, at least under current policy. Whether other agencies will follow the BIS lead remains to be seen.

However, there are circumstances in which disclosure is mandatory (for example, the requirement under the International Traffic in Arms Regulations to disclose violations involving arms embargoed countries, such as China).[52] In addition, in some jurisdictions there may be mandatory obligations to report known or suspected breaches of AML laws or terrorist financing prohibitions,[53] as well as specific obligations to report known or suspected breaches of sanctions.[54] Moreover, EU regulations giving effect to sanctions laws are accompanied by general obligations to report information that would facilitate compliance.

If the filing of a disclosure is determined to be warranted or required, or if an enforcement action is commenced during the period of diligence, the buyer and its counsel may wish to have input into the disclosure or response to the enforcement action. In these circumstances, a joint defence agreement may be considered as a means of protecting privilege. In the absence of a joint defence agreement, sellers should keep in mind that legal privilege does not attach to responses to the buyer's diligence queries. Furthermore, depending upon the jurisdiction, disclosures to one's own in-house counsel likewise may not be protected, in which case it may be prudent to channel compliance diligence regarding potentially sensitive matters through external counsel.

---

51 US Department of Justice, 'SAP Admits to Thousands of Illegal Exports of its Software Products to Iran and Enters into Non-Prosecution Agreement with DOJ' (2021); Export Control and Sanctions Enforcement Policy for Business Organizations, US Department of Justice (13 December 2019), available at www.justice.gov/nsd/ces_vsd_policy_2019/download.

52 22 C.F.R. § 126.1(e)(2).

53 See, e.g., the anti-money laundering reporting requirements that must be implemented in EU Member States in accordance with Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (OJL 156, 19/6/2018), at 43–74.

54 See, e.g., the UK reporting obligation as extended by the European Union Financial Sanctions (Amendment of Information Provisions) Regulations 2017.

Remediation

Both parties can and should take steps to remediate compliance breaches and enforcement risks identified during diligence.

In the lead-up to a merger or acquisition, a seller that discovers historical breaches bears primary responsibility for stopping the unlawful conduct and beginning to implement corrective actions. However, while some remediation steps (such as disciplining employees involved in the misconduct) can be taken fairly quickly, other more systemic responses (such as overhauling compliance programmes and procedures) may be best left to the buyer, particularly if the buyer has a robust compliance programme that it intends to roll out to the newly acquired business. In these instances, the seller may choose to only implement those short-term remediation measures required to ensure that no further breaches occur prior to the closing.

The buyer, however, is responsible for lapses that continue or occur on its watch, and several recent OFAC enforcement actions discussed in this chapter (*Keysight*, *Expedia*, *Stanley Black & Decker*, *AppliChem* and *Kollmorgen*) illustrate the importance of regular compliance monitoring in the context of integrating newly acquired businesses.[55] Therefore, it is not enough merely to have compliance policies and procedures and provide training; companies must also monitor compliance with their policies and procedures if they wish to avoid enforcement action.

This can be of particular concern for newly acquired non-US companies. For instance, as the *Keysight* and *Kollmorgen* cases highlight, parent companies should be particularly careful when acquiring non-US companies that have pre-existing relationships with sanctioned persons and jurisdictions that may continue despite directives from the parent company to the non-US subsidiary that these relationships be terminated.[56] As in both *Keysight* and *Kollmorgen*, the non-US subsidiary may even undertake efforts to conceal continued business with sanctioned parties from the parent company by falsifying corporate records. Because of the risk that non-US subsidiaries may continue to do business with sanctioned parties, it becomes particularly important for companies acquiring non-US companies not simply to rely on certification from non-US subsidiaries that they have ceased the business, but also to take proactive steps to ensure that the business has actually ceased by insisting on parent company visibility into the newly acquired non-US subsidiary's corporate records. Although in both *Keysight* and *Kollmorgen* the buyer

55 See, e.g., *Expedia* (footnote 26); *Stanley Black & Decker* (footnote 26); *AppliChem* (footnote 26); *Kollmorgen* (footnote 26).

56 See *Keysight* (footnote 26); *Kollmorgen* (footnote 26).

did not have knowledge of its newly acquired subsidiary's continued sales to Iran, in *Kollmorgen* OFAC detailed the buyer's 'extensive efforts' to ensure post-acquisition compliance and determined the violations to be non-egregious (imposing a base penalty of only US$7,434 rather than the US$750,000 that would have been imposed if OFAC had found the violations egregious). In finding the violations non-egregious, OFAC credited the buyer's 'extensive and preventative remedial conduct'. However, in *Keysight*, in which OFAC did not make a similar finding as to the buyer's post-acquisition compliance efforts, OFAC found the violations egregious and imposed a base penalty of US$1,051,460 (half the statutory maximum) – the lesson being that the more post-acquisition diligence that is conducted, and the more remedial measures that are implemented, the more likely the buyer is to receive leniency from OFAC should violations continue to occur post-closing. The *SAP* case also illustrates the benefits of remediation. As noted by the Department of Justice, 'SAP will suffer the penalties for its violations of the Iran sanctions, but these would have been far worse had they not disclosed, cooperated, and remediated.'[57] The disclosure, cooperation and remediation culminated in a non-prosecution agreement with the Department of Justice and administrative agreements with OFAC and BIS.

In the context of agreements with customers and other third parties, the parties must decide the extent to which a breach of compliance obligations triggers termination rights. The agreement should also clearly address the role that each party will play in remediation, in the absence of a triggering breach.

Supplementing diligence with compliance representations and covenants

Agreements recording corporate transactions, whether with business partners or buyers or sellers of businesses, contain numerous clauses designed to allocate risks associated with past or future violations.

All agreements should contain basic representations and warranties about the identity and ownership of the parties. To the extent that an agreement is intended to govern a relationship between the parties going forward, it should include covenants of both parties to advise the other if its circumstances change (e.g., if it or any of its owners is added to a sanctions list), as well as covenants to comply

57 US Department of Justice, 'SAP Admits to Thousands of Illegal Exports of its Software Products to Iran and Enters into Non-Prosecution Agreement with DOJ' (2021).

with applicable sanctions and export controls, related information exchange and termination rights, and, if applicable, rights and obligations of the parties in connection with any required remedial action.

The OFAC enforcement action against Apollo illustrates the importance OFAC assigns to regular compliance monitoring in the context of customer relationships.[58] Although the party to whom Apollo leased aircraft engines failed to comply with lease provisions that prohibited the transfer of the engines to a country subject to US sanctions, and the violations were disclosed voluntarily, OFAC nevertheless penalised Apollo, noting that:

> *Notwithstanding the inclusion of this clause, Apollo did not ensure the aircraft engines were utilized in a manner that complied with OFAC's regulations. For example, at the time, Apollo did not obtain U.S. law export compliance certificates from lessees and sublessees. Additionally, Apollo did not periodically monitor or otherwise verify its lessee's and sublessee's adherence to the lease provision requiring compliance with U.S. sanctions during the life of the lease.*

Caution should be exercised, however, as including unmanageable audit requirements in agreements with customers and other third parties can come back to haunt companies that do not avail themselves of their audit rights. This is another area in which collaboration between various compliance functions within a company can add value. For example, personnel who conduct periodic audits for other purposes, such as financial or quality control, can be trained to incorporate checks for sanctions and export compliance into their audit process.

In the M&A context, representations and warranties regarding past compliance are critical, but there is a tension between the objectives of the buyer and seller in negotiating these clauses. Sellers will often prefer to couch these representations and warranties with varying degrees of materiality and knowledge qualifiers, while buyers may favour more robust disclosures.

Purchase agreements typically also contain various provisions under which a buyer may seek indemnification from a seller for breaches of representations and warranties. These clauses impose monetary limitations on recovery, require claims to be made within a certain time, and exclude claims for known exceptions disclosed to the buyer. Occasionally, however, the parties may agree to include special indemnity provisions relating to potentially significant issues. However, it

58 See *Apollo* (footnote 48).

is important to understand that the indemnification clauses, read in the context of the representations and warranties, will define the limits of the seller's responsibility to reimburse the buyer for costs associated with pre-completion compliance lapses. As a result, buyers must satisfy themselves during the diligence process that they are willing to bear any enforcement risk not covered by the negotiated indemnity or representation and warranty insurance, which typically excludes coverage of damages arising from known material violations.

Ongoing diligence expectations

In the end, irrespective of the scope of the representations and warranties that may be negotiated, or how 'clean' the results of a diligence review may be, the enforcement agencies have made clear their expectation that acquirers should conduct further diligence post-completion[59] and that parties to commercial agreements should monitor compliance for the life of the relationship.[60] For instance, OFAC's US$862,318 settlement with First Bank SA and JC Flowers & Co in August 2021 arose from First Bank's alleged violations after being acquired by JC Flowers, and JC Flowers' failure to ensure that First Bank understood the full scope of US sanctions applicable to financial institutions without a physical presence in the United States.[61] Among other things, OFAC clearly expects buyers to conduct heightened diligence of parties known to do business with countries or entities subject to OFAC sanctions, appoint management personnel who are committed to compliance, conduct regular audits and risk assessments, provide ongoing training, and respond to red flags promptly.[62] In the context of commercial relationships, OFAC expects risk assessments, exercise of caution when doing business with entities with known contacts with OFAC-sanctioned entities and jurisdictions, compliance monitoring throughout the life of the relationship, training, KYC screening procedures and, when applicable, the obtaining of compliance certification.[63]

---

59 See, e.g., *Stanley Black & Decker* (footnote 26); *Kollmorgen* (footnote 26).

60 See *Apollo* (footnote 48), and discussion above at 'Streamlining diligence'.

61 OFAC, 'OFAC Enters Into $862,318 Settlement with First Bank SA and JC Flowers & Co. for Apparent Violations of Iran and Syria Sanctions Programs' (August 2021).

62 See, e.g., *Kollmorgen* (footnote 26); *Stanley Black & Decker* (footnote 26); *Expedia* (footnote 26); *AppliChem* (footnote 26).

63 See *Apollo* (footnote 48) and discussion above at 'Supplementing diligence with compliance representations and covenants'.

In light of these ongoing diligence and compliance expectations, buyers evaluating potential mergers or acquisitions and parties contemplating commercial transactions should ensure that their pre-completion due diligence includes not only an assessment of the legal and business risks discussed in this chapter, but also an evaluation of their capacity to meet the expectations of regulators for ongoing diligence and compliance, as well as the enforcement risks they will face if these expectations are not met.

CHAPTER 17

Key Sanctions Issues in Civil Litigation and Arbitration

Satindar Dogra, Kerstin Wilhelm, Sterling Darling and James Bowen[1]

Impact of sanctions on contractual relations

One of the key factors likely to lead to a dispute involving sanctions is a pre-existing contractual relationship that is impacted by the imposition of sanctions after the formation of the relevant contract. This can take a number of forms, the most obvious being where a contractual party is subject to an asset freeze, which would prohibit the provision of funds, goods or services under the relevant contract. However, with the broad range of new sanctions mechanisms put in place since February 2022, contracts can be impacted in a range of ways, including:

- trade sanctions preventing the import or export of contracted goods, including the G7 oil price cap restrictions;
- professional services restrictions (for example, the EU and UK ban on the provision of IT consulting and design services to a person connected with Russia) interfering with the provision of contracted services, including causing interruptions to statutorily required services (for example, hindering or preventing audits);
- restrictions on dealing with or acquiring the securities of specified entities impairing dealings in transferable securities and, in some instances, preventing contracted trades from being settled; and

---

1 Satindar Dogra and Kerstin Wilhelm are partners, Sterling Darling is a counsel and James Bowen is a managing associate at Linklaters LLP. The authors wish to thank their colleagues Michael Lamson, Guillaume Croisant, Clara Tung, Eriko Kadota, Joanne Denton, Gert-Jan Hendrix, Jacqueline Kusserow and Maike Michels for their assistance in the preparation of this chapter.

- restrictions on the provision of trust services interfering with existing trusts and security arrangements in loan documents.

As such, the courts of various jurisdictions have found themselves having to determine the interaction of contractual obligations and sanctions – a collision between contract law and criminal law, which is unusual for businesses to have to grapple with.

Exemptions for pre-existing contracts

In some cases, an exemption, derogation or general licence permits the continuation of a contractual relationship – often subject to onerous conditions. However, there is no general, broadly applicable sanctions principle that exempts pre-existing contracts. Each of the US, EU and UK sanctions regimes – with a particular focus on the sanctions imposed on Russia since February 2022 – deals with pre-existing contractual relationships in a different manner.

This is in part driven by the availability of general licences (and broader licensing grounds) in the US and UK regimes. In both regimes, the tendency has been to deal with pre-existing contracts through the provision of a general licence permitting wind-downs or the continuation of services for a specified period;[2] for example:

- an Office of Foreign Assets Control Determination imposing a US person prohibition on the provision of 'accounting, trust and corporate formation, or management consulting services to any person located in the Russian Federation' was released 8 May 2022, but had a delayed effective date of 7 June 2022;[3]
- the UK regime dealt with the wind-down of the provision of trust services to designated persons by issuing a general licence permitting the continuation of trust services for a 90-day period after designation;[4] and

2 Under the UK regime, this is not always the case; in some instances, UK wind-downs are dealt with through exceptions in the relevant legislation (for example, the wind-down exceptions in relation to the provision of certain professional services in relation to Russia at Section 60DA(2) and(3(b) of the Russia (Sanctions) (EU Exit) Regulations 2019 (Russia Regulations)). It is not presently clear what policy drives certain wind-downs to be dealt with through exceptions and others through licensing.

3 US Department of the Treasury, Office of Foreign Assets Control (OFAC), Determination Pursuant to Section 1(a)(ii) of Executive Order 14071 (8 May 2022).

4 UK General Licence INT/2023/2589788.

- the US blocking of high-profile entities is sometimes accompanied by a wind-down general licence, which authorises all transactions ordinarily incident and necessary to the wind-down of any transaction involving a covered entity, such as the 90-day wind-down general licence issued upon the designation of high-profile Russian entities on 12 April 2023.[5]

Often, these general licences appear to have been issued to mitigate unanticipated impacts of asset freezes; for example, the UK general licence issued in relation to Truphone Limited (which appears to have been prompted by a realisation of the disruption that the sanctioning of Abramov and Frolov, who owned and controlled Truphone Limited, would cause to the UK financial sector).

In the EU, wind-downs have tended to be dealt with through exemptions and specific licensing grounds in the relevant EU regulations that deal with different wind-down scenarios for pre-existing contracts, as EU sanctions law does not provide for a general licensing regime.[6] Hence, the EU legislator tends to follow a more formalistic approach. Particularly in the case of EU-specific licences, EU persons must approach the competent EU authorities on a case-by-case basis.

For various restrictions – principally those that have historically been characterised as 'sectoral sanctions' – the regimes permit the continuation of pre-existing contractual relationships. One example is the restriction on making loans or credits available to various specified classes of persons and entities under the UK, US and EU Russia sanctions regimes.[7] For this restriction, a carve-out to the legislation permits drawdowns to be made under pre-existing facilities where the terms and conditions of the drawdown or disbursement remain unchanged since prior to the imposition of sanctions (subject to compliance with certain other conditions that vary between regimes).[8]

These exceptions reflect a balance struck by sanctioning authorities between achieving the foreign policy goals of sanctions and avoiding unnecessary disruption to legitimate pre-existing business relationships. Ultimately, however, as has

5 OFAC, Russian Harmful Foreign Activities Sanctions Regulations General Licence No. 62 (12 April 2023).

6 See, for example: Article 6 and 6b, Regulation (EU) No. 269/2014; Articles 2(5), 2a(5), 3b(3), 3k(3), (3b) and (3c), Regulation (EU) No. 833/2014.

7 See, for example: Regulation 17, Russia Regulations; and Articles 5(6) and 5a(2), Regulation (EU) No. 833/2014.

8 See Regulation 59, Russia Regulations; and Articles 5(7)(a) and 5a(3)(a), Regulation (EU) No. 833/2014; see also, OFAC FAQ 394, at https://ofac.treasury.gov/faqs/394.

been seen over the past year, pre-existing business relationships (and the harm to companies incorporated in friendly states occasioned by disruption to these) will take a backseat to geopolitical goals.

Non-performance: illegality, frustration and force majeure

However, assuming that no exemption, derogation or general licence permits the continuation of a contractual relationship, one or both parties are likely to consider whether they will accrue civil liability for failing to perform their obligations under the relevant contract or whether any statutory common law or contractual protection exists.

Statutory protections from civil liability

Both the UK and EU sanctions regimes include express protections from civil liability for actions taken to ensure compliance with sanctions.[9] In the UK, this protection is cast broadly – protecting acts and omissions that take place in the 'reasonable belief' that they are in compliance with sanctions – and this has recently been considered by the Commercial Court of England and Wales. The Commercial Court evidenced a willingness to look at the underlying decision-making around payment to determine the objective reasonableness of the decision.[10] In the EU, no liability arises if acts and omissions are carried out in good faith on the basis that they were in accordance with the respective EU regulation and unless it is proven that the EU person acted negligently, although this only assists in relation to EU asset freezes (and not in relation to EU sectoral sanctions).

Common law protections from civil liability

In addition, in common law jurisdictions, the common law doctrine of illegality may operate to prevent liability from accruing for contractual breaches.

9 See Section 44, Sanctions and Money-Laundering Act 2018 (SAMLA); Articles 10(1) and 11, Regulation (EU) No. 269/2014; and Article 11, Regulation (EU) No. 833/2014.

10 *Celestial Aviation Services Limited v. Unicredit Bank AG (London Branch)* [2023] EWHC 1071 (Comm).

In England and Wales, this doctrine has a number of limbs potentially relevant to sanctions:

- the English courts will not compel a party to perform a contract (or award damages for its breach) where the obligation is rendered unenforceable by a statute; in the sanctions context, this would be a contractual obligation to make a payment to a person subject to a UK asset freeze;[11]
- the English courts will not compel a party to perform a contract (or award damages for its breach) where to do so contravenes the proper law of the contract[12] or would require an unlawful act in the place of performance;[13] and
- more generally, the English courts will take into account public policy considerations in certain circumstances while assessing whether a contract should be valid and enforceable, although one of the primary public policy considerations that should be taken into account is the public interest in the enforceability of freely entered contractual relations.[14]

A number of sanctions cases have turned on the second limb, above. A frequent issue that arises is where the performance of the contract would not contravene UK sanctions but involves a dollar payment that is argued to necessarily involve the performance of some part of the contract in the US (because of the involvement of US correspondent banks). The UK courts have not tended to give much weight to these arguments, finding that it would be open to payers to make US dollar payments in cash and so without the involvement of US correspondent banks – even if the preparatory steps to making the payment might be illegal

11 Noting that not all contractual obligations that might involve a contravention of statute will necessarily be rendered unenforceable by this doctrine; see *Okedina v. Chikale* [2019] EWCA Civ 1393, where the court adopted a purposive approach. In the sanctions context, however, it seems almost certain that a payment obligation expressly prohibited by an asset freeze would be amenable to the illegality defence (in addition to the statutory defence under Section 44, SAMLA). On a related note, see *Al-Kishtaini v. Shanshal* [2001] EWCA Civ 264, in which the Court of Appeal determined that it would be contrary to public policy to compel the repayment of monies that had been advanced contrary to public policy.

12 *Kleinwort, Sons & Co. v. Ungarische Baumwolle Industrie Aktiengesellschaft* [1939] 2 K.B. 678.

13 This is known as the rule in *Ralli Bros* (based on *Ralli Brothers v. Compañia Naviera Sota Y Aznar* [1920] 2 K.B. 287, 297).

14 *Printing and Numerical Registering Co v. Sampson* (1875) L.R. 19 Eq. 462.

in the United States,[15] and even if the contractual documents governing the relationship between the parties provide for payment to be made through a US correspondent bank.[16]

In US courts, the precise contours of a defence based on the doctrine of illegality will depend on the law applicable to the dispute (e.g., the law of a particular US state). In general, however, a party cannot successfully enforce or defend upon a contract that is illegal under the laws of a US state or under the laws of the United States.[17]

By way of an example of an Asian jurisdiction applying the common law, Singapore law largely mirrors English common law on illegality in that a court may decline to enforce a contract prohibited by domestic or foreign law (including where the prohibition arises from sanctions) or where the contract is entered into with the object of committing an illegal act.

While there are currently no reported Singaporean cases specifically on sanctions forming grounds of illegality, it is likely that the courts will apply general principles of illegality to the sanctions context. The courts have, however, indicated that they will apply the usual test for frustration in determining whether the imposition of sanctions would constitute frustration of the contract.[18]

Civil law regimes

While EU sanctions are directly applicable in EU Member States, the effects of those sanctions on contracts are determined by the national law of each Member State. These effects might take different forms and include voidness of a contract concluded after the imposition of sanctions[19] and impossibility to perform obligations entered into before the imposition of sanctions.[20]

---

15 *Libyan Arab Foreign Bank v. Bankers Trust Co.* [1989] Q.B. 728, at 744.

16 *Celestial Aviation Services Limited v. Unicredit Bank AG (London Branch) [2023]* EWHC 663 (Comm), at [174] and [175].

17 See, e.g., Restatement (First) of Contracts, § 608.

18 *VTB Bank (Public Joint Stock Co) v. Anan Group (Singapore) Pte Ltd* [2018] SGHC 250 at [77].

19 e.g., Section 134, German Civil Code; Articles 1128, 1162 and 1178, French Civil Code; and Article 5.58, Belgian Civil Code.

20 e.g., Section 275, German Civil Code (Court of Justice of the European Union (CJEU) Case No. C-117/06, *Möllendorf*); Article 1218, French Civil Code (on *force majeure*); and Article 5.226, Belgian Civil Code.

In addition, if the contract and its performance remain legal but the sanctions have triggered negative economic consequences, parties may try to renegotiate a contract on the grounds of a hardship clause or that it was not foreseeable.[21]

Contractual protections from civil liability

Frequently – particularly given uncertainties around the application of the common law illegality principle[22] – parties will have sought to address sanctions considerations in their contracts. This may be through an express sanctions clause, or the parties may seek to rely on *force majeure* or illegality clauses.

Each question of contractual interpretation will turn on its own facts. Some recent key cases – spread across a range of jurisdictions – include the following.

- *MUR Shipping BV v. RTI Ltd*,[23] in which an arbitral tribunal applying English law was held to have incorrectly determined that a 'reasonable endeavours' provision in a *force majeure* clause could require the non-sanctioned party to a contract to agree a variation to a contract to permit it to make payment in a sanctions-compliant manner; the position at English law was clarified: the 'reasonable endeavours' obligation was around the use of reasonable endeavours to perform the contract, rather than to modify the contract.
- *Red Tree Investments, LLC v. Petroleos de Venezuela, SA*,[24] in which the court notes that the provisions of a credit agreement 'demonstrate that the parties contemplated that the activities of [Petroleos de Venezuela, SA (PDVSA)] could "become the subject of sanctions . . . imposed by [the Office of Foreign Assets Control]" or require a governmental approval or license at some point in the future. The parties could have but did not contractually excuse or postpone PDVSA's performance in that eventuality. Certainly, none of the agreements excused performance if members of the banking community were hesitant, reluctant or unwilling to process lawful payments because of risk-adversity on sanctions. Because the expansion of the pre-existing Venezuelan sanctions to include a state-owned business and the risk-adverse reaction

21 e.g., Section 313, German Civil Code (however, the applicability of this for sanctions cases is debated in literature and will only be relevant where no impossibility based on Section 275 of the German Civil Code applies); Article 1195, French Civil Code (on lack of foresight); and Article 5.74, Belgian Civil Code (on change of circumstances).

22 Noting, in this regard, *Chitty on Contracts*, 34th edition (Sweet & Maxwell, 2022), at 18-002, which draws out in detail judicial criticism of the unsatisfactory current state of the doctrine of illegality.

23 *MUR Shipping BV v. RTI Ltd* [2022] EWHC 467 (Comm) at [131].

24 *Red Tree Invs., LLC v. Petroleos de Venezuela, S.A.*, No. 19-CV-2519 (PKC), 2021 WL 6092462 (S.D.N.Y. 22 December 2021), appeal docketed, No. 22-232 (2d Cir. 3 February 2022).

of some members of the banking community could have been foreseen and guarded against in the contract, defendants cannot meet its burden of proof on the affirmative defense of impossibility'.

- *Kuvera Resources Pte Ltd v. JPMorgan Chase Bank, NA*,[25] where the High Court of Singapore held that the defendant bank was entitled to rely on the sanctions clause to refuse payment under a letter of credit relating to sale of coal shipped on a Syrian-owned vessel that fell within the scope of US sanctions on Syria.

Civil litigation

Aside from the impact on contractual relationships of sanctions that may potentially lead to civil litigation, the involvement of a Specially Designated National or person subject to an asset freeze may have a number of impacts on civil litigation to which they are a party – both procedural and substantive. This is notwithstanding the fact that none of the UK, US or EU have taken steps to bar designated persons from access to their courts, and any decision to do so would no doubt face challenges based on rule-of-law.

Ability of a sanctioned litigant to have a judgment or costs order entered into against it

A key initial challenge to a claim by a sanctioned litigant will be the defendant or defendants asserting that it is not possible, under applicable sanctions regimes, for judgment to be granted in favour of the sanctioned litigant; in particular, a litigant subject to a UK or EU asset freeze or US blocking sanctions. In the UK, a January 2023 case[26] confirmed that the entering into of a judgment in favour of a person subject to an asset freeze does not amount to a 'dealing' in the underlying cause of action that would be prohibited by an asset freeze. This was consistent with a previous line of cases in which it had been held that entering a judgment debt against a sanctioned person did not contravene sanctions, and interestingly, where the payment fell to be made outside the EU (as was at the relevant time), no licence was required (in the specific circumstances of the case).[27]

25 *Kuvera Resources Pte Ltd v. JPMorgan Chase Bank, NA* [2022] SGHC 213.

26 *PJSC National Bank Trust and other v. Boris Mints and others* [2023] EWHC 118 (Comm) at [134] to [138], [162] (*Mints*).

27 *R v. R* [2016] Fam 153 at [26].

An ancillary argument deployed in the *Mints* case was that permitting proceedings to continue while the claimants remained subject to an asset freeze would cause serious prejudice to the defendants because the claimants would be unable to satisfy adverse costs orders, provide security for costs or, in the particular circumstances of the *Mints* case, satisfy cross-undertakings in damages. These arguments were given short shrift in the *Mints* case, in which it was confirmed that it was possible for Office of Financial Sanctions Implementation (OFSI) to license the payment of an adverse costs order, the provision of security for costs or a payment under a cross-undertaking in damages.[28]

Under US sanctions laws and regulations, US proceedings against a sanctioned litigant are possible, although the persons participating in those proceedings must comply with regulations relating to reports on litigation, arbitration and dispute resolution proceedings.[29] However, the regulations make clear that an attachment, judgment, decree, lien, execution, garnishment or other judicial process with respect to blocked property requires an applicable licence.[30]

Likewise, EU sanctions do not prohibit a judgment from being rendered against a sanctioned defendant. However, enforcement of the judgment may prove difficult if the defendant entity is subject to any type of asset freeze. In its judgment in the *Bank Sepah* case,[31] the Court of Justice of the European Union held that the attachment of frozen funds would constitute a change of their destination in breach of an asset freeze. Hence, any attempt at enforcing a judgment against the frozen assets of a sanctioned entity would require prior authorisation by the relevant sanctions authority.

28 *Mints* at [179], [183] and [198].

29 31 Code of Federal Regulations (C.F.R.) § 501.605.

30 31 C.F.R. § 501.605(c).

31 *Bank Sepah v. Overseas Financial Ltd. And Oaktree Finance Ltd.*, CJEU, 11 November 2021, ECLI:EU:C:2021:903.

Acting for a sanctioned litigant

The US, UK or EU do not prohibit providing legal advice to, or making an appearance for, a sanctioned litigant.[32] In the US, this is based on applicable general licences, in light of the general prohibition on providing services to a blocked person. However, it is likely to be impossible to receive payment from a sanctioned litigant in respect of legal fees (or disbursements) in the absence of an applicable exception or general licence.

In the UK, a general licence[33] permits the payment of legal fees and expenses (up to a cap of £500,000, with a further £25,000 of expenses permitted, although only where total fees are not estimated to exceed this amount)[34] where either: (1) the legal fees are based on an obligation entered into with the designated person prior to the date of their designation; or (2) certain specified hourly rates provided for in the general licence are not exceeded.

It is open to a designated person to apply for a specific licence if these caps are to be exceeded, but a recent case involving VTB was adjourned notwithstanding the existence of the general licence because of delays involved in obtaining a specific licence to pay for legal fees above the cap.[35]

By contrast, the EU does not have a similar general licence in place but does allow national sanctions authorities (on an ad hoc basis) to authorise the release of frozen funds provided those funds are exclusively for payment of reasonable professional fees or reimbursement of incurred expenses associated with the provision of legal services.[36] The sanctions regulations do not place a cap on the fees but leave it up to the national sanctions authority to decide whether a cap should be imposed in each individual case.

In addition, while EU law does not generally restrict access by sanctioned persons or persons from sanctioned jurisdictions to courts of EU Member States, there is a general prohibition on the provision of legal advisory services to the

---

32 It is worth noting in this regard the decision of Justice Adrian Jack in *JSC VTB Bank v. Alexander Katunin* (BVIHC (COM) 2014/0062, 22 March 2022) in which he determined that it was not open to solicitors to VTB to come off the record upon VTB being subject to a UK asset freeze (which took effect in the British Virgin Islands under the Russia (Sanctions) (Overseas Territories) Order 2020), and which specifically stated, '[s]ave that their assets are frozen, sanctioned entities retain all their civic rights, including full access to the Courts and an entitlement to have their rights and obligations determined by this Court', at [12] , www.eccourts.org/jsc-vtb-bank-v-alexander-katunin-4/ (accessed on 2 April 2023).

33 UK General Licence INT/2023/2954852.

34 *VTB Commodities Trading DAC v. JSC Antipinsky Refinery* [2022] EWHC 2795, at [31].

35 *VTB Commodities Trading DAC v. JSC Antipinsky Refinery* [2022] EWHC 2795, at [69] and [70].

36 See Article 4, EU Regulation No. 269/2014.

government of Russia or legal persons, entities or bodies established in Russia. Nonetheless, a significant carve-out is made if these services are strictly necessary for the exercise of the right of defence in judicial proceedings, the right to an effective legal remedy and the right of access to judicial, administrative or arbitral proceedings in a Member State (as well as subsequent enforcement proceedings). As such, even sanctioned persons remain able to bring and participate in proceedings in the EU.

Under US sanctions regimes, there is typically a general licence for the provision of certain legal services, which includes 'representation of persons named as defendants in or otherwise made parties to legal, arbitration, or administrative proceedings before any U.S. federal, state, or local court or agency'; 'initiation and conduct of legal, arbitration, or administrative proceedings before any U.S. federal, state, or local court or agency'; 'representation of persons before any U.S. federal, state, or local court or agency with respect to the imposition, administration, or enforcement of U.S. sanctions against such persons'; and 'provision of legal services in any other context in which prevailing U.S. law requires access to legal counsel at public expense'.[37] A further general licence typically authorises payments for legal services from funds originating outside the United States (i.e., from non-blocked funds).[38] However, it is necessary to confirm the exact general licences available under the relevant programme under which the sanctioned litigant is blocked.

Finally, notwithstanding the possibility of acting for a sanctioned litigant if an appropriate licence or exception can be relied upon, legal professionals should be aware of the reputational risks associated with acting for sanctioned persons. In the UK, this has been particularly acute in the context of acting in defamation actions against journalists or critics, and HM Treasury has recently indicated that there is a presumption that licences will not be granted for defamation cases and the above-referenced general licence will be amended to carve out defamation actions.[39]

37 See, e.g., 31 C.F.R. § 587.506.

38 See, e.g., 31 C.F.R. § 587.507.

39 Statement to UK Parliament of Baroness Penn (30 March 2023) UIN HLWS686, https://questions-statements.parliament.uk/written-statements/detail/2023-03-30/hlws686 (accessed on 2 April 2023).

Other practical impacts of sanctions on civil litigation

Availability of witnesses and travel bans

Sanctions may also affect the ability of witnesses to give evidence at trial.

In the UK, the Secretary of State may designate individuals as being the subject of travel bans.[40] These individuals are unable to enter the UK and may not be able to attend court in-person to give evidence. No guidance has been issued about whether a court would allow an application to hear evidence given remotely due to the witness being unable to enter the UK as a result of a travel ban, although this would seem like a potential solution.

The same applies for the EU: individuals subject to an EU asset freeze are generally also subject to EU travel bans. Under EU law, EU Member States may grant exemptions from travel bans (e.g., for the EU Russia sanctions regimes) where travel is justified on the grounds of urgent humanitarian need or on grounds of attending certain intergovernmental meetings.

Under US sanctions, the entry into the United States of persons subject to blocking, as immigrants or non-immigrants, is generally suspended, although the Secretary of State or the Secretary of Homeland Security can authorise exceptions, if warranted. For example, blocking-related executive orders typically contemplate 'a recommendation of the Attorney General, that the person's entry would further important United States law enforcement objectives'.[41]

Payment of court fees

As well as considering a sanctioned entity's ability to pay its lawyers, thought must also be given to the payment of court fees. In the UK, a licence (general or specific) will be required for a designated person to pay court fees. Under US sanctions, general licences may permit the payment of fees from funds outside the US.

Under EU sanctions law, the competent authorities of the Member States may authorise the release of certain frozen funds that are intended exclusively for payment of reasonable professional fees or reimbursement of incurred expenses associated with the provision of legal services.[42] However, no EU guidance exists

40 Guidance issued by the Home Office (11 November 2022), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1118529/Travel_bans_guidance.pdf (accessed on 4 April 2023).

41 See, e.g., Executive Order 15065 – Blocking Property of Certain Persons and Prohibiting Certain Transactions With Respect to Continued Russian Efforts To Undermine the Sovereignty and Territorial Integrity of Ukraine (21 February 2022).

42 See, for example, Article 4(1)(b), Regulation (EU) No. 269/2014.

regarding whether court fees are covered by this provision (although arguments based on rule of law and right to be heard may be available in favour of permitting the payment of court fees in a similar manner to legal fees).

While the designated person's lawyers may decide to pay court fees up-front, and later invoice these to the client, there is a risk of this being seen as making a financial benefit available to a designated person (or as a circumvention of sanctions). OFSI guidance suggests that these payments may contravene the sanctions if the financial benefit is 'significant'.

Arbitration

Impact on parties

There are many ways in which sanctions can impact the procedure of arbitration, and, given the international nature of arbitration, numerous sanctions regimes may apply. To assess which regimes apply and their impact, parties may need to consider:

- the nationality, residence and location of the parties, arbitrators, legal counsel and witnesses;
- the seat of the arbitration;
- the location of the subject matter of the dispute;
- the location of any assets against which enforcement is sought;
- the location of any bank accounts to and from which payments may be made; and
- any sanctions laws that purport to have extraterritorial effect.

Referring a dispute involving a sanctioned party to arbitration is generally (in itself) not precluded by UK or EU sanctions, and with respect to the US is generally (in itself) not precluded with respect to arbitration in the United States. However, whether acting for or against a sanctioned party, sanctions will impact the payment and receipt of funds in connection with the arbitration, including the ability of: arbitrators to receive their fees; any arbitral institution to receive administrative or tribunal fees and any registration fee; the sanctioned party to pay or receive payment in satisfaction of the award; and any banks involved to process any payment. Applications for licences to authorise these payments can take many months. Parties should consider at the outset how sanctions might impact the procedure of the arbitration and apply for any necessary licences as early as possible to avoid delays in the procedure, particularly if a limitation period

is near expiry and a licence is required before an arbitral institution will accept payment of a registration fee and register the arbitration. Under US regulations, certain reports are also required.[43]

If a party wishes to nominate an arbitrator or expert from a sanctioned country, or the seat of the arbitration is in a sanctioned country, parties should consider whether any applicable sanctions regime contains comprehensive territory-wide sanctions. For example, the US maintains comprehensive sanctions against Cuba, Iran, North Korea, Syria and the Crimea and so-called 'Donetsk People's Republic' and 'Luhansk People's Republic' regions in Ukraine, which generally prohibit participation in most commercial activities within those countries. This may, for example, prohibit a US party from nominating an arbitrator based in Iran, or prevent a US arbitrator from sitting in an arbitration that is seated in the Crimea region of Ukraine. In the EU and the UK, sanctions regimes tend to be targeted to specific individuals and entities; however, parties should consider whether an arbitrator appears on a sanctions list. For example, as a result of sanctions imposed by the government of China in March 2021, barristers from Essex Court Chambers may be unable to sit as arbitrators in arbitrations involving Chinese parties or seated in China.

Impact on arbitrators

Where one of the parties to an arbitration is sanctioned, arbitrators may be precluded from acting as arbitrator, or from receiving payment for their services as arbitrator, in the absence of a licence or authorisation from any relevant sanctions authority. The applicable sanctions regime may contain an exemption that covers payments of arbitrators' fees[44] or require that prior authorisation or a licence is obtained from the relevant sanctions authority. It may be necessary to make a licence application to more than one sanctions authority, and (if the terms of the licence authorise only a specific amount) multiple applications may be required over the course of the arbitration to authorise additional payments.

43 31 C.F.R. § 501.605.

44 Exemptions often refer to legal fees and fees for the provision of legal services, without specifying whether this includes arbitrators' fees. If in doubt, parties should seek a licence or clarification from the relevant sanctions authority.

For example, an arbitrator (of any nationality) in an arbitration seated in London would be unable to receive payment for their services[45] from a sanctioned person without a licence from OFSI. In the absence of a general licence from OFSI permitting these payments,[46] the arbitrator would need to apply for a specific licence.[47] For cases administered by the London Court of International Arbitration (LCIA), the payment of the arbitrators' fees from persons subject to UK sanctions against Russia and Belarus to the LCIA, and the LCIA's onward payment of those fees to the arbitrators, is covered by the general licence issued by OFSI on 17 October 2022 (discussed below). Similarly, an arbitrator (of any nationality) in an arbitration seated in the EU or the US would require a licence from the relevant sanctions authority (whether a specific licence or, in the case of the US, an applicable general licence) before receiving payment for their services. In addition, a US arbitrator would require a licence from the relevant sanctions authority to serve as an arbitrator outside the United States, where a blocked person is a party.

In addition to the arbitrator receiving authorisation, the sanctioned party will also need to seek authorisation from the relevant sanctioning country (or countries) to access its frozen funds to make the payment, and a further authorisation may be required for any bank processing the payment.

Impact on arbitral institutions

Arbitral institutions will be bound by the sanctions legislation applicable in their jurisdiction, which may impact their ability to register new cases, receive funds and administer cases involving sanctioned entities. The International Chamber of Commerce (ICC), LCIA and the Stockholm Chamber of Commerce have

45 Merely accepting an appointment as arbitrator and acting as an arbitrator is unlikely to constitute a breach of UK or EU sanctions. However, under US sanctions, serving as arbitrator may (depending on the restrictions that apply to the sanctioned party) be considered to be a prohibited provision of services to a sanctioned party and therefore require a licence.

46 On 28 October 2022, the Office of Financial Sanctions Implementation issued a general licence permitting the payment of professional legal fees and counsel fees (up to a maximum of £500,000) owed by persons sanctioned under the Russia Regulations or the Republic of Belarus (Sanctions) (EU Exit) Regulations 2019 to UK law firms and UK barristers. UK General Licence INT/2023/2954852 does not, on its face, cover arbitrators' fees.

47 The payment of 'reasonable professional fees for the provision of legal services' and 'reasonable expenses associated with the provision of legal services' are permitted licensing grounds (see, e.g., Schedule 5, Paragraph 3, Russia Regulations 2019.

confirmed that they will continue to accept requests for arbitration and administer cases brought by or against sanctioned entities.[48] However, they will carry out due diligence and request information from the parties (before registering and during the arbitration) to identify whether any licence or exemption application needs to be made. This is likely to necessitate delays in the arbitration procedure.

For arbitrations administered by the LCIA, on 17 October 2022, OFSI issued a general licence of indefinite duration permitting persons sanctioned under the Russia (Sanctions) (EU Exit) Regulations 2019 and the Republic of Belarus (Sanctions) (EU Exit) Regulations 2019 to make payments to the LCIA for arbitration costs (including the tribunals' fees and expenses, the LCIA's administrative charges and the registration fee), and permitting the LCIA to use these funds to pay for arbitration costs. However, the general licence does not apply to cases in which the LCIA merely acts as fund holder, or to United Nations (UN) Commission on International Trade Law cases administered by the LCIA. In these cases, and in arbitrations administered by other institutions, specific licences will be required before payments are made.

The ICC's Note to Parties and Arbitral Tribunals on ICC Compliance provides guidance to parties and arbitrators in ICC arbitrations involving a sanctioned party. For example, where any party is subject to US sanctions, no payment by any party may be made in US dollars (including the filing fee). Instead, the ICC may apply a different fee scale denominated in euros.

As a result of sanctions, there has been a rise in the number of parties choosing arbitral institutions in jurisdictions that do not have comprehensive sanctions regimes (the Hong Kong International Arbitration Centre being a popular example). However, this would not avoid the need for arbitrators and processing banks to comply with sanctions applicable to them.

Enforcement of awards

Numerous sanctions issues may arise when a party seeks to enforce an award. Enforcement of an award that involved sanctions issues may be resisted on one of two grounds under the New York Convention: (1) if the subject matter of

48 On 17 June 2015, the International Chamber of Commerce, the London Court of International Arbitration and the Stockholm Chamber of Commerce issued a joint statement entitled 'The potential impact of the EU sanctions against Russia on international arbitration administered by EU-based institutions', which explained that the sanctions imposed by the EU on Russia in 2014 do not preclude parties from referring their disputes to arbitration at an EU-based institution or result in a substantial change in the administration of arbitral proceedings, with the exception of compliance measures.

the dispute was not considered arbitrable according to the rules in the enforcing country; or (2) if recognition or enforcement of the award would be contrary to public policy in the enforcing country.[49]

In terms of arbitrability, the prevailing view among commentators and in most jurisdictions is that disputes involving sanctions are arbitrable. However, some national courts have held otherwise. A good example of the diverging views is the *Fincantieri* cases, which concerned a dispute between two Italian companies and an agent they had appointed to conclude contracts with the Republic of Iraq. The tribunal ruled[50] that the dispute was arbitrable, and the Swiss Federal Tribunal affirmed that decision,[51] rejecting the allegation that the dispute was not arbitrable as a result of the UN embargo against Iraq. However, in parallel proceedings before the Italian courts, the Genoa Court of Appeal held that the dispute was inarbitrable and should instead be referred to the Italian courts.[52] In subsequent proceedings in Paris, the Paris Court of Appeal refused to enforce the decision of the Genoa Court of Appeal, reasoning that the dispute was arbitrable and that therefore the Genoa Court of Appeal did not have jurisdiction to determine it.[53] Parties should check the position in any domestic courts in which enforcement may be sought.

In terms of public policy, different courts take different views on what constitutes 'public policy'. However, a number of courts have distinguished between transnational sanctions regimes (such as UN sanctions and, for EU Member States, EU sanctions), which may form part of international public policy, and sanctions regimes imposed by individual states, which do not.[54] The 'contrary to public policy' exception in the New York Convention is generally construed narrowly, in recognition of the finality of arbitral awards, and instances of the exception being invoked

---

49 The United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards, New York, 1958, Article V(2)(a) and (b).

50 *Fincantieri Cantieri Navali Italiani SpA and OTO Melara Spa v. ATF* (25 November 1991), ICC Award No. 6719 (Interim Award) *Journal du droit international* (1994), 1071.

51 *Fincantieri-Cantieri Navali Italiani SpA and Oto Melara SpA v. M et* Tribunal arbitral (23 June 1992, 118 II 353).

52 *Fincantieri-Cantieri Navali Italiani SpA and Oto Melara SpA v. Ministry of Defence*, Armament and Supply Directorate of Iraq, Republic of Iraq (1996), XXI YBCA 594.

53 *Legal Department of the Ministry of Justice of the Republic of Iraq v. Fincantieri-Cantieri Navali Italiani* (15 June 2006) Rev Arb (2007) (Paris Court of Appeal, France), 87.

54 For example, the Paris Court of Appeal in *Sofregaz v. Natural Gas Storage Company* (Chamber 5-16, 3 June 2020, No. 19-07261) rejected an application to set aside an award rendered in favour of an Iranian company, holding that US sanctions did not form part of international public policy and therefore could not found a set-aside application.

successfully are rare. For example, as a matter of procedural public policy, a sanctioned party that is prevented from obtaining legal advice for the arbitration may resist enforcement on the grounds of a lack of due process.[55]

On a more practical level, the settlement or enforcement of an award, whether in favour of or against a sanctioned party, is likely to require an exemption or licence under the applicable sanctions regime to enable the sanctioned party to make or receive any payment or transfer.

Particular issues may arise where enforcement is sought in a country that has imposed its own counter-sanctions. For example, any attempt to enforce an arbitral award against a Russian sanctioned party's assets located in Russia is almost certain to fail as a result of the change to the Russian Arbitrazh Procedure Code introduced on 19 June 2022, which granted exclusive jurisdiction to the Russian courts over disputes involving Russian sanctioned parties, in effect enabling Russian parties to disregard arbitration clauses in their contracts.

55 See, generally, *Redfern and Hunter on International Arbitration*, 7th edition (Oxford University Press, 2022) [11.69]–[11.77] for an explanation of the grounds of due process, as provided under Article V(1)(b) of the New York Convention.

CHAPTER 18

Issues Arising for Financial Institutions and Regulated Entities

John Bedford, Andris Ivanovs and Navpreet Moonga[1]

Introduction

The critical role of financial institutions in intermediating and facilitating global commerce means that they are under an unabating spotlight, from governments and the public alike, concerning their implementation and administration of sanctions regimes. Due to the global and often complex nature of their business and the fact that they have touch points with so many transactions and other movements of assets, financial institutions bear the brunt of navigating multiform, and at times conflicting, sanctions regimes and often on a real-time basis. Further, the unprecedented nature, scale and evolution of sanctions enacted in response to the war in Ukraine stretched financial institutions' operational capabilities to their limits. This chapter considers some of the key practical issues for regulated financial institutions in managing sanctions risks and designing and implementing effective sanctions compliance programmes.

Compliance programme design and implementation

Financial institutions should seek to operate sanctions compliance programmes that incorporate guidance from key sanctions authorities, industry good practice and lessons learnt from publicly available records of historical enforcement actions. These programmes will include: written policies and procedures detailing internal rules and controls that are designed to prevent breaches of sanctions; mechanisms for escalating and reporting (internally and, as needed, externally) potentially

1 John Bedford is a partner, Andris Ivanovs is an associate and Navpreet Moonga is a special legal consultant at Dechert LLP.

restricted transactions or suspected breaches; mechanisms for horizon-scanning to monitor and identify new and emerging sanctions trends and developments; measures for auditing and testing the operational effectiveness of the compliance programme; and adequate record-keeping processes.

When designing or reviewing its compliance programme, the financial institution should ensure that its policies and procedures enable it to navigate all sanctions regimes that may potentially apply to its business. This means that the policies and procedures should enable the financial institution's staff members to identify when a relevant sanctions regime might apply to a particular transaction or activity (i.e., when there is a territorial 'nexus' requiring compliance with a particular sanction regime) and assess and, as appropriate, mitigate the potential sanctions risk prior to engaging in the transaction or activity. In practice, the policies and procedures will need to provide sufficient guidance to allow staff members to establish whether a particular sanctions regime may apply to a contemplated transaction or activity due to the citizenship, residence rights or location or domicile of any parties involved in the transaction, including the staff members themselves or whether a particular transaction or activity may be caught by extraterritorial sanctions measures, such as the US secondary sanctions.[2] An effective sanctions compliance programme should also incorporate regular training to ensure the policies and procedures are implemented and applied consistently across the organisation.

In designing its compliance programme, a multinational financial institution may also face the onerous challenge of reconciling inconsistent and potentially conflicting sanctions regimes into global policies and procedures that can be applied consistently throughout the institution. Although the conflict between Russia and Ukraine saw an unprecedented coordination of sanctions responses between the United States, the United Kingdom, the European Union and other allies, major differences remain within their sanctions regimes. Applying the strictest requirement (i.e., 'gold-plating'), even in circumstances where it may not apply as a matter of law, may be impractical and could expose the institution to increased regulatory and litigation risk. Therefore, the institution may choose, instead, to have higher-level global policies that are further implemented through more detailed country or regional policies and procedures for local operating

2 Under secondary sanctions, a non-US person faces the threat of US sanctions if they engage in a specified activity even where that activity has no US nexus.

business. At the same time, the institution should ensure that the local policies and procedures are not parochial and continue to enable an effective assessment of risks arising under all potentially applicable sanctions regimes.

The financial institution will also need to ensure that its programme is sufficiently flexible to help it navigate any blocking or counter-sanctions measures. For many years, financial institutions operating in the European Union and seeking to fully comply with US sanctions have had to navigate the Blocking Regulation, which counteracts certain extraterritorial US sanctions on Iran and Cuba.[3] Although EU Member State authorities have not actively enforced the Blocking Regulation, there have been cases of private parties whose rights have been affected by EU operators' compliance with US extraterritorial sanctions bringing successful damages claims against those operators to recover loss resulting from this compliance.[4] Moreover, institutions that operate in, or have exposure to, China or Russia may also need to consider whether their transactions or business activities in those countries may be affected by Chinese or Russian counter-sanctions.[5] These conflicts of law issues will invariably require a fact-specific analysis and balancing of competing risks, and financial institutions' policies and procedures should retain this flexibility.

Finally, financial institutions should consider how their sanctions compliance programme fits within their broader financial crime compliance programmes. Historically, in line with industry practice, large financial institutions would maintain separate sanctions compliance teams and anti-money laundering (AML) compliance teams (sitting within a wider financial crime compliance team) that generally would operate independently of each other. With key Russian oligarchs and politicians becoming subjects of asset freezing measures in the wake of the war in Ukraine, there has been an explosion in sanctions evasion and related money laundering typologies and a re-invigorated focus by government on the pursuit of

3 The Blocking Regulation prohibits EU persons from complying with certain US sanctions relating to Iran and Cuba. Council Regulation (EC) No. 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom, Article 5.

4 See, for example, Case C-124/20, *Bank Melli Iran v. Telekom Deutschland GmbH*.

5 For example, the Decision of the Board of Directors of the Bank of Russia of 1 April 2022 prohibiting companies from 'unfriendly states' from buying any non-rouble currency in Russia, and the Chinese Anti-Foreign Sanctions Law, which gives the Chinese government powers to place sanctions on individuals involved in the development, decision-making and implementation of discriminatory restrictive measures by foreign governments against China.

'corrupt elites' and their enablers.[6] Financial institutions may, therefore, consider whether a merger of sanctions and AML teams or other means for facilitating exchange of knowledge and expertise are needed to ensure a holistic assessment of financial crime and reputational risks emerging following the war in Ukraine. This is particularly the case in circumstances where effective AML controls ensure that financial institutions have good visibility on the operations of their customers and counterparties, which, in turn, assists with subsequent analyses of ownership or control for sanctions compliance purposes.

Risk assessment

Business risk assessment

A comprehensive business-wide risk assessment lies at the core of an effective and risk-based sanctions compliance programme and justifiable sanctions risk appetite. A financial institution should ensure that it refreshes its sanctions risk assessment on a regular basis (e.g., annually) as well as in response to external trends (e.g., the recent increase in virtual currencies and cryptoassets) and material regulatory developments. Changes to the institution's risk profile (from either internal or external developments) should result in new or updated controls to mitigate any identified risks. While the assessment underpins and rationalises a financial institution's general risk-based approach to sanctions compliance, the financial institution will need to ensure that it promptly implements, and complies with, any newly adopted sanctions measures such as new sanctions designations (which most institutions will do by ensuring that the data feeds they use for sanctions screening are updated and integrated on a real-time basis).

In designing and carrying out their business-wide risk assessments, financial institutions should have regard to relevant sanctions authority guidance. For example, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) has included in its Economic Sanctions Enforcement Guidelines a 'risk matrix' that financial institutions can use in evaluating their compliance programmes.[7]

Although there is no 'one-size-fits-all' framework, a financial institution should consider whether it operates in, or has exposure to, jurisdictions that are subject to sanctions or are hotspots for sanctions evasion activities, or whether it

6 Home Office, 'New plan puts UK at the forefront of fight against economic crime' (30 March 2023), www.gov.uk/government/news/new-plan-puts-uk-at-the-forefront-of-fight-against-economic-crime, accessed 11 May 2023.

7 31 C.F.R. Appendix A to Part 501, Annex.

provides products and services that inherently pose higher sanctions risks, such as trade finance, virtual currencies or cryptoassets, cross-border payments or correspondent banking. The institution should also assess the type of clients it services (domestic or international) and whether it interacts with its direct or indirect clients through intermediaries or agents. In this regard, the financial institution may want to pay particular attention to whether its clients are subject to the same sanctions regimes as the institution and consider the risk of its clients using the institution's services to engage in or facilitate business activities with sanctioned parties or countries.

The financial institution's risk assessment framework should also be updated to reflect the institution's compliance requirements under novel sanctions tools deployed by governments. For example, the US, UK, EU and their allies' measures to impose a cap on the price of seaborne Russian oil and petroleum products were unprecedented and continue to have significant ramifications for financial institutions, which are expected to assess their direct and indirect exposure to transactions in seaborne Russian oil and petroleum products and seek appropriate attestation from their clients or counterparties concerning the price of the traded oil and petroleum products. As appropriate, the risk assessment should consider existing and emerging risks posed by the financial institution's exposure to blocking or counter-sanctions measures.

Customer risk assessment

A financial institution should also have appropriate processes to enable assessment of whether its clients or counterparties are the targets of sanctions. In addition to customer screening (see below), the financial institution should have policies and procedures to enable it to assess whether a customer who is not listed on any sanctions lists may nonetheless be a target of sanctions by operation of applicable law. The financial institution should be mindful of the fact that the 'ownership and/or control' rules vary between the major sanctioning jurisdictions and their application can lead to, at times, inconsistent and counter-intuitive outcomes.

OFAC applies the 50 Percent Rule, meaning that a non-listed legal entity will be treated as sanctioned if one or more listed persons directly or indirectly own a 50 per cent or greater interest in the legal entity.[8] OFAC guidance does not require an institution to consider whether, regardless of the ownership position,

8 Office of Foreign Assets Control, 'Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property are Blocked' (13 August 2014), https://ofac.treasury.gov/media/6186/download?inline, accessed 11 May 2023.

the listed person exercises control over the non-listed entity. In theory, therefore, the financial institution can, in each case, arrive at a bright-line assessment of whether the non-listed legal entity must be treated as sanctioned as a matter of US law. This assumes that the institution has access to, or an understanding of, the relevant ownership structures, which are likely to have been identified or obtained via an effective AML compliance programme.

In contrast to the US position, the assessment can become a veritable Gordian Knot under the UK and EU regimes. Under both EU and UK sanctions regimes, a non-listed legal entity will be subject to sanctions restrictions if owned 50 per cent or more or 'controlled' by a person listed on the EU or UK sanctions list.[9] As per EU and UK guidance, the assessment of 'control' requires consideration of whether, notwithstanding the formal ownership of and management arrangement for the non-listed legal entity, the listed person has de facto or informal direct or indirect control over the non-listed legal entity. Conducting this assessment becomes fraught with danger where the listed person transferred formal ownership or control of an entity to their family members or business associates around the time of their listing, which is a common fact pattern in the context of the post-2022 Russia sanctions.[10]

As both the UK and EU authorities look to ramp up enforcement of their sanctions regimes, in particular with the UK's introduction of strict liability civil penalties for breaches of financial sanctions in June 2022, the stakes and potential consequences of getting the 'ownership and control' determination wrong continue to increase for financial institutions.[11] While the UK's Office of Financial Sanctions Implementation (OFSI) has indicated that it will treat a financial institution's reasonable and good faith (but incorrect) determination concerning ownership and control as a mitigating factor, it stopped short of confirming that

9 Office of Financial Sanctions Implementation (OFSI), 'UK Financial Sanctions: General guidance for financial sanctions under the Sanctions and Anti-Money Laundering Act 2018' (August 2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1144893/General_Guidance_-_UK_Financial_Sanctions__Aug_2022_.pdf, pp. 17–19, accessed 11 May 2023. See also European Commission, 'Commission opinion of 19.6.2020 on Article 2 of Council Regulation (EU) No. 269/2014' (19 June 2020), C(2020) 4117 final.

10 National Crime Agency, OFSI, Joint Money Laundering Intelligence Taskforce, National Economic Crime Centre, 'Financial Sanctions Evasion Typologies: Russian Elites and Enablers' (0697-NECC, July 2022).

11 Giles Thomson, 'New enforcement powers – a message from Giles Thomson, Director of OFSI' (8 June 2022), https://ofsi.blog.gov.uk/2022/06/08/new-enforcement-powers-a-message-from-giles-thomson-director-of-ofsi/, accessed 11 May 2023.

this determination would immunise the financial institution from enforcement.[12] Therefore, when conducting ownership and control assessments, the financial institution may have to continue to balance the regulatory (and potential enforcement) risk against the risk of litigation from a customer or counterparty that may reasonably believe that it is not a target of sanctions.

In addition, a financial institution's customer risk assessments should take account of the differences in the application of UK and EU ownership and control rules. While the EU guidance suggests that financial institutions must aggregate different listed persons' holdings in a non-listed legal entity for the purposes of assessing whether it is more than 50 per cent owned (or controlled) by listed persons, OFSI, in contrast, would not aggregate different listed persons' interests in a non-listed legal entity unless they hold their interests pursuant to a joint arrangement or one listed person controls the rights or interests of the other listed persons. Furthermore, from an EU perspective, where a non-listed legal entity is found to be owned or controlled by a listed person, the legal entity is only presumed to be subject to asset freezing measures. That presumption can be rebutted on a case-by-case basis by the legal entity concerned if it can be demonstrated that some or all of its assets are outside the control of the listed person or (as the case may be) that funds or economic resources made available to it would in fact not reach or benefit the listed person.[13]

In practice, these differences have led to an entity that is owned by the same UK and EU listed persons being treated as sanctioned for UK but not EU law purposes (or vice versa), as well as competent authorities in different EU Member States reaching diametrically opposite conclusions concerning the sanctions status of the same legal entity. This, in turn, makes it paramount that the financial institutions document their assessment of ownership and control matters and consider confirming those assessments with competent authorities where that is appropriate.

---

12 OFSI, 'OFSI enforcement and monetary penalties for breaches of financial sanctions' (March 2023), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1143219/March_2023_Monetary_Penalty_and_Enforcement_Guidance.pdf, paragraphs 3.22–3.31, accessed 11 May 2023.

13 European Commission, 'Commission Consolidated FAQs on the implementation of Council Regulation No. 833/2014 and Council Regulation No. 269/2014' (updated 10 May 2023), https://finance.ec.europa.eu/system/files/2023-05/faqs-sanctions-russia-consolidated_en.pdf, accessed 11 May 2023.

Internal controls

Sanctions screening controls

To mitigate the risk of dealing with sanctioned parties, most financial institutions will implement two main screening controls: customer screening and transaction screening. Customer screening is designed to identify relationships with sanctioned persons during onboarding or among the existing customer population, while transaction screening identifies whether transactions involve sanctioned persons or assets. While the financial institution will conduct transaction screening in real time, customer screening will take place on a periodic basis. A large and sophisticated financial institution will ordinarily have automated screening processes underpinned by detailed protocols for escalation and adjudication of potential matches.

In calibrating its screening processes, the financial institution will need to consider a number of important factors, including which sanctions lists it will screen, how 'fuzzy' to set the screening filters, which customer relationships or transactions to screen, and whether to screen against specific locations (e.g., cities or ports) within countries targeted with sanctions, such as jurisdictions subject to OFAC comprehensive sanctions. Financial institutions, particularly banks, may want to incorporate sanctions evasion typologies into their screening processes to the extent they are able to do so.

A financial institution will typically engage a vendor to supply it with relevant screening lists that are ingested by the financial institution's screening systems. In practice, there will be a delay between the enactment of new sanctions and the updating of internal screening filters. This period of delay may expose the financial institution to the risk of engaging in prohibited transactions, including dissipation of funds liable to freezing. As a result, the financial institution may want to consider additional measures to mitigate its sanctions risks during this period, including proactively identifying relationships with newly listed persons.

The vendor may also supply a package that includes data concerning entities believed to be owned by one or more listed persons. However, the vendor's assessment is likely to be based on publicly available information (which can be out of date) and, on its own, is unlikely to enable the financial institution to determine whether the non-listed entity may be controlled by one or more listed persons.

Moreover, financial institutions should consider reviewing the sanctions authorities' press releases and notices announcing new listings because they may contain important indications concerning entities that are potentially owned or controlled by listed persons. For example, when the UK government imposed asset freezing sanctions on Roman Abramovich on 10 March 2022, the associated statement of reasons explained that Abramovich 'exercises effective control

of' Evraz PLC.[14] However, Evraz PLC itself was not listed on the same day and, in fact, was only directly targeted on 5 May 2022. Similarly, when the UK government targeted Elvira Nabiullina, the Governor of the Central Bank of the Russian Federation, the associated press release stated that the 'UK Government does not consider that Elvira Nabiullina owns or controls the Central Bank'.[15]

Controls relating to activity-based sanctions

A financial institution, depending on its business, should consider instituting and maintaining appropriate risk-based systems and controls to counter the risk of violating activity-based sanctions. While the above-mentioned sanctions screening processes enable a financial institution to identify and mitigate the risk of the institution dealing with a sanctioned person (including a non-listed legal entity owned or controlled by a listed person), it is more challenging to implement an effective screening process for activity-based or trade sanctions. This is because activity-based sanctions may only restrict the provision of specific services or goods to, or undertaking specific dealings with, certain or all persons associated with a sanctioned country. In turn, this means that controls relating to activity-based sanctions can be more difficult to automate and are also reliant on having a sufficient understanding of a client or counterparty's business activities via the know-your-customer and customer due diligence process.

To successfully navigate these sanctions, a financial institution should, in the first instance, consider undertaking an assessment of its exposure to the risk of violating these sanctions. Once the financial institution has identified business areas that pose heightened exposure to activity-based sanctions, it can design and implement effective systems and controls to mitigate its risks. In this section, we consider some of the most impactful activity-based sanctions imposed following the commencement of the war in Ukraine and the potential risk mitigation measures.

Asset managers and other financial institutions that, on behalf of underlying clients, invest or trade in securities of issuers established in the European Union are likely to be aware of the EU prohibition on selling transferable

14 OFSI, 'Financial Sanctions Notice' (10 March 2022), https://webarchive.nationalarchives.gov.uk/ukgwa/20220310185330/https:/assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1059928/Notice_Russia_100322.pdf, accessed 11 May 2023.

15 Foreign, Commonwealth & Development Office (FCDO), 'Sanctions in response to Putin's illegal annexation of Ukrainian regions' (30 September 2022) , www.gov.uk/government/news/sanctions-in-response-to-putins-illegal-annexation-of-ukrainian-regions, accessed 11 May 2023.

securities denominated in any official currency of a Member State issued after 12 April 2022, or units in collective investment undertakings providing exposure to these securities, to any Russian or Belarusian nationals or residents, or legal entities incorporated in Russia or Belarus. In practice, financial institutions have sought to navigate these sanctions by undertaking enhanced due diligence on clients (fund investors) who have potential connections to Russia or Belarus and seeking appropriate contractual representations and warranties from financial institutions that introduce or distribute investments that they are not acting on behalf of the restricted Russian or Belarusian parties.

The US,[16] UK[17] and EU[18] bans on new investments relating to Russia have prompted financial institutions to increase scrutiny of the utilisation of any credit or equity financing that they might provide or arrange for non-Russian clients. To guard against the risk of funds being diverted to finance prohibited new investment activities in Russia, financial institutions may conduct enhanced due diligence on their clients' operations in, or exposure to, Russia and insist on more onerous covenants that prevent the direct or indirect use of the proceeds of any financing in Russia in breach of applicable sanctions.

Finally, financial institutions continue to grapple with their trade sanctions obligations. Across the US, UK, EU and other sanctions regimes, trade sanctions typically prohibit not only the actual trade in the restricted goods with the sanctioned country, but also the provision of financing relating to that trade. In the United Kingdom, these trade sanctions are particularly onerous for financial institutions because they prohibit the provision of any financial services relating to the prohibited trade, including payment processing and money transmission services.[19] This also applies under US sanctions rules. US persons could be subject to penalties if they 'facilitate' sanctions violations. OFAC has interpreted the prohibition on 'facilitation' broadly: there is a prohibition on arranging, assisting, supporting or approving non-US persons' dealings with sanctioned parties or countries, if those dealings would be unlawful if carried out by a US person.

16 Executive Order 14071.

17 The Russia (Sanctions) (EU Exit) Regulations 2019, Regulation 18B.

18 Council Regulation (EU) No. 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, Article 3a.

19 Export Control Joint Unit, FCDO, OFSI, 'Russia sanctions: guidance' (updated 24 April 2023), www.gov.uk/government/publications/russia-sanctions-guidance/russia-sanctions-guidance, accessed 11 May 2023.

To date, financial institutions have had limited operational ability to conduct effective and proportionate real-time screening of financial transactions to identify whether they relate to trade in restricted goods. Therefore, financial institutions have chosen to focus their resources on ensuring that these trade sanctions risks are adequately managed in high-risk business activities such as trade finance and other forms of working capital financing through detailed due diligence on clients, manual review and screening of underlying trade documentation, and re-screening of direct or indirect counterparties involved in the trade transaction at all key stages of the financing. Nevertheless, the explosion in the use of trade sanctions against Russia (particularly in the context of the oil price cap mechanism, discussed above), as well as increased focus on financial institutions' measures to counter proliferation financing,[20] may require financial institutions to rethink their general onboarding and AML transaction monitoring processes to help them identify clients that present an increased exposure to trade sanctions risks proactively and at an earlier stage.

Correspondent banking relationships

A financial institution providing correspondent banking services (i.e., an arrangement where a financial institution (correspondent) provides payment and other services to another financial institution (respondent)) presents heightened sanctions as well as other financial crime risks to the correspondent because the correspondent is unable to conduct due diligence on the respondent's clients whose transactions may be processed through the correspondent. The correspondent is in a position where it must rely on the respondent bank's financial crime systems and controls even where the respondent may be subject to a different and potentially weaker regulatory regime.

In this context, non-US financial institutions should be aware of the risks of undertaking cross-border US dollar payments or other transactions that touch on the US financial system. Historically, OFAC has aggressively asserted US jurisdiction over cross-border payments that clear through US correspondent banks, even when the underlying transaction is between non-US clients of non-US financial institutions. In a stark example of its aggressive enforcement approach, in 2019 OFAC entered into a settlement with a UK bank that had provided US dollar funding to certain Sudanese banks in violation of the US–Sudan sanctions programme. Although the UK bank's transactions with the Sudanese banks

20 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulations 18A and 19A.

did not use the US financial system, US financial institutions, which were several layers removed from the prohibited activity, were ultimately the source of the US dollar funding made available to the Sudanese banks. Aside from risks in the correspondent banking sphere, the case illustrates that non-US financial institutions, when considering any potential transactions involving US sanctioned parties or countries, should be thorough in their analysis and conclusion of any US nexus to those transactions.

Given that sanctions violations relating to correspondent banking services have led to record-breaking OFAC settlement figures in the past, it is perhaps unsurprising that financial institutions globally continue to focus on their sanctions risks and controls relating to correspondent banking services. Due to the elevated risks, correspondents typically implement a suite of controls to monitor: the respondent institution's transactions with a view to detecting any changes in the respondent institution's risk profile; any unusual activity or transaction on the part of the respondent; or any potential deviations from the agreed terms of the arrangements governing the correspondent relationship, including the respondent's adherence to the sanctions regimes applicable to the correspondent.[21] The monitoring techniques and tools will invariably depend on the risks associated with the correspondent banking relationship. Where the correspondent identifies concerns, it should investigate and follow up with the respondent institution by making requests for information on particular transactions or customers of the respondent bank.

Internal auditing and testing

Establishing internal auditing and testing processes ensures that the financial institution is aware of how well its sanctions compliance programme and sanctions screening processes are performing. Audits allow for an assessment of the effectiveness of internal structures to determine whether procedures need to be updated or recalibrated to account for weaknesses in existing compliance programmes, changes in the sanctions and adaptations in risk assessments.

21 Financial Action Task Force, 'Guidance on Correspondent Banking Services' (October 2016), p. 14, www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Correspondent-Banking-Services.pdf.coredownload.pdf, accessed 11 May 2023.

To measure the effectiveness of internal controls in this way, financial institutions should commit to ensuring that the senior management is held accountable for carrying out internal auditing and testing with sufficient authority, skill, expertise and resources. Furthermore, financial institutions should ensure that auditing and testing assessments are objective and relevant to their size and sophistication.

In conducting internal audits, should any actual or suspected breaches or deficiencies be found, financial institutions should take prompt action to conduct a robust investigation, analyse root causes of any breaches or deficiencies, and adequately remediate any issues in keeping with the relevant regulatory requirements and expectations. Financial institutions should also consider self-reporting the suspected or actual breaches to relevant authorities.

Reporting obligations and information sharing

Under the US, UK, EU and other sanctions regimes, financial institutions are obliged to report to the relevant sanctions authorities if they hold or control blocked funds or assets in which a sanctioned person has an interest or if they reject transactions prohibited by sanctions. Moreover, financial institutions may be required, or expected to, self-report actual or suspected violations of applicable sanctions. There are common features to reporting under the US, EU and UK sanctions regimes, although the timing and information requirements for reports may vary depending on the regime. In designing their internal processes for escalation of true matches or suspected breaches of sanctions, financial institutions should be mindful of these reporting obligations and expectations.

Under US law, if a financial institution's sanctions screening processes identify a true match, the financial institution, depending on the facts and the relevant sanctions programme, may be required to either block or reject the transaction and report this to OFAC.[22] Financial institutions are required to report to OFAC

22 There is a clear distinction between blocking and rejecting a transaction: to block a transaction, the financial institution must not process the transaction, and hold or freeze the funds; to reject the transaction, the financial institution will simply refuse to process the transaction. An example of a transaction that must be blocked is one in which the funds are designated for, or received from, a person or entity included on the Office of Foreign Assets Control's (OFAC) Specially Designated Nationals and Blocked Persons List (the SDN List). By contrast, a transaction that may have to be rejected does not include any parties on the SDN List, and thus there is no property interest that is subject to blocking. Financial institutions must reject transactions to avoid facilitating prohibited trade; for example, financial institutions must refuse to process a transaction with a North Korean company as, pursuant to OFAC's regulations concerning North Korea, all trade with North Korea is prohibited.

any blocked or rejected transactions within 10 days of the action.[23] In the event that a financial institution believes it has violated US sanctions laws and regulations, of which OFAC is unaware, proactive and voluntary disclosure of any potential violation can reduce potential penalties.

OFAC guidelines provide for voluntary self-disclosures (VSD), which are defined as a 'self-initiated notification to OFAC of an apparent violation by a Subject Person that has committed, or otherwise participated in, an apparent violation of a statute, Executive Order, or regulation administered or enforced by OFAC, prior to or at the same time that OFAC, or any other federal, state, or local government agency or official, discovers the apparent violation'.[24] VSD should be timely, include sufficient detail to explain the circumstances surrounding the apparent violation, address corrective actions taken, including the existence and effectiveness of existing compliance programmes, and offer full cooperation with OFAC. However, financial institutions must bear in mind that OFAC is required by memoranda of understanding entered into with a number of state regulators to share information concerning sanctions violations with those regulators. In situations where a financial institution is potentially facing both regulatory and criminal liability, it must also consider disclosing to the National Security Division of the US Department of Justice (DOJ) as well as OFAC, and in what order to do so. DOJ prosecutors are required to consider non-criminal alternatives in determining whether to initiate criminal enforcement actions, but non-disclosure may cause further problems and increased penalties if sanctions violations are later determined.

In contrast, under UK law, financial institutions (and some other regulated entities) are typically required to report to OFSI as soon as practicable if they have reasonable cause to suspect that their customer or counterparty is a sanctioned person (providing details of any frozen assets) or that any person has committed a breach of financial sanctions.[25] The UK regime, therefore, requires financial institutions to self-report their own suspected breaches of sanctions to OFSI, and, in

23 31 C.F.R. Part 501.

24 31 C.F.R. Appendix A to Part 501.

25 HM Treasury, 'Reporting information to OFSI – what to do' (16 December 2022), www.gov.uk/guidance/suspected-breach-of-financial-sanctions-what-to-do, accessed 11 May 2023.

practice, OFSI places considerable emphasis on timely reporting of breaches.[26] More generally, OFSI also requires all persons holding or controlling funds or economic resources belonging to sanctioned persons to submit annual frozen assets reports to it.

Should the Economic Crime and Corporate Transparency Bill be enacted by the UK Parliament, financial institutions and other regulated business will obtain the ability to voluntarily share customer information with each other for the purposes of preventing, investigating and detecting economic crime, without risking the breach of client confidentiality obligations. These provisions could facilitate, among other things, the UK financial institutions' sharing of intelligence to counter sanctions violations and circumvention.

EU sanctions regulations typically require any person (including a financial institution) to 'immediately supply' their competent authority with 'any information which would facilitate compliance' with EU sanctions, such as information concerning any frozen funds. In the context of the Russia sanctions regulations, the European Union has also clarified that these reporting obligations require reporting of suspected breaches of EU financial sanctions.[27] Similar to the United Kingdom, this obligation could be considered to require financial institutions to self-report their own breaches of sanctions.

Finally, when designing and executing sanctions reporting procedures, financial institutions should bear in mind that in certain cases they may be required to report suspected sanctions breaches, frozen assets or compliance programme weaknesses to their financial services regulator in addition to the sanctions enforcement authority[28] and there may also be other relevant reporting obligations (e.g., money laundering reporting obligations, such as suspicious activity reports). They should also consider whether and when they may be required to report issues to sanctions or financial services regulatory authorities in multiple jurisdictions. The new sanctions on Russia have heralded an unprecedented era of

---

26 OFSI, 'OFSI enforcement and monetary penalties for breaches of financial sanctions' (March 2023), paragraph 3.43, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1143219/March_2023_Monetary_Penalty_and_Enforcement_Guidance.pdf, accessed 11 May 2023.

27 Council Regulation (EU) No. 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, Article 8(1).

28 See, for example, Financial Conduct Authority, 'Financial sanctions' (updated 21 February 2023), www.fca.org.uk/firms/financial-crime/financial-sanctions, accessed 11 May 2023.

coordination between different countries.[29] Given the governments' intense focus on enforcing this regime and stamping out its circumvention, there is every reason to expect this coordination to translate into ever-closer cooperation on investigation and enforcement of sanctions breaches. Financial institutions should be aware that navigating and resolving sanctions issues may increasingly require a global approach and should prepare for this accordingly.

29 See, for example, OFSI, 'OFAC-OFSI Enhanced Partnership' (17 October 2022), https://ofsi.blog.gov.uk/2022/10/17/ofac-ofsi-enhanced-partnership/, accessed 11 May 2023.

CHAPTER 19

Sanctions and Export Controls Considerations for Higher Education and Research Institutions

Ama Adams, Emerson Siegle, Junsuk Lee and Brendan Hanifin[1]

Universities and research institutions are dedicated to the development of human understanding, which in the twenty-first century often involves cross-border collaborations, international travel and engagement with peers, faculty and students from around the world. While these activities are an indispensable aspect of academic progress, they can also come into conflict with the national security objectives underlying US sanctions and export controls that restrict the flow of sensitive commodities and technology to parties and jurisdictions of concern. In recognition of this tension, US sanctions and export control regulations incorporate various exceptions and exemptions for academic and research-related activities. However, these carve-outs are not absolute, and their application is heavily fact dependent. Further, universities have been the focus of recent legislative proposals at the federal and state levels that would impose additional restrictions and administrative requirements.

This chapter discusses key US sanctions and export control compliance considerations for higher education and research institutions, as well as select legislative proposals for further regulation of academic and research activities on a prospective basis.

---

1 Ama Adams and Brendan Hanifin are partners, Emerson Siegle is a counsel and Junsuk Lee is an associate at Ropes & Gray LLP.

Research

Research has long been a core function of higher education institutions in the United States. However, in the 1980s, policymakers grew concerned that countries in the Soviet Union were exploiting research relationships to obtain advanced technology and know-how.[2] A 1982 report prepared by the National Academy of Sciences observed that, while there had:

> *been a significant transfer of U.S. technology to the Soviet Union, the transfer . . . occurred through many routes with universities and open scientific communication of fundamental research being a minor contributor. Yet as the emerging government–university–industry partnership in research activities continues to grow, a more significant problem may well develop.*[3]

As such, the Reagan administration issued National Security Decision Directive (NSDD) 189, titled National Policy on the Transfer of Scientific, Technical and Engineering Information, which:

- defined 'fundamental research' as 'basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons';[4] and
- clarified 'the policy of [the Reagan] Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted'.[5]

The principle that 'fundamental research' should be freely conducted and shared for the betterment and education of society forms the framework for application of US export control laws to research activities.

---

2 'Science and Security in a Post 9/11 World: A Report Based on Regional Discussions Between the Science and Security Communities' (National Academies Press, 2007), www.ncbi.nlm.nih.gov/books/NBK11499/pdf/Bookshelf_NBK11499.pdf.

3 ibid.

4 National Security Decision Directive 189: 'National Policy on the Transfer of Scientific, Technical and Engineering Information' (21 September 1985), https://irp.fas.org/offdocs/nsdd/nsdd-189.htm.

5 ibid.

To this end, the principal US export control authorities each incorporate broad exceptions for the results of fundamental research.

- The Export Administration Regulations (EAR), administered by the Bureau of Industry and Security (BIS) within the US Department of Commerce, regulate the export of dual-use items, software and technology. The EAR exempt certain items from their scope, including information and software that '[a]rise during, or result from, fundamental research'.[6] In this context, fundamental research is defined as 'research in science, engineering, or mathematics, the results of which ordinarily are published and shared within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons'.[7]
- The International Traffic in Arms Regulations (ITAR), administered by the Directorate of Defense Trade Controls (DDTC) within the US Department of State, regulate the manufacture, export and brokering of defence articles and defence services. Like the EAR, the ITAR contain an exemption for 'public domain' information available to the public, including '[t]hrough fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community'. For purposes of the ITAR, '[f]undamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls'.[8]

The above exemptions reflect the policy goals of NSDD 189 and protect the ability of higher education and research institutions to engage in research activities that would ordinarily be restricted. For example, under the EAR, the transmission via email of controlled technical data to a foreign research collaborator would ordinarily be treated as an export subject to the EAR's jurisdiction, potentially requiring BIS authorisation depending on the export control classification of the technical data and the identity or location of the foreign collaborator. Similarly, the release of controlled technical data to a visiting professor, graduate student or other non-US national within the United States would be 'deemed' an export to

6 15 Code of Federal Regulations (C.F.R.) § 734.3(b)(3)(ii).

7 id., § 734.8(c).

8 22 C.F.R. § 120.34(a)(8).

the foreign national's home jurisdiction. By virtue of the fundamental research exemption, universities can undertake a significant range of activities that otherwise would be subject to export licensing requirements.

Importantly, however, the fundamental research exemption is subject to limitations. As such, universities must be cognisant of the limits of the fundamental research exemption in planning and executing their research activities.

First, the fundamental research exemption applies to research and information but not to commodities. As such, if collaboration with a foreign researcher would involve the export of material commodities (including equipment or chemicals), an export licence may be required from BIS or DDTC, even if the ultimate output of the research collaboration qualifies as fundamental research. To this point, BIS has advised that 'fundamental research only applies to technology', as defined under the EAR, and so the export of a controlled pathogen or another item in connection with research collaboration 'may require a license depending on the recipient university's country'.[9]

Second, for information to qualify as fundamental research, the institutions involved in the collaboration must not accept restrictions for proprietary or national security reasons. These restrictions may arise in different contexts, including: (1) restrictions on the publication of research findings; (2) access and dissemination restrictions contained in material transfer or licensing agreements; and (3) restrictions pursuant to federal government contracts or federal government-funded grants, which may flow down to institutions conducting research as subcontractor where a prime contractor has accepted research-related restrictions (whether or not known to a university at the time of contracting).

Third, the fundamental research exemption may not apply where an institution knows, or has reason to know, that a collaborator has violated (or intends to violate) US export control laws. For example, pursuant to General Prohibition Ten under the EAR, parties may not 'sell, transfer, export, reexport, finance, order, buy, remove, conceal, store, use, loan, dispose of, transport, forward or otherwise service, in whole or in part, any item subject to the EAR . . . with knowledge that a violation . . . is about to occur, or is intended to occur in connection with the item'.[10] In the university context, this may mean that certain collaborations

9 US Department of Commerce, Deemed Exports and Fundamental Research for Biological Items, www.bis.doc.gov/index.php/2011-09-08-19-43-48.

10 15 C.F.R. § 736.2(b)(10).

(e.g., arrangements where it is known that a research sponsor or licensee has violated, or will violate, the EAR) may be impermissible, notwithstanding the general availability of the fundamental research exemption.

Fourth, even when the fundamental research exemption is available, other trade regulations may impose collateral restrictions. For example, the economic sanctions programmes administered by the US Department of the Treasury's Office of Foreign Assets Control (OFAC) prohibit US persons – including US higher education and research institutions – from engaging in broad categories of activities with designated countries, regions, entities and individuals. In some cases, these sanctions programmes broadly restrict US persons from engaging in business or dealings with parties located in certain jurisdictions, even if the party has not been individually targeted with sanctions. For example, the Iranian Transactions and Sanctions Regulations (ITSR) broadly restrict US persons from engaging in transactions with persons ordinarily resident in Iran, regardless of whether the research in question is covered by the fundamental research exemption. While OFAC has published various general licences authorising certain academic and research-related activities, application of these licences is fact specific. The relevant general licence under the ITSR, for example, authorises US undergraduate institutions to hire faculty or educate students that are ordinarily resident in Iran, but the general licence applies only to: (1) certain fields of study (e.g., social sciences, law, business and the humanities); and (2) undergraduate, rather than graduate, studies.[11]

Comprehensive, country-based sanctions programmes – targeting, at the time of writing, Crimea, Cuba, the so-called 'Donetsk People's Republic' and 'Luhansk People's Republic' regions of Ukraine, Iran, North Korea and Syria (hereinafter, embargoed countries) – can present particular challenges in the context of online higher education activities. US persons are generally prohibited from providing services, including in-person or virtual online teaching services, to persons located or ordinarily resident in embargoed countries. Covid-19, which gravely affected cross-border travel, exacerbated the impact of these prohibitions and affected the educational experiences of students ordinarily resident in embargoed countries, who could not travel to the United States, even with the appropriate visa, to take advantage of relevant authorisations. OFAC has responded by publishing limited carve-outs to authorise certain online education. For example, for students located or ordinarily resident in Iran, accredited US universities are authorised to provide online courses, limited to certain fields of study (see above) or certain introductory

11 31 C.F.R. § 560.544.

courses (e.g., in science, technology, engineering or mathematics), for the completion of undergraduate degree programmes.[12] OFAC has also authorised (although only until 1 September 2023) activities related to the completion of graduate degree programmes in social sciences, law, business or the humanities for Iranian students who have been granted certain non-immigrant visas (e.g., F (students) or M (non-academic students) but who are not physically present in the United States due to the covid-19 pandemic).[13] OFAC has also authorised exports of certain video conferencing software and related services, as well as educational technology software and related services, if they relate to authorised courses of study and if specified, additional criteria are met.[14]

While in some circumstances, US sanctions restrictions can trump applicability of the fundamental research exemption, existing OFAC authorisations can help to close the gap. For example, transactions related to certain information or informational materials are generally exempted across sanctions programmes. Under Section 1702(b)(3) of the International Emergency Economic Powers Act, the foundational legal authority for most OFAC sanctions programmes, 'the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials' is not prohibited.[15] Examples of information or informational materials include 'publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds'.[16] Importantly, this exception may include published fundamental research findings. However, OFAC has also clarified that this exemption does not apply to materials 'not fully created and in existence at the date of the transactions',[17] and that the 'provision of services to market, produce or co-produce, create, or assist in the creation of information or informational materials' is not authorised.[18] Therefore, US persons' participation in the process of conducting fundamental research, as opposed to distributing already concluded fundamental research, may trigger sanctions concerns when sanctioned parties or parties resident in embargoed countries are involved.

12 Office of Foreign Assets Control (OFAC), General License G.
13 OFAC, General License M-2.
14 See 15 C.F.R. § 560.540; OFAC, General License D-2; OFAC, FAQ #853, https://ofac.treasury.gov/faqs/853.
15 50 U.S.C. § 1702(b)(3).
16 ibid.
17 See, e.g., 31 C.F.R. § 560.210(c)(2).
18 ibid.

While US sanctions therefore impose certain restrictions on research collaborations, they are not the only source of collateral restrictions. In addition, foreign research collaborations, particularly those involving parties in jurisdictions perceived as unfriendly to the United States (e.g., China, Russia), have been the subject of increased scrutiny at both the state and federal levels. For example, in 2022, the state of Louisiana enacted the Higher Education Foreign Security Act of 2022 (the Louisiana Act), which imposed new policy requirements on Louisiana 'postsecondary education institutions'. Among other requirements, the Louisiana Act requires covered institutions to implement screening policies and procedures for individuals seeking employment in research positions, which require universities to: (1) conduct due diligence to assess whether job applicants have connections to China or other countries of concern; (2) obtain additional documentation and information from applicants with these connections; and (3) potentially submit information discovered through the diligence process to law enforcement authorities. As concerns regarding technology transfer and geopolitical competition continue to attract political attention, it is foreseeable that universities may be subject to increasing regulation on both the federal and state levels, which may further complicate their traditional reliance on the fundamental research exclusion to enjoy open and free collaboration with partners worldwide.

Travel-related transactions

While international travel, including to most embargoed countries, is permitted, US export controls and sanctions may restrict the items that can be transported across international borders in support of research activities or the types of activities that can be engaged in by US persons in foreign jurisdictions.

For example, researchers carrying equipment, biological materials, laptops with technical data or other items controlled under the EAR or the ITAR must comply with export licensing requirements, which can apply in the same manner to hand-carried and shipped items and equipment. Certain existing licence exceptions authorise the hand-carrying of laptops, tools and other goods. For example, under the EAR, the BAG licence exception authorises the unlicensed hand-carrying under certain circumstances of, inter alia, 'tools of the trade', defined as '[u]sual and reasonable kinds and quantities of tools, instruments, or equipment and their containers and also technology for use in the trade, occupation, employment, vocation, or hobby of the traveler or members of the household who are

traveling or moving'.[19] However, researchers can nevertheless run afoul of export restrictions if they presume that a licence exception applies, particularly when carrying sensitive technology in hand luggage.

In addition, if researchers travel to an embargoed country, there may be further restrictions on either the travel (in the case of Cuba) or activities that may be conducted upon arrival.

Cuba is subject to a congressionally mandated embargo and only certain categories of travel-related transactions are authorised. For example, under the Cuban Assets Control Regulations, travel-related transactions are authorised only if they relate to a specified set of activities, including certain educational trips.[20] Educational activities that are compliant include:

- participation in structured exchange programmes under the auspices of a US academic institution;
- non-commercial academic research or teaching at a non-Cuban research institution;
- certain educational exchange programmes; and
- work by private foundations or research institutes with an 'established interest in international relations to collect information related to Cuba for noncommercial purposes'.[21]

In addition, limited travel-related transactions are authorised for professional research or meetings, including conferences, in Cuba. Trips to Cuba related to professional research or meetings must meet two minimum requirements: (1) the purpose of the research or meetings must directly relate to the traveller's profession, professional background or area of expertise; and (2) the travel schedule may not include free time or recreation in excess of that consistent with a full-time schedule of professional research or attendance at, or organisation of, professional meetings.[22] For each category of authorised travel to Cuba (including travel related to education and research), US sanctions requirements are specifically tailored and must be carefully observed.

For other jurisdictions, although travel itself is not restricted, only certain categories of activities are permitted. For example, travelling to Iran for professional research or conferences that benefit persons resident in Iran is generally

19 15 C.F.R. § 740.14(b)(4).

20 31 C.F.R. §§ 515.560(a)(5), (10).

21 See id., §§ 515.565, 515.576.

22 id., § 515.564(a).

prohibited, with limited availability for specific licences that can be reviewed on a case-by-case basis. Under the ITSR, a specific licence may be issued for US persons' participation in projects in or related to Iran, including conferences and training, to support human rights, democratic freedoms and democratic institutions, or to help meet basic human needs.[23] In addition, certain transactions involving a person resident in Iran (excluding the Iranian government or Iranian financial institutions, among others) related to participation in or US person sponsorship of a public conference or similar event are allowed, if the event takes place in the United States or in a third country other than the United States or Iran.[24] In each case, specific conditions must be met for authorisation. As a general rule, if academic conferences or other events require travel to an embargoed country, or dealings with parties ordinarily resident in an embargoed country, restrictions may apply, and compliance with existing general authorisations requires careful review and attention.

Most major universities have adopted formal export compliance policies and procedures to manage these and other circumstances, and it is incumbent on both institutions and their employees to ensure compliance with the requirements. As a matter of risk mitigation, some universities encourage researchers to travel with clean or loaner devices to avoid the inadvertent export of controlled data (or release of other personal information, as some jurisdictions – including China – purportedly may access information upon a traveller's entry).

Investment activity

Many US universities have significant investment portfolios, including as limited partners in third-party-managed investment funds, which are generally subject to the same US restrictions as for other US institutional investors and asset managers.

Among the relevant restrictions, US universities are not permitted to invest, directly or indirectly, in entities designated to OFAC's Specially Designated Nationals and Blocked Persons (SDN) List, or entities that – per OFAC's 50 Percent Rule – are owned, 50 per cent or more (whether directly or indirectly, and not accounting for share dilution) by one or more SDNs. In recent years, OFAC has promulgated novel, investment-focused sanctions programmes, including in respect of China, Russia and Venezuela. For example, the Chinese Military Companies Sanctions prohibit US persons – including universities – from engaging in 'the purchase or sale of any publicly traded securities, or any publicly

23 id., § 560.545(a)(1).

24 id., §§ 560.544(a)(5), 560.554(a)–(b).

traded securities that are derivative of such securities, of any person' designated to the Non-SDN Chinese Military-Industrial Complex Companies (NS-CMIC) List. US persons are prohibited from acquiring new securities of designated parties within 60 days of designation to the NS-CMIC List. In addition, US persons have 365 days after designation to divest of targeted NS-CMIC securities (after which point, a specific licence would be required, although divestment is not a regulatory requirement). Notably, OFAC has advised that US persons are prohibited 'from investing in U.S. or foreign funds, such as exchange-traded funds . . . or other mutual funds' that hold securities of a party on the NS-CMIC List.[25]

Many US universities have developed template sanctions compliance provisions to manage investment-related sanctions risk, particularly when investing via non-US-managed funds whose compliance obligations may deviate from – or even conflict with – US sanctions requirements. However, these side letter protections are commonly subject to negotiation, and even unqualified undertakings by third-party fund managers may not present a complete defence if a manager were to implicate a US university or other research institution in a violation of US sanctions (which are subject to strict liability for civil violations). Further, non-US fund managers are increasingly proposing novel, untested ring-fencing strategies to accommodate US investors' regulatory concerns without imposing equivalent restrictions on non-US investors or risking violation of local anti-sanctions regulations. Particularly as US and Chinese sanctions and other investment restrictions (and countermeasures) continue to proliferate, US universities increasingly may be faced with difficult, conflict-of-laws scenarios, for which there may not be an opportunity to secure unqualified contractual protections.

In addition to OFAC sanctions lists, there are a host of other restricted party lists that impose restrictions on counterparties (including restrictions on exporting items subject to the EAR to a given party), including the Entity List, the Unverified List and the Military End User (MEU) List (all administered by BIS), and the Covered List administered by the Federal Communications Commission, which identifies developers of communications equipment and services that are deemed to present an unacceptable national security threat. Because these restricted party lists do not impose investment-related restrictions, many universities do not prohibit their managers from investing in listed companies (as they are not prohibited by US law from doing so), although these

25 OFAC, FAQ #861, https://ofac.treasury.gov/faqs/861.

investments can carry a degree of reputational risk and be captured by third-party (e.g., banking partner) compliance certification requests that exceed the scope of applicable US restrictions.

Further complicating investment strategies, universities have been the subject of numerous congressional proposals to prohibit investments in: (1) parties designated to restricted party lists, even if the restrictions attendant to the designation generally do not prohibit investment activity; or (2) Chinese companies writ large. While many of these proposals appear relatively unlikely to be enacted under the current administration, they are representative of increased, bipartisan scrutiny of US universities' international investments and financial entanglements. Examples of recent legislative proposals include:

- the Protecting Endowments from Our Adversaries Act (PEOAA). The PEOAA would apply to private colleges and university endowments valued at over US$1 billion and would impose: (1) a 50 per cent excise tax on an initial investment in a party on the Entity List, the MEU List, the Unverified List or the Covered List; and (2) a 100 per cent excise tax on the realised gains of these investments; and
- the Dump Investments in Troublesome Communist Holdings (DITCH) Act. The DITCH Act would deny organisations tax exemptions if they hold an interest in a 'disqualified Chinese company', defined to include any corporation incorporated in China or for which 10 per cent or more of the stock is held by Chinese governmental entities, Chinese corporations or Chinese individuals.

As the US government expands its arsenal of tools to combat perceived national security threats such as the rise of China, and Russia's invasion of Ukraine, higher education and research institutions may find that their investment activity will prove as complicated to administer in a compliant manner as their general trade compliance policies and procedures, particularly to the extent that they continue to rely upon third parties to facilitate this activity.

Compliance considerations and conclusion

As compared to private sector businesses, US universities have access to more exemptions and exclusions to the application of US export control and sanctions laws. However, these exemptions are not absolute, and universities and research institutions must ensure compliance with US national security laws and regulations, even when those restrictions appear in conflict with the traditional ideological tenets of academia. Further, as new laws and legislative proposals

demonstrate, universities and research institutions are increasingly under scrutiny by lawmakers, whether motivated by genuine concerns about US adversaries' exploitation of research activities for technological gain or pure political expediency.

In the current environment, US universities and research institutions should ensure that they have in place policies and procedures that govern, inter alia, tone from the top, delegation of authority, deemed export compliance (and associated technology control plans), guidance for researchers and administrators regarding the scope of fundamental research (and exceptions to that exclusion), investment activity and standard trade compliance functions, such as restricted party screening, export classification and licensing, and record-keeping. While higher education and research institutions have not traditionally been a focus of enforcement activity, the proliferation of complex trade laws and regulations that apply to universities is growing, and universities would be well served to ensure that they and their employees have a sufficient understanding and appreciation for the delicate interplay between these restrictions and academic activities.

CHAPTER 20

Impacts of Sanctions and Export Controls on Supply Chains

Alex J Brackett, J Patrick Rowan, Jason H Cowley, Laura C Marshall, Edwin O Childs, Jr and Elissa N Baur[1]

Overview

Today's globalised, on-demand supply chains rely on increasingly seamless cross-border movement of raw materials and goods in order to be cost efficient and effective. Sanctions and export controls present potential impediments that, if not managed properly, can imperil a company's performance, whether as an original or intermediate supplier, or as the final recipient of supplied goods or technology. In some cases, governments may impose new sanctions or export controls with little or no warning, with similarly swift knock-on effects cascading through impacted supply chains. However, this tends to be the exception rather than the rule; a business that is watching carefully will generally spot the storm clouds on the horizon. A well-designed, risk-based compliance programme tailored to a company's specific circumstances, including the risk profiles of its suppliers, intermediaries and customers, will help with this forecasting, allowing a company to identify and address even the most challenging sanction and export control developments.

---

1 Alex J Brackett, J Patrick Rowan, Jason H Cowley, Laura C Marshall and Edwin O Childs, Jr are partners, and Elissa N Baur is an associate, at McGuireWoods LLP. The authors wish to thank associates Abigail G Urquhart and Alex J Scandroli for their contributions to this chapter.

Effective development of compliance strategies starts with understanding the basis for sanctions and export controls, how they overlap and interact, and how to mitigate their related risks. It is also critical to understand how sanctions and export controls have evolved in recent years, and how still-developing trends could impact their trajectory in the near term and over the long term.

Rapidly evolving enforcement environment

By any measure, the use of sanctions and export controls reached critical mass following Russia's 2022 invasion of Ukraine. In its wake, governments implemented sweeping multilateral policies designed to severely restrict Russia's influence on the world stage and immobilise its war efforts. As an example of how this was achieved in a global economy, US regulators promoted policies aimed at achieving international implementation and enforcement. The result was a previously unthinkable united front in cross-agency, multinational collaboration, leading to the most robust sanctions and exports controls regime ever imposed on the modern supply chain. The depth of international cooperation achieved in responding to the invasion of Ukraine sets a strong precedent for nations increasingly turning to sanctions and export controls to address foreign conflicts and crises. For example, the recent efforts by like-minded countries to withhold advanced technology from China is emblematic of this new approach to trade policy, under which national security interests rather than traditional market forces appear to be the predominant guiding principles.

In the third edition of the *Guide to Sanctions*, this chapter outlined the distinctions and similarities between sanctions and exports controls, with an emphasis on the key strategies companies should consider when developing internal compliance protocols. Against the Russia–Ukraine backdrop, the distinctions between the two policy instruments are becoming less clear, as US regulators expand the scope of trade restrictions while broadening enforcement efforts within the sanctions and export control space. In this edition, the chapter includes analysis of the post-invasion regulatory landscape and its impact on supply chains, with a particular eye towards new rules governing trade with China and restricting transactions for advanced technologies.

Sanctions and export control overview

Perhaps the key economic takeaway from the global response to Russia's invasion and recent actions towards China is that sanctions and export controls reflect foreign policy. For example, in the post-Cold War era, the trend towards a global free market economy was directly correlated with the relatively low level of disruptive conflict that reduced the barriers to international trading. This model,

however, assumes that nations will contribute to the global economy by aspiring to be good-faith state actors. By contrast, Russia's decision to invade Ukraine, coupled with China's deteriorating trade relations with multiple jurisdictions, has forced an inverse trend. Now, businesses are looking to shore up local and regional trade relationships to prepare for future disruptions to the supply chain as the geopolitical landscape signals the potential for further deterioration. The upshot of this interplay with foreign policy is that companies can often prognosticate the consequences that new or upcoming sanctions and export controls may have on supply chains by paying careful attention to the trends within the targeted activities and types of product.

In the case of sanctions, they are imposed by one country or multilateral organisation against an individual, entity, sector, government or country to respond to, or deter, some course of conduct. Typically, they are designed to isolate and pressure their target via some combination of financial and trade restrictions (e.g., preventing the sanctions target from having access to certain financial markets, goods or technologies). In some cases, they are narrowly tailored, such as by targeting a single individual or entity, while in others they are widespread, up to and including imposition of country- or territory-wide embargoes. In many cases, including under US law, sanctions operate on strict liability principles (i.e., if you engage in a prohibited transaction with a sanctions target, you have violated the law regardless of your knowledge or intent). However, whether an enforcement action is pursued, and whether and what penalties may be imposed, will hinge heavily on intent. For example, the United States' primary sanctions enforcer, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) has developed enforcement guidelines[2] that turn primarily on the question of whether a violation was 'egregious' or 'non-egregious'. Key factors in that determination include whether the violation occurred due to wilful or reckless conduct, and whether supervisory or management-level personnel had actual knowledge of, reason to know of, or involvement in, the conduct at issue. Other factors include the size and sophistication of the implicated company, the existence, nature and adequacy of its compliance programme, and its remedial response to the apparent violation.

Export controls, on the other hand, generally reflect foreign policy not via an outward-facing targeting of specific individuals, entities or jurisdictions, but rather via an inward-facing defensive motive to identify and limit the export of particularly critical goods and technologies on an individual or multilateral basis. That

2 These guidelines are located at 31 Code of Federal Regulations (C.F.R.) Part 501, Appendix A.

being said, export controls can have many of the same characteristics as sanctions, have always had a level of interplay with sanctions, and have become increasingly intertwined with sanctions in recent years. Although the leading sanctions and export control regimes (i.e., those of the US, UK, EU and the United Nations) often differ in the specific targets of their restrictions, they all tend to have significant overlap in the types of conduct for which they impose sanctions and the types of technologies over which they impose export controls. From a sanctions perspective, terrorist activity, destabilising military or political activity, drug trafficking and human rights abuses predominate. Whether a particular individual, entity or regime will be targeted by a particular sanctions enforcer tends to turn on complicated questions of internal politics, geopolitics and geography.

From an export perspective, the rule is typically that military technology is subject to the most stringent restrictions (e.g., in the United States, most military technology must be licensed for export by the State Department's Directorate of Defense Trade Controls under the International Traffic in Arms Regulations, with limited exceptions), and everything else is typically subject to few restrictions on export unless the item falls into a particularly sensitive category (e.g., nuclear, biological or chemical processing technology). Whether a particular technology will be subject to export controls turns on a balancing of the sensitivity of the technology (particularly if it can be used in problematic ways), a protectionist desire to limit distribution of the technology, and a counterbalancing desire to avoid limiting innovation by artificially restricting access to markets and talents by being overly protectionist.

Targeted supply chains

Sanctions and export controls impacting western supply chains are not a new development. As a prime example, for over 10 years world powers have imposed severe economic sanctions on North Korea. While the primary impetus behind these sanctions has been to pressure North Korea to denuclearise, some of the most robust sanctions regimes against the Kim regime also target its use of forced labour and have specifically sought to limit the flow of commercial goods to or from North Korea.[3] Among other things, OFAC regulations currently prohibit the importation into the United States of any goods made in North Korea or by its Worker's Party or other state agencies. Separately, since the passage of the

3 This concern was highlighted in some detail in a 23 July 2018 Advisory by the US Departments of the Treasury, State and Homeland Security entitled 'Risks for Businesses with Supply Chain Links to North Korea'.

Countering America's Adversaries Through Sanctions Act in 2017,[4] 'any significant goods, wares, articles, and merchandise mined, produced, or manufactured wholly or in part by the labour of North Korean nationals or citizens' have been prohibited from entry into the United States unless US Customs and Border Protection (CBP) 'finds through clear and convincing evidence that the merchandise was not produced with a form of prohibited labour'. Because the North Korean government is known to send its citizens abroad to work under government contracts, including in China and Russia, the risk that North Korean forced labour has been exploited to produce raw materials or manufactured goods exists even when the materials or goods come from a country other than North Korea. As a result, businesses in the United States are obligated to assess the risk that their global supply chain may be tainted by North Korean labour.[5]

More recently, similar concerns regarding forced labour and other human rights violations by China's government against the Uyghur populations in the Xinjiang region of north-western China have been at the forefront, as discussed further below.

Semiconductors and advanced technologies

We are now seeing export controls evolve to restrict the flow of sophisticated technologies deemed critical to the IT arms race in markets such as China, in a manner that swims against the current of recent cross-border supply chain evolution. For decades, the semiconductor and advanced computing industry built transnational supply lines predicated on unrestrained cross-border logistics. As modern export controls have evolved to become more restrictive, and, increasingly, the preferred policy instrument to further US national security interests, the technology sector faces unprecedented vulnerabilities. A prime example is the technological competitiveness legislation passed during the Trump administration with the Export Control Reform Act of 2018 (ECRA), and recently during the Biden administration with the CHIPS and Science Act of 2022. In particular, passage of ECRA represented a sea change in US free trade philosophy. ECRA delegated expansive authority to the Bureau of Industry and Security (BIS) to

4 Countering America's Adversaries Through Sanctions Act, 22 U.S. Code § 9241a.

5 See, e.g., US Customs Ruling HQ H317249 (5 March 2021) (finding that the company did not have the clear and convincing evidence needed to overcome a presumption that imported goods were made using North Korean forced labour when manufactured at a specific Chinese company).

establish export controls on emerging and foundational technologies designed to prevent the modernisation of military adversaries and incentivise domestic manufacturing.

After years of escalating trade rhetoric, pursuant to its new legislative grant, BIS promulgated a series of rules in 2022 aimed at limiting China's ability to develop and produce advanced semiconductors, semiconductor production equipment and advanced supercomputers.[6] The rules set thresholds for high-end model software chips, requiring an export licence from BIS before transacting with Chinese entities. Notwithstanding the thresholds, BIS announced that all licence applications to export software chips to China face a presumption of denial, functioning as a de facto embargo on computing technology bound for China. To effectuate the rules, BIS expanded the scope of the Export Administration Regulations (EAR),[7] which is the control regulation for commercial and dual-use goods. Previously, the EAR applied to goods exported from the United States, goods produced in the United States and foreign-produced goods made with controlled US-manufactured components.

The new EAR China-related export controls also apply to goods produced wholly outside the United States that are the direct product of certain US technologies or that are produced from equipment that is the direct product of certain US technologies. This extraterritorial component functions by broadening the Foreign Direct Product Rule, which was previously used to prohibit products from being shipped directly or indirectly to affiliates of Huawei and ZTE, to include scores of Chinese technology and military conglomerates already designated on the BIS Entity List.[8] The revised controls further apply to restrict US persons from providing support for the development or production of covered technologies in applicable locations or in connection with covered end users or end uses, without a licence.

---

6 87 Federal Register 62186; 15 C.F.R. Part 734 et seq.

7 15 C.F.R. Part 730 et seq.

8 The Entity List, which is maintained by the Bureau of Industry and Security (BIS) within the US Department of Commerce, is a list of individuals and entities (including businesses, research institutions, government and private organisations, individuals and other types of legal persons) whose privilege to receive US exports has been limited or prohibited due to some form of misconduct or national security concern. Those placed on the Entity List, found in Supplement No. 4 to Part 744 of the Export Administration Regulations (EAR), are subject to specific licence requirements for the export, re-export or transfer (in-country) of specified items, supplemental to those found elsewhere in the EAR. The BIS Entity List imposes licence requirements before an individual or entity may transact with a restricted party.

In hopes of minimising the impact on allies, the United States granted entities in Taiwan and South Korea, where some of the most advanced computer circuitry to date is manufactured, one-year waivers to continue production at China-based facilities. For example, Taiwanese semiconductor manufacturers were authorised to import restricted components into plants in Nanjing to continue production without subjecting exporters to the new restrictions. However, one year provides insufficient time to stave off the long-term challenges for exporters that may be unable to scale trading commensurate to pre-restriction demands, as Asian markets will inevitably turn to non-US trade partners to source component parts. This reflects the potential risk in imposing unilateral export control regimes. Without multilateral cooperation from other international markets, certain US industries could be rendered uncompetitive, specifically those that rely heavily on trade with Asian markets.

To be certain, a declining domestic semiconductor sector will have collateral consequences across US industry, manufacturing and production, at a time when inflation costs are already soaring due to supply chain disruptions. As a tacit acknowledgement of these risks, the Biden administration has engaged in ad hoc negotiations with foreign counterparts and heavily subsidised domestic technology markets, with some degree of success. In January 2023, two leading superconductor markets, Japan and the Netherlands, announced multilateral export control packages that operate in tandem with the US restrictions. Further, stateside investment has yet to slow as US companies and foreign-based interests race to build ultramodern, multibillion-dollar plants in Arizona, Texas and Ohio.

Meanwhile, the Chinese government has not stood idly by. Beijing announced plans for its own 'Unreliable Entity List' in response to the expanded US Entity List. In 2023, China's Ministry of Commerce imposed export and investment controls on two major US defence contractors for supplying arms to Taiwan, barring Chinese entities from transacting with them and prohibiting their investments into China. For companies caught in this political crossfire, these retaliative escalations complicate their cross-border operations and could permanently disrupt their global supply chains.

While the net result remains to be seen, targeted technology sectors will suffer challenges from the volatility in the coming years as nationalistic attitudes prevail. To mitigate this, companies in this space must begin planning for worst-case scenarios and develop continuity plans that contemplate relocation of their supply ecosystem away from China.

Targeted conduct

Human rights abuses

As mentioned above, sanctions are regularly deployed against human rights violations and abuses. Outside the Russia–Ukraine context, recent sanctions have focused predominantly on human rights violations and forced labour campaigns by China's government against the Uyghur Muslim populations in the Xinjiang region. In July 2020, the US departments of State, the Treasury, Commerce and Homeland Security issued an advisory alerting businesses to supply chain risks from links to entities exploiting forced labour and other human rights abuses in Xinjiang. Those government departments, joined by the US Trade Representative and the US Department of Labor, updated and reissued that guidance in July 2021. The US Department of Commerce also restricted exports to several Chinese companies and government ministries by placing them on its Entity List.

In parallel, in July 2020, OFAC imposed sanctions on the Xinjiang Production and Construction Corps (XPCC), a paramilitary organisation that has been identified as building and running re-education camps holding Uyghur and other Muslim minorities in Xinjiang. According to news reports, the XPCC was responsible for up to one-third of China's cotton production, which translates to up to 7 per cent of the world's cotton. Under the sanctions, US companies may not buy from or sell to the XPCC or subsidiaries in which it has a majority stake. To complement OFAC's actions, CBP issued a series of withhold release orders (WROs)[9] against cotton and other products from Xinjiang based on information that reasonably indicates the use of forced labour in their production. The first several WROs targeted products made by specific entities in Xinjiang, including the XPCC and several other entities involved in the operation of 're-education camps', cotton processing and the production of electronics, textiles and hair products. The most recent WRO, dated 23 June 2021, cited information that reasonably indicated that a major Chinese manufacturer uses forced labour to manufacture silica-based products. China, and in particular the Xinjiang region, is the world's largest producer of products containing silica, a critical raw material for the manufacture of cement, brick and glass. The WRO stood to have an immediate impact on the production of solar cells and to implicate the production of many downstream chemicals to which silica is a requisite component.

9 These withhold release orders were authorised under Section 307 of the Tariff Act of 1930, which prohibits the importation of merchandise mined, produced or manufactured in any foreign country by convict labour or forced or indentured labour, including forced child labour.

In June 2022, Congress enacted the Uyghur Forced Labor Prevention Act (UFLPA)[10] on a broadly bipartisan basis, which, among other things, created a rebuttable presumption that all goods manufactured in whole or in part in the Xinjiang Uyghur Autonomous Region are the product of forced labour and are not entitled to entry at US ports. The UFLPA significantly enhanced CBP's authority in this space and largely superseded the Xinjiang-related WROs by requiring detention, exclusion or seizure of defined goods originating in China that are presumed to have involved forced labour in their production. For the commodities subject to the UFLPA or a WRO, CBP will prevent the admission into the United States of all merchandise within scope and can detain, exclude or seize merchandise that is present in the United States but has not yet cleared customs. The overlapping Xinjiang sanctions and export controls have forced companies and industries doing business in key sectors of the Chinese economy to revisit whether and how they screen their Chinese supply chains.

Leveraging a fuller spectrum of trade restrictions

As the foregoing illustrates, the United States and like-minded governments and their adversaries have all been deploying an increasingly wide array of trade restriction tools in furtherance of their diplomatic prerogatives – and with direct impacts on global supply chains. For example, WROs have been an increasingly popular tool since 2016, when the Tariff Act of 1930 was amended to eliminate a statutory exemption and to give CBP more enforcement power.[11] The Xinjiang region has not been the only target of WROs, and the use of WROs is expected to continue, if not expand, during the Biden administration.

Further, in 2019, the US Department of Commerce issued regulations enabling it to block any information communications technology and service (ICTS) transaction involving goods or services designed, developed, manufactured or supplied from foreign adversaries or companies organised in, or otherwise subject to the direction or control of, a foreign adversary. These regulations were issued under Executive Order 13873, signed by President Trump in May 2019, intended to protect sensitive information, critical infrastructure and vital emergency services in the United States. The Department of Commerce has identified China, Cuba, Iran, North Korea and Russia as foreign adversary countries, and Venezuelan president Nicolás Maduro individually as a foreign adversary. On 17 March 2021,

10 Pub L 117-78 (2021).

11 This amendment was part of the Trade Facilitation and Trade Enforcement Act of 2015, signed on 24 February 2016.

and again on 13 April 2021, the Department of Commerce issued subpoenas to multiple Chinese companies that provide ICTS in the United States in a move that the Department described as an 'important step in investigating whether the transactions involving these companies meet the criteria set forth in the Executive Order'. These actions indicate that the Biden administration intends to actively use this new power to evaluate transactions, although there has been little to no public enforcement activity to date.

As the geopolitical exchange plays out, the full spectrum of sanctions and export control strategies that have evolved over recent years are being promulgated across a rapidly developing legal and political landscape that is largely unrecognisable from the sanctions philosophies of just a decade ago. Sanctions and counter-sanctions are already proving disruptive to global supply chains, as companies facing import and export restrictions on one side of relevant borders or another are forced to find alternative sources of supply, to divert shipments to alternative markets or to otherwise revise or unwind sourcing and supply strategies. This includes disruptions due to direct prohibitions on particular imports or exports; indirect impacts due to finance and investment-related restrictions; and market-driven pressures to curtail or cease certain wholly allowable activities as a matter of moral or ethical compulsion, or political expediency.

For example, China has issued retaliatory sanctions against the United States for what it views to be unjustifiable extraterritorial measures. Pursuant to Beijing's 2021 Anti Foreign Sanctions Law, Chinese entities are prohibited from either directly or indirectly implementing discriminatory measures taken by a foreign country, establishing a private cause of action for Chinese citizens to sue enabling entities. Importantly, the Law empowers Chinese authorities to issue countermeasures, including criminal prosecutions, against individuals who directly or indirectly participate in the formulation of foreign restrictive measures. Further, these lists may be extended to spouses, relatives and entities with which they are associated. Construed broadly, foreign nationals or entities with subsidiaries in China can be deemed as facilitating US sanctions by redirecting supply chains to competitors in western-allied jurisdictions.

These countervailing sanctions regimes will impose conflicting compliance and contract obligations on multinational businesses, all at a time when regulatory agencies are promising more civil and criminal enforcement action and greater penalties for sanctions and exports violations. Whereas in the past, many violations were deemed too trivial or attenuated to prosecute, recent enforcement actions underscore a new willingness from US regulators to incentivise corporate compliance through harsher punishment. On this last point, as part of a series of announcements, in March 2023 the US Department of Justice

(DOJ) re-emphasised that it views sanctions and export control violations as not just a technical area of concern, but rather as a top prosecutorial priority, akin to the corporate prosecutions of prior decades under the US Foreign Corrupt Practices Act.

Compliance strategies

Sanctions and export controls can be highly dynamic in the speed with which they can be implemented and adjusted. Accordingly, businesses operating with international supply chains need to be prepared to be equally nimble. Fortunately, there are relatively straightforward and scalable strategies that companies can deploy to ensure they have a robust and effective compliance framework through which to operate, as detailed below.

US regulators now expect that sanctions and export compliance is a board room-level topic. Recent agency actions signal that enhanced control protocols are expected to be the rule for companies when dealing with higher-risk markets and trading in advanced technologies. For example, in a first-of-its-kind announcement in March 2023, BIS, the DOJ and OFAC issued a joint warning on compliance expectations, advising that companies must exercise heightened caution and conduct additional diligence upon indicia that a transaction will involve a party engaged in evasion efforts. The joint announcement is emblematic of the new unified regulatory front and reinforces that for companies engaged in cross-border activity, compliance requires a multifaceted approach to classification, training, risk-based due diligence, end-user certification and screening.

Classification and risk analysis

It is imperative that companies moving goods and technologies across borders fully understand the potential restrictions that may apply to those transactions. This starts with a clear understanding of which goods and technologies fall under which applicable export control regimes. Companies should understand which regimes apply (e.g., whether they are subject to control as military items, dual-use items or purely commercial items), where their products are classified within each applicable regime and what licensing, reporting and other requirements might apply to their export. As the BIS restrictions on advanced technologies illustrate, a frequent mistake is to focus too narrowly on the finished products that a company might ship to customers abroad.

Once applicable classifications are well understood, companies should conduct supply chain risk analysis to determine whether and where they might face challenges in securing licences or other export authorisations, and whether and where they might face heightened risk of sanctions impacting their supply chains. Among

other things, companies must know the source of their raw materials and other goods and have some understanding of how their suppliers conduct business. As part of the risk analysis, contracts should be reviewed to ensure that appropriate contractual language is employed and that the company is properly exercising its rights under each contract. Not only will this risk analysis help identify and avoid potential pitfalls, but it can also serve as a baseline for demonstrating that a company's compliance programme is being reasonably risk-calibrated.

Resource allocation

Companies operating across borders that leave sanctions and export control compliance as an afterthought do so at their own peril. Companies should allocate adequate resources to this compliance function, both internally and through the use of outside advisers. The larger and more sophisticated the company and its global activities, the more enforcement authorities will expect to be invested in related compliance efforts.

Training

It goes without saying that a company's workforce can only address compliance risks if it is aware of and attuned to those risks. Training is therefore imperative, not only for those expected to serve as frontline compliance gatekeepers, but also for anyone in a function that touches on the supply chain. Personnel in finance and accounting, sales and marketing, logistics and fulfilment, and – critically – management should all have at least a baseline understanding of how sanctions and export controls work and impact the company and its supply chain, so that they can be positioned to identify, report and escalate red flags indicating potential violations as early as possible.

Due diligence

As the Xinjiang discussion above illustrates, due diligence is an increasingly important consideration when dealing with higher-risk markets. It will only become increasingly so. Just as a company should understand its goods and technology through classification, so too should it understand its counterparties and third-party partners through some level of due diligence. While the level and type of due diligence can and should be calibrated to the relative risks presented by the market, transactions and type of parties involved, it should not be ignored altogether. Further, an effective third-party due diligence programme can protect a company not just against sanctions and export control risk, but also against

bribery and corruption risks, money laundering risks and business risks, including potential exposure to undue financial or reputational risks associated with human rights abusers or unqualified (or underqualified) partners and counterparties.

Screening

Screening is an often overlooked but mission-critical compliance strategy in the context of sanctions and export control compliance. It is necessary to determine not only whether a company might be dealing with a designated sanctions target or export-restricted entity, but also whether it can be readily automated and built into existing business infrastructure such as enterprise resource planning platforms and payment systems.

As a good starting point, to facilitate screening the US government has compiled the Consolidated Screening List and an online search tool that purports to be an easily queried comprehensive database for foreign entities sanctioned or subject to trade restrictions across the US regulatory system.[12] That said, companies should have a more robust policy of checking new agency guidance and updates to restricted entities lists, along with requiring disclosure and beneficial ownership information before transacting with suppliers engaged in high-risk activities or based in targeted jurisdictions.

Practical considerations

Sanctions, export controls and import prohibitions can be deployed in a coordinated and complementary way. In considering them, companies should bear in mind that when they see an emergent use of one to target particular conduct or companies, there is a good chance the other will follow.

One key consideration is that sanctions, export controls and import prohibitions can be 'sticky', insofar as they can follow a person or an entity as they operate outside their home jurisdiction based on their nationality, and they can follow a product as it moves through commerce because of its origin. For example, a US national working for a European company outside the United States cannot be involved in that company's dealings with Iran without violating US sanctions (without a particular licence or other authorisation). Similarly, a US-origin air traffic control system that has been exported to a customer in Europe will continue to be subject to US export controls if the customer wants to re-export it to a recipient in Asia. Accordingly, the selling company may need to obtain a

12 The Consolidated Screening List can be found at www.trade.gov/data-visualization/csl-search.

licence to conduct the sale, even if none was required for the original export (as licensing requirements can vary depending on the country to which an item is being exported or re-exported). Export controls are also sticky insofar as they can attach to an item once it is imported into a jurisdiction, unless it is simply moving in transit through the jurisdiction or is being held in a free trade zone or other special-status area. As a result, it is important to have a thorough, holistic and comprehensive view of where and how sanctions and export controls can impact an organisation.

For example, it is not unusual for the documentation for an item originally exported from the United States to include EAR or OFAC declarations notifying any intermediate consignees or end users of the US origin of the shipment and asserted extraterritorial application of US laws and regulations. It is also the case that some US exporters request information and certifications to assess their potential export obligations[13] and satisfy best practice guidance promulgated by BIS in support of efforts to ensure re-export controls are operating effectively and preventing improper diversion to prohibited end uses, end users and locations.[14] Although these inquiries are not necessarily required, particularly in the case of exports of products subject to limited export classifications (e.g., the EAR99 catch-all classification under the EAR), BIS considers it a 'red flag' (that should be resolved before completion of a transaction) if a company refuses to cooperate with reasonable requests for information.[15] Accordingly, unless there is a reasonable, good faith and readily articulable reason not to comply, counterparties making reasonable requests should be given adequate information and assurances to satisfy their inquiries.

13 Although a destination control statement is not required for most EAR99 exports or most re-exports (see 15 C.F.R. 732.5(b)), it is not unreasonable for a company to inquire as to end-user and end-use information to fully assess whether an export is allowable under General Prohibition Five (see 15 C.F.R. §§ 732.3(m) (encouraging performance of 'Know Your Customer' due diligence) and 744.1 (regarding prohibited end uses and end users)).

14 See 15 C.F.R. Part 732, Supplement 3 (outlining guidance for 'Know Your Customer' due diligence); 'BIS "Best Practices" for Industry to Guard Against Unlawful Diversion through Transshipment Trade', available at www.bis.doc.gov/index.php/documents/pdfs/625-best-practices/file.

15 See 15 C.F.R. Part 732, Supplement 3 (identifying 'red flags': when '[t]he customer or purchasing agent is reluctant to offer information about the end-use of a product'; and '[w]hen questioned, the buyer is evasive or unclear about whether the purchased product is for domestic use, export or reexport').

Finally, companies should be aware that while sanctions and export restrictions can be imposed quickly in the face of a developing foreign policy issue, the run up to the imposition often develops quite slowly and with a good deal of purposeful foreshadowing. In the example of more restrictive export controls with China, this was a years' long evolution across multiple administrations, legislative acts, agency announcements and notices of proposed rule-making. Whether examined individually or read together, the United States announced these moves to industry well in advance of the eventual punch. Companies with cautious advisers were well apprised and benefited from a period to recalibrate before new restrictions took effect. Where prevailing political and economic policy views put specific regions, entities or commodities in an entity's cross hairs, there is a significant risk that sanctions of some form will follow. Businesses should not wait for a designation or WRO to be issued before addressing potential issues and considering options for supply chain redundancy or other changes.

By the same token, sanctions and export controls can be nimble and quickly deployed, as we have seen in the case of the response to Russia's invasion of Ukraine. Taking largely unforeseeable circumstances such as Russia's aggression into account, having a well-trained compliance function in place, supported by trusted outside advisers, is the key to having the system resiliency needed to rapidly pivot in the wake of precipitous sanction and export control developments.

Conclusion

The sanction and export control regimes described above are complex, with a variety of overlapping considerations and jurisdictional vagaries that can vary from country to country and transaction to transaction, and that are subject to periodic amendment. Companies seeking to navigate them successfully need to thoroughly understand the goods and technology with which they deal and the supply chains through which they operate.

CHAPTER 21

Practical Issues in Cyber-Related Sanctions

Timothy O'Toole, Christopher Stagg, FeiFei Ren, Caroline Watson, Manuel Levitt and Samuel Cutler[1]

Development of US cyber-related sanctions regimes

Overview of the Cyber-Related Sanctions Program

The United States has been at the forefront of establishing a cyber-focused economic sanctions regime,[2] which is primarily administered by the US Department of the Treasury's Office of Foreign Assets Control (OFAC), although criminal prosecutions for certain wilful sanctions violations are the responsibility of the US Department of Justice.

---

1 Timothy O'Toole is a member, Christopher Stagg and FeiFei Ren are counsel, Caroline Watson and Manuel Levitt are senior associates, and Samuel Cutler is an associate, at Miller & Chevalier Chartered.

2 Other jurisdictions, including the EU and UK, have begun taking significant steps to develop sanctions programmes to deter malicious cyber actors and respond to increasingly frequent and severe cyberattacks. See Council Decision 2019/797 2019 OJ (L 129/13) (EU); and Council Regulation 2019/796 2019 OJ (L 129/1) (EU). See, generally, the Cyber (Sanctions) (EU Exit) Regulations 2020, www.legislation.gov.uk/uksi/2020/597/contents/made. While these developments are significant, the EU and UK have used sanctions far less frequently than the United States, with just eight persons and four entities sanctioned under the EU's cyber-related sanctions framework thus far. See Council Decision 2020/1127, 2020 OJ (L 246/12) (EU); and Press Release, European Council, 'Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack' (22 October 2020), www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/.

OFAC administers a variety of sanctions targeting malicious cyber-related activities, such as cyberespionage, cyber-intrusions on critical infrastructure and computer networks, and disinformation campaigns conducted from abroad. The bulk of these sanctions are administered under OFAC's Cyber-Related Sanctions Program, which was established in 2015 as part of the Obama administration's response to malicious cyber-enabled activities originating from foreign countries that were directed at both US government agencies and private sector US entities. However, sanctions targeting malicious cyber-related activities are also authorised under other statutory and executive branch sanctions authorities, including the Countering America's Adversaries Through Sanctions Act (CAATSA),[3] as well as Executive Order (EO) 14024, 'Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation', issued on 15 April 2021.[4]

Prior to the Obama administration's first EO authorising cyber-related sanctions, malicious cyber-intrusions and cyberespionage from abroad were becoming increasingly frequent and severe. For example, on 19 May 2014, in its first major prosecution against a state actor for malicious cyber-enabled activities, the US Department of Justice indicted five Chinese nationals, allegedly affiliated with the Chinese military, for gaining unauthorised access to computer networks for the apparent purpose of engaging in economic espionage targeted at six US entities involved in the nuclear power, metals and solar products industries.[5] In September 2014, President Obama said his administration viewed cyber-enabled theft of trade secrets as 'an act of aggression that has to stop' and warned that the US was prepared to impose countervailing actions 'to get [China's] attention'.[6]

Before the establishment of OFAC's cyber-related sanctions programme, US law enforcement agencies had legal authority to pursue charges against individuals engaged in various types of cyberespionage or unauthorised intrusions into US government and private sector computers and networks.[7] Nevertheless, facing an

3 CAATSA, Pub. L. No. 115–44, 131 Stat. 886 (2 August 2017).

4 Executive Order (EO) 14024, 86 Fed. Reg. 20,249 (15 April 2021).

5 Press Release, US Dep't of Justice, 'US Charges Five Chinese Military Hackers for Cyber Espionage Against US Corporations and a Labor Organization for Commercial Advantage' (19 May 2014), www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

6 Graham Webster, 'Obama: Cyber Theft "an Act of Aggression" but US and China Can Develop Norms', *The Diplomat* (18 September 2015), https://thediplomat.com/2015/09/obama-cyber-theft-an-act-of-aggression-but-us-and-china-can-develop-norms/.

7 Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030; Economic Espionage Act of 1996, 18 U.S.C. § 1831 et seq.

increasingly severe threat posed by foreign-based hackers targeting valuable US intellectual property and sensitive private data, among other things, US national security agencies viewed sanctions as a tool well-designed to address the extraterritorial nature of cyber-enabled attacks from foreign actors.

This culminated on 1 April 2015 when President Obama issued EO 13694, which declared a national emergency to deal with 'the unusual and extraordinary threat to the national security, foreign policy, and economy of the United States' arising from 'the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States'.[8] As with most US economic sanctions authorities, this EO was issued pursuant to the International Emergency Economic Powers Act[9] and the National Emergencies Act.[10]

On 28 December 2016, President Obama issued EO 13757, which amended EO 13694 to broaden the scope of cyber-related activities subject to sanctions. As amended, those EOs permit the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to impose blocking sanctions[11] on persons determined:

> • *to be responsible for or complicit in, or to have engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of:*
>   • *harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;*
>   • *significantly compromising the provision of services by one or more entities in a critical infrastructure sector;*
>   • *causing a significant disruption to the availability of a computer or network of computers;*

8 EO 13694, 80 Fed. Reg. 18,077 (1 April 2015), reprinted as amended in 22 U.S.C. § 9522.

9 50 U.S.C. §§ 1701–1708.

10 50 U.S.C. §§ 1601, 1621–1631 and 1641.

11 Persons blocked pursuant to EO 13694, as amended by EO 13757, are included on the Specially Designated Nationals and Blocked Persons List maintained by the Office of Foreign Assets Control (OFAC). The initial designations under this authority were made on 28 December 2016.

- *causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; or*
- *tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions; and*

- *[t]o be responsible for or complicit in, or to have engaged in, the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of trade secrets misappropriated through cyber-enabled means, knowing they have been misappropriated, where the misappropriation of such trade secrets is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States;*
- *to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, [certain activities described above] or any person whose property and interests in property are blocked pursuant to [EO 13694, as amended];*
- *to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked [pursuant to EO 13694, as amended]; or*
- *to have attempted to engage in any of the activities described in [EO 13694, as amended].*[12]

Cyber-related sanctions under CAATSA

On 2 August 2017, President Trump signed into law CAATSA, which authorised, inter alia, the imposition of cyber-related sanctions targeting Russia and codified the cyber-related sanctions imposed through EO 13694 and EO 13757.[13] On 20 September 2018, President Trump issued EO 13849, 'Authorizing the Implementation of Certain Sanctions Set Forth in the Countering America's Adversaries Through Sanctions Act (CAATSA)', which delegates authority to impose sanctions under CAATSA to the Secretary of the Treasury.[14]

12 EO 13757 § 1(ii)–(iii), 82 Fed. Reg. 1 (28 December 2016).

13 22 U.S.C. § 9524. OFAC has since promulgated cyber-related sanctions regulations at 31 C.F.R. Part 578.

14 EO 13849, 83 Fed. Reg. 48,195 (20 September 2018).

With respect to Russia, Section 224 of CAATSA includes additional sanctions provisions targeting malicious cyber activities that are distinct from OFAC's Cyber-Related Sanctions Program. Specifically, Section 224(a)(1) of CAATSA requires the President to impose blocking sanctions on any person that the President determines '(A) knowingly engages in significant activities undermining cybersecurity against any person, including a democratic institution, or government on behalf of the Government of the Russian Federation; or (B) is owned or controlled by, or acts or purports to act for or on behalf of, directly or indirectly' that person.[15] 'Significant activities undermining cybersecurity' include:

- *significant efforts:*
  - *to deny access to or degrade, disrupt, or destroy an information and communications technology system or network; or*
  - *to exfiltrate, degrade, corrupt, destroy, or release information from such a system or network without authorization for purposes of:*
    - *conducting influence operations; or*
    - *causing a significant misappropriation of funds, economic resources, trade secrets, personal identifications, or financial information for commercial or competitive advantage or private financial gain;*
- *significant destructive malware attacks; and*
- *significant denial of service activities.*[16]

Additionally, the President is required to impose five or more menu-based sanctions on persons the President determines knowingly 'materially assists, sponsors, or provides financial, material, or technological support for, or goods or services (except financial services)' in support of, the cyber-related activity described in CAATSA Section 224(a)(1).[17] Those menu-based sanctions include restrictions on a sanctioned person's ability to participate in, conduct or obtain: US export licences; loans or assistance from certain US and foreign financial institutions, including the US Export-Import Bank; certain foreign exchange transactions; various transactions involving property in the United States; or US visas.[18] These authorities have been delegated to the Secretary of the Treasury in consultation with the Secretary of State.

15 22 U.S.C. § 9524(a)(1)(A)–(B).
16 id., § 9524(d)(1)–(3).
17 id., § 9524(a)(2).
18 id., § 9529.

For a person the President determines 'provides financial services' in support of the cyber-related activities described in CAATSA Section 224(a)(1), CAATSA requires the President to impose three or more menu-based sanctions, described separately at 22 USC Section 8923.[19] These include many of the same types of sanctions mentioned above.

Cyber-related sanctions under the new EO targeting harmful foreign activities of Russia

On 15 April 2021, President Biden issued EO 14024, which is aimed at countering a wide array of malign Russian government-sponsored activities, including interference in the 2020 US presidential election and the SolarWinds cyberattack.[20] EO 14024 significantly expands the categories of Russian persons that can be targeted for sanctions by the United States, and includes persons determined 'to be responsible for or complicit in, or to have directly or indirectly engaged or attempted to engage in . . . malicious cyber-enabled activities'.[21] Sanctions may also be imposed under EO 14024 on the spouses and adult children of persons subject to sanctions under this EO, as well as those determined by the Secretary of the Treasury, in consultation with the Secretary of State, to have materially assisted, sponsored or provided financial, material or technological support for, or goods or services to or in support of, among other things, malicious cyber-enabled activities. Notably, EO 14024 has been the tool of choice for the US to impose blocking and non-blocking sanctions targeting Russia in response to its military invasion of Ukraine in February 2022.

Re-issue of Cyber Related Sanctions Regulations

On 6 September 2022, OFAC published regulations replacing the original Cyber-Related Sanctions Regulations to 'further implement' EOs 13694 and 13757 and Section 224 of CAATSA. The re-issued regulations effectively add interpretive guidance, definitions, general licences and other regulatory provisions, some of which conform the scope of restrictions and regulations with other OFAC sanctions programmes. The regulations include, for example, provisions prohibiting actions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate any of prohibitions under the Cyber-Related Sanctions Regulations, which is a restriction found in nearly all of the other OFAC

19 id., § 9524(a)(3).

20 See footnote 4.

21 id., §1(a)ii.

sanctions programmes.[22] Additionally, the re-issued regulations also now explicitly define 'critical infrastructure sector' as 'any of the designated critical infrastructure sectors identified in Presidential Policy Directive 21 of February 12, 2013'[23] and 'cyber-enabled activities' as 'any act that is primarily accomplished through or facilitated by computers or other electronic devices'.[24]

OFAC Ransomware Advisory

On 1 October 2020, OFAC issued its 'Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments' (the 2020 Ransomware Advisory) to highlight the sanctions compliance risks associated with facilitating ransomware payments related to malicious cyber-enabled activities (e.g., by providing cyber insurance, digital forensics and incident response, and financial services related to processing ransom payments including by depository institutions and money services businesses).[25] In the Advisory, OFAC warned that facilitating a ransomware payment may not only enable and embolden criminals, as well as adversaries with a nexus to a sanctioned party or country, but also, critically, may not guarantee that a victim regains access to stolen data, and noted that victims of a ransomware attack should: contact OFAC immediately if they believe a request for a ransomware payment may involve a sanctions nexus; and contact the US Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection if an attack involves a US financial institution or may cause 'significant disruption to a firm's ability to perform critical financial services'.[26]

OFAC expanded its guidance on 21 September 2021 in a publication entitled 'Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments' (the 2021 Ransomware Advisory), which OFAC issued 'to highlight the sanctions risks associated with ransomware payments' and 'the proactive steps companies can take to mitigate such risks', including those actions that OFAC would consider to be mitigating factors with respect to enforcement. The 2021 Ransomware Advisory adds to the 2020 Ransomware Advisory in several

22 31 C.F.R. § 578.205.

23 id., § 578.302.

24 id., § 578.303.

25 OFAC, 'Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments' (1 October 2020) (the 2020 Ransomware Advisory), https://ofac.treasury.gov/media/48301/download?inline.

26 ibid.

significant ways:[27] it adds a strong discouragement of engaging in ransomware payments and a warning that entities making ransomware payments to a blocked person or a sanctioned jurisdiction are subject to strict liability and risk facing penalties, even without knowledge of a connection to a blocked person or sanctioned jurisdiction.[28] Consequently, OFAC also recommends that companies expand controls to account for the risk of ransomware payments being made to prohibited persons.[29] Further, OFAC strongly encourages, and even incentivises, companies to report ransomware demands to law enforcement and will consider cooperation with law enforcement as a mitigating factor when assessing penalties against entities that have been involved in making ransomware payments to blocked, or otherwise sanctioned, parties.[30]

The 2021 Ransomware Advisory references several other agencies and encourages the adoption of practices laid out in the Cybersecurity and Infrastructure Security Agency's Ransomware Guide[31] and consideration of applicable Financial Crimes Enforcement Network (FinCEN) regulatory obligations.[32]

Sanctions Compliance Guidance for the Virtual Currency Industry

On 15 October 2021, OFAC published guidance entitled 'Sanctions Compliance Guidance for the Virtual Currency Industry' (the Virtual Currency Guidance), which provides an overview of compliance best practices.[33] The Guidance clarifies that the sanctions compliance obligations imposed by OFAC apply equally to transactions involving virtual currencies and those involving traditional fiat currencies and that companies are responsible for ensuring that they do not

27 OFAC, 'Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments' (21 September 2021), https://ofac.treasury.gov/media/912981/download?inline.

28 ibid.

29 ibid.

30 ibid.

31 See Cybersecurity and Infrastructure Security Agency, 'Ransomware Guide' (September 2020), www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf.

32 Financial Crimes Enforcement Network (FinCEN), 'Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments' (1 October 2020), www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf. The 1 October 2020 FinCEN Advisory was revised and updated on 8 November 2021. See FinCEN, 'Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments' (8 November 2021) (the FinCEN Advisory),www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf.

33 OFAC, 'Sanctions Compliance Guidance for the Virtual Currency Industry' (October 2021), https://ofac.treasury.gov/media/913571/download?inline.

engage in direct or indirect transactions that are prohibited by OFAC sanctions when dealing in virtual currency.[34] The Virtual Currency Guidance acknowledges that OFAC sanctions have increasingly targeted persons that have used virtual currency in connection with various types of malign activity. Given the industry's rising level of importance, the Guidance encourages companies to have in place a risk-based compliance programme, which includes internal controls to identify and stop virtual currency transactions that would violate OFAC sanctions. Ultimately, the Guidance makes clear that companies are under the same obligations with respect to virtual currency as they are for fiat currency when it comes to complying with OFAC sanctions.

FinCEN Advisory

As noted above, OFAC's 2021 Ransomware Advisory made note of guidance from other agencies, including FinCEN. On 1 October 2021, FinCEN issued an advisory entitled 'Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments' (the FinCEN Advisory).[35] The FinCEN Advisory lists several red flag indicators to assist in identifying, preventing and reporting ransomware attacks and reminds financial institutions of their regulatory obligations regarding reporting suspicious activity involving ransomware. Financial institutions should note that although OFAC strongly encourages reporting of ransomware attacks and payments, the FinCEN Advisory makes clear in some instances that financial institutions may be required to report incidents.

OFAC enforcement and recent illustrative cases

OFAC's use of cyber-related sanctions authorities appears to be on the rise. OFAC enforcement of these sanctions authorities can generally be divided into two parts: (1) the imposition of blocking or menu-based sanctions on individuals and entities for engaging in sanctionable activities (e.g., perpetrating cyberattacks or materially assisting by laundering funds obtained thereby); and (2) the imposition of civil penalties for the violation of sanctions (e.g., transacting with a blocked person sanctioned for malign cyber activities). Criminal prosecutions for sanctions violations, which typically focus on the most egregious wilful misconduct, are within the purview of the US Department of Justice.

34 ibid.

35 FinCEN Advisory, footnote 32.

Since 2015, OFAC has designated numerous parties under cyber-related sanctions authorities each year. However, OFAC has, at least based on what has been made public, imposed relatively few civil penalties connected to cyber-related sanctions or other cyber-related sanctions compliance failures. Nevertheless, based on guidance issued in 2020 and OFAC's recent imposition of civil penalties against certain internet-based businesses and entities involved in the use of digital currencies,[36] OFAC has demonstrated that it expects parties to implement fully fledged risk-based sanctions compliance programmes to address malign cyber activities and other cyber-related vulnerabilities.

Cyber-related sanctions designations

OFAC has designated numerous persons under its cyber-related sanctions programme over the past few years, with more designations in 2022 than in any other year. Persons designated under these authorities include individual hackers, money launderers, non-state actors such as organised 'troll farms' (e.g., Internet Research Agency), international cybercriminal organisations (e.g., Evil Corp, Hydra Market, Garantex),[37] virtual currency mixers (e.g., Tornado Cash)[38] and even a few foreign government agencies (e.g., the Russian Federation Federal Security Service).

OFAC has mainly focused on actors residing in or associated with foreign nation states perceived as hostile to the United States – primarily Russia, China, Iran and North Korea – and engaging in certain malicious cyber-enabled activities, such as:

- development and distribution of malware, ransomware and phishing and spoofing scams;
- interference with electoral processes and institutions worldwide through false information or hacking;[39]

---

36 OFAC defines 'digital currency' to include 'sovereign cryptocurrency, virtual currency (non-fiat), and a digital representation of fiat currency'. OFAC, 'Virtual Currency FAQ 559' (15 October 2021), https://ofac.treasury.gov/faqs/559.

37 Press Release, OFAC, 'Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex' (Garantex and Hydra) (5 April 2022), https://home.treasury.gov/news/press-releases/jy0701.

38 See, e.g., Press Release, OFAC, 'U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash' (Tornado Designation) (8 August 2022), https://home.treasury.gov/news/press-releases/jy0916.

39 See, e.g., Press Release, OFAC, 'Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election' (18 November 2021), https://home.treasury.gov/news/press-releases/jy0494.

- theft of economic resources, trade secrets, personal identifying information or financial information by cyber intrusions for private financial gain;
- publication of stolen sensitive documents obtained and sometimes manipulated through cyber intrusions;
- disruption of network access;
- compromise of US government entities and US critical infrastructure sectors; and
- the use of virtual currency or other digital assets to evade or otherwise violate US sanctions.

OFAC's 2022 designations indicate its continued focus on the virtual currency industry's role in sanctions evasion.

More recently, OFAC has targeted state-backed groups engaging in cyber-enabled activities against the United States and its allies. In September 2022, for example, OFAC designated Iran's Ministry of Intelligence and Security and its Minister of Intelligence, which it alleged 'conducted malicious cyber operations targeting a range of government and private-sector organizations around the world and across various critical infrastructure sectors', through networks of cyber threat actors such as the now-sanctioned groups Muddy Water and APT39, and engaged in malicious cyber activities that disrupted the Albanian government's computer systems.[40] OFAC also designated 10 individuals and two entities associated with the Islamic Revolutionary Guard Corps, which engaged in various forms of ransomware activity and cybercrime against small businesses, a children's hospital, an accounting firm, a law firm, a New Jersey municipality, emergency service providers, healthcare practices, educational institutions and an electricity utility company serving a rural area.[41]

As noted above, entities involved in providing cryptocurrency-related services are also becoming a more frequent target of OFAC sanctions designations, with several major cryptocurrency-related service providers being designated in 2022, often for engaging in or facilitating money laundering, sanctions evasion and ransomware attacks. On 8 November 2022, for example, OFAC sanctioned Tornado Cash, a virtual currency mixer that, according to OFAC, obfuscated

40 Press Release, OFAC, 'Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities' (9 September 2022), https://home.treasury.gov/news/press-releases/jy0941.

41 Press Release, OFAC, 'Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity' (14 September 2022), https://home.treasury.gov/news/press-releases/jy0948.

the movement of over US$455 million stolen in March 2022 by the OFAC-designated, North Korea-controlled Lazarus Group in the largest known virtual currency heist to date.[42] Previously, Blender.io, which OFAC described as 'a virtual currency mixer that operates on the Bitcoin blockchain and indiscriminately facilitates illicit transactions by obfuscating their origin, destination, and counterparties' was sanctioned under EO 13694, as amended, marking the first time a virtual currency mixer has been sanctioned by OFAC.[43]

Another sanctions announcement from 2023 indicates increased coordination between the US and allied governments. On 9 February 2023, the US and UK jointly announced that a group of seven individuals who associated with a Russia-based cybercrime gang called Trickbot were being sanctioned for reportedly engaging in a string of illegal cyber activities, including ransomware attacks.[44]

Most recently, on 5 April 2023, OFAC designated Genesis Market, a 'criminal marketplace' believed to be located in Russia, which has reportedly been involved in, among other things, 'packaging' computer and mobile device identifiers, email addresses, usernames, passwords and other credentials stolen through the use of malware from leading US and international companies and selling them on its website.[45]

In many cases, persons that OFAC has found engaging in activities that are similar or analogous to those targeted under the Cyber-Related Sanctions Regulations have been designated under EOs or programmes that are distinct from the Cyber-Related Sanctions Regulations. For example, in addition to being designated under EO 13694, Tornado Cash's sanctions designation was updated to note that it was also sanctioned under the North Korea sanctions programme pursuant to EO 13772, based on OFAC's determination that the company had a role in 'enabling malicious cyber activities, which ultimately support the [Democratic People's Republic of North Korea]'s WMD program'.[46] In the case of Garantex, while the company appeared to have facilitated various cyber-enabled

42 Tornado Designation, footnote 38.

43 Press Release, OFAC, 'U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats' (6 May 2022), https://home.treasury.gov/news/press-releases/jy0768.

44 Press Release, OFAC, 'United States and United Kingdom Sanction Members of Russia-Based Trickbot Cybercrime Gang' (8 February 2023), https://home.treasury.gov/news/press-releases/jy1256.

45 Press Release, OFAC, 'Treasury Sanctions Illicit Marketplace Genesis Market' (5 April 2023), https://home.treasury.gov/news/press-releases/jy1388.

46 Press Release, OFAC, 'Treasury Designates DPRK Weapons Representatives' (8 November 2022), https://home.treasury.gov/news/press-releases/jy1087.

activities sanctionable under the Cyber-Related Sanctions Regulations, OFAC ultimately imposed sanctions on the virtual currency exchange under EO 14024, an EO that falls under OFAC's Russian Harmful Foreign Activities Sanctions programme, 'for operating or having operated in the financial services sector of the Russian Federation economy'.[47]

OFAC civil penalties

To date, OFAC has not imposed any publicly disclosed civil penalties specifically tied to cyber-related sanctions violations. However, the following civil settlements generally illustrate OFAC's compliance expectations in the cyber and digital areas. A constant theme is the offending company's failure to apply relevant knowledge in its possession – particularly internet protocol (IP) addresses – to identify, prevent or block prohibited users or transactions. US enforcement agencies, including OFAC and the departments of Justice and Commerce, called particular attention to a company's failure to identify and screen transaction parties by their IP addresses in the following enforcement actions:

- a settlement agreement that US-based company Bittrex, Inc, which provides an online virtual currency exchange and hosted wallet services, entered into with OFAC on 11 October 2022 relating to 116,421 apparent violations of multiple sanctions programmes, where the company failed to prevent persons apparently located in the Crimea region of Ukraine, Cuba, Iran, Sudan and Syria from using its platform to engage in over US$263 million worth of virtual currency-related transactions;[48]
- a settlement agreement that Payoneer Inc, a publicly traded New York-based online money transmitter and provider of prepaid access, entered into with OFAC on 23 July 2021 in connection with 2,220 apparent violations of multiple sanctions programmes;[49]

47 Garantex and Hydra, footnote 37.

48 Enforcement Release, OFAC, 'OFAC Settles with Bittrex, Inc. for $24,280,829.20 Related to Apparent Violations of Multiple Sanctions Programs' (11 October 2022), https://ofac.treasury.gov/media/928746/download?inline.

49 Enforcement Release, OFAC, 'OFAC Enters Into $1,385,901.40 Settlement with Payoneer Inc. for Apparent Violations of Multiple Sanctions Programs' (23 July 2021), https://ofac.treasury.gov/media/911571/download?inline.

- a settlement agreement that the German-based software company SAP SE entered into with OFAC on 29 April 2021 relating to 190 apparent violations of the US sanctions against Iran;[50]
- a settlement agreement that US-based company BitPay, Inc, a digital currency payment service provider, entered into with OFAC on 18 February 2021 in connection with 2,102 apparent violations of multiple sanctions programmes;[51] and
- a settlement agreement that US-based technology company BitGo, Inc entered into with OFAC on 30 December 2020 in connection with 183 apparent violations of multiple sanctions regimes.[52]

In its announcements of the Bittrex, BitGo and BitPay settlements, OFAC emphasised that US persons involved in the provision of digital currency services (including companies that facilitate or engage in online commerce or process transactions in digital currency) – like all other US persons – have 'sanctions compliance obligations'. Additionally, citing the essential components of compliance in its 'Framework for OFAC Compliance Commitments', OFAC highlighted the importance of implementing technical controls, such as sanctions list and IP address screening, IP blocking mechanisms and blockchain tracing, to mitigate sanctions risks in connection with digital currency services.[53]

Cyber-related sanctions compliance risks

Ransom payments

As discussed in OFAC's 2020 Ransomware Advisory, a compliance risk unique to cyber-related sanctions relates to ransomware attacks, specifically the payment of ransoms themselves.[54] Unless OFAC grants a specific licence, a person who

50 Enforcement Release, OFAC, 'OFAC Settles with SAP SE for Its Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations' (SAP Settlement) (29 April 2021), https://ofac.treasury.gov/media/97351/download?inline.

51 Enforcement Release, OFAC, 'OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions' (BitPay Settlement) (18 February 2021), https://ofac.treasury.gov/media/54341/download?inline.

52 Enforcement Release, OFAC, 'OFAC Enters Into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions' (BitGo Settlement) (30 December 2020), https://ofac.treasury.gov/media/50266/download?inline.

53 See BitGo Settlement, footnote 52, at 3; BitPay Settlement, footnote 51, at 3.

54 OFAC, 2020 Ransomware Advisory, footnote 25.

makes ransom payments to sanctioned parties or jurisdictions may face penalties for violating OFAC regulations. Particularly for ransom payments made in a digital currency, the difficulty of definitively determining whether the transaction involves a sanctioned party or sanctioned jurisdiction can create serious compliance challenges. Although no public civil penalty has been announced in connection with this type of violation, OFAC has emphasised the risks related not only to direct payments of ransoms in contravention of sanctions regulations, but also to facilitating these payments (e.g., ransomware insurance businesses, payment processors). On 21 September 2021, OFAC released the 'Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments',[55] which emphasises the US government's strong discouragement of payment of cyber ransom or extortion demands and the importance of improving cybersecurity practices and reporting to, and cooperating with, US government in the event of ransomware attacks.

Digital currency sector

Via its enforcement actions and guidance,[56] OFAC has also been clear that transactions and services involving digital currency present sanctions compliance risk. Therefore, businesses that allow digital currency payments or that are involved in the digital currency market or sector (e.g., digital currency trading platforms, asset management, security) need to consider how to implement appropriate risk-based compliance measures that address the specific vulnerabilities of digital currency. Without appropriate compliance measures, a digital currency service provider could incur liability not only for violating sanctions (e.g., by dealing with blocked persons or persons in sanctioned jurisdictions), but also for facilitating sanctions violations by other parties to a transaction (even if inadvertent).

For example, just as with fiat currency, businesses involved in digital currency transactions would be expected to deploy risk-based sanctions screening for involved parties and to ensure that the funds are not destined for a sanctioned jurisdiction.[57] As described above, recent enforcement actions highlight OFAC's expectation that internet-based businesses should use all relevant known

55 Press Release, OFAC, 'Treasury Takes Robust Actions to Counter Ransomware' (21 September 2021), https://home.treasury.gov/news/press-releases/jy0364.

56 OFAC has also periodically released FAQs addressing various topics concerning cyber-related sanctions and digital currency compliance issues more broadly. See OFAC, 'Cyber-Related Sanctions FAQs', https://ofac.treasury.gov/faqs/topic/1546; OFAC, 'Virtual Currency FAQs', https://ofac.treasury.gov/faqs/topic/1626.

57 OFAC, 'Virtual Currency FAQ 560' (19 March 2018), https://ofac.treasury.gov/faqs/560.

information in the course of their business for sanctions compliance purposes as well. Specifically, OFAC has recently imposed civil penalties on multiple businesses that knew customers' IP addresses (e.g., by their use of internet services) but did not ensure that customers with IP addresses in sanctioned jurisdictions were screened or blocked from using their services or transacting on their platforms.[58]

Cryptocurrency, a type of digital currency reliant on cryptography to secure and verify transactions, also presents risk because cybercriminals and other sanctioned parties (including the government of North Korea, Iranian entities and many Russian entities and individuals that have been designated by OFAC since the Russian invasion of Ukraine) may resort to using cryptocurrency as a tool to evade sanctions, launder money and facilitate other illegal activities (e.g., nuclear weapons proliferation[59]).[60] The proceeds of malicious cyber activities are regularly transferred to cryptocurrency exchanges and peer-to-peer marketplaces with negligible customer screening compliance programmes, or individual peer-to-peer or over-the-counter traders operating on exchanges that do not screen their customers.[61] More broadly, digital currency infrastructure has been targeted by some cybercriminals who use illegitimate websites and malicious software to conduct phishing attacks on the digital currency sector.[62] Due diligence and controls to determine whether digital currency has been tainted by sanctionable or criminal cyber activities may be needed in certain transactions or businesses. In relation to this, OFAC has emphasised how anti-money laundering and combating the financing of terrorism controls play a vital role in sanctions and law enforcement generally because these can force cybercriminals to take measures to circumvent the controls that leave trails of evidence and traceability.[63] OFAC

58 See SAP Settlement, footnote 50; BitGo Settlement, footnote 52; and BitPay Settlement, footnote 51.

59 Michelle Nichols and Raphael Satter, 'UN experts point finger at North Korea for $281 million cyber theft, KuCoin likely victim', Reuters (9 February 2021), www.reuters.com/article/us-northkorea-sanctions-cyber/u-n-experts-point-finger-at-north-korea-for-281-million-cyber-theft-kucoin-likely-victim-idUSKBN2AA00Q.

60 See Press Release, OFAC, 'Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses' (28 November 2018), https://home.treasury.gov/news/press-releases/sm556; Press Release, OFAC, 'Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group' (2 March 2020), https://home.treasury.gov/news/press-releases/sm924.

61 ibid.

62 See 'Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group', footnote 60.

63 See Press Release, OFAC, 'Treasury Sanctions Russian Cyber Actors for Virtual Currency Theft' (16 September 2020), https://home.treasury.gov/news/press-releases/sm1123.

has been identifying certain digital currency addresses[64] associated with Specially Designated Nationals (SDNs) and other blocked persons. This new type of information, which OFAC expects to be part of standard screening protocols, typically entails a more arduous screening process due to the difficulty of searching these addresses in the SDN List.[65]

OFAC has also noted that as various sanctioned jurisdictions (e.g., Iran, Russia and North Korea) resort to using or creating digital currencies, the risk entailed in the digital currency sector may increase.[66] The mere use of certain digital currencies could be subject to blanket prohibition, which has already occurred with respect to the 'Petromoneda' digital currency issued by the government of Venezuela.[67] As more government-backed digital currencies are issued, this will be an evolving risk area.

Inadvertent exports to sanctioned jurisdictions

Another potential area of compliance risk is the cybertheft of export-controlled information for use in a sanctioned jurisdiction. Any cyber-enabled theft may represent an unauthorised and illegal export of controlled US technology or software. While this type of event may raise more direct export control compliance concerns, especially depending on the nature of the stolen technology or software, OFAC could potentially consider a victim entity accountable for facilitating a sanctions violation for failing to implement appropriate risk-based measures to prevent the compromise and export of the controlled information (e.g., inadequate data security). This scenario highlights that in addition to sanctions regulations, entities should also consider other areas of related compliance risk implicated by malicious cyber-enabled activities, including export controls.

64 OFAC, 'Virtual Currency FAQ 559', footnote 36 (OFAC defines a 'digital currency address' as 'an alphanumeric identifier that represents a potential destination for a digital currency transfer. A digital currency address is associated with a digital currency wallet').

65 See OFAC, 'Virtual Currency FAQs 562' (19 March 2018), '563' (6 June 2018) and '594' (18 May 2023), https://ofac.treasury.gov/faqs/topic/1626.

66 See, e.g., 'Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses', footnote 60.

67 EO No. 13827, 83 Fed. Reg. 12,469 (19 March 2018).

Practical considerations to mitigate cyber-related sanctions compliance risks

In response to the risks described above, and depending on the circumstances, companies may wish to consider some of the following compliance measures.

Risk assessment and risk-based compliance programme

Depending on the nature of a company's business activities, the risks and challenges in complying with cyber-related sanctions may differ substantially. Conducting an appropriate risk assessment, and tailoring a risk-based compliance programme appropriately with sanctions compliance training for relevant personnel, are essential steps in mitigating risk. Businesses of any size that utilise the internet, even if only for email, may face an increasing risk of ransomware attacks, which raises cyber-related sanctions compliance concerns. This is also a particular concern following Russia's military invasion of Ukraine and the expansion of US sanctions and other restrictions that target numerous sectors of the Russian economy, including the financial and energy sectors. Businesses involved in e-commerce could potentially face higher cyber-related sanctions compliance risks, including the risk of inadvertently providing goods or services to a sanctioned person or jurisdiction. Those involved in the digital currency sector, including companies that facilitate or engage in online commerce or process transactions using digital currencies, may be more likely to face malicious cyber-enabled attacks, incurring increased sanctions compliance risks and, given the expanded sanctions on Russia and other regions, may also have to contend with sanctioned parties seeking to use digital currencies to evade US sanctions. These risks could be even greater for companies involved in providing cyber insurance, digital forensics services, cyberattack incident response services and financial services that facilitate ransom payments.

Risk-based screening, due diligence, IP blocking and geolocation measures

Depending on a company's risk profile, it is often best to ensure that all relevant parties are properly screened before engaging in a transaction, to ensure no payments or deliveries of goods or services are made to sanctioned parties or jurisdictions. Reliable screening depends on the collection and review of information reasonably accessible to the company, which means companies should proactively consider ways to verify users' identities and locations. As evidenced in the BitGo settlement, merely relying on attestations from users concerning their locations without conducting any further due diligence may not suffice to meet compliance obligations in OFAC's view.

As the world becomes more digitised, bad actors become more sophisticated and determined to conceal their identity or location, and certain sanctions programmes targeting particular jurisdictions (e.g., Russia and the Crimea, Donetsk and Luhansk regions of Ukraine) are introduced, the screening function must adapt as well. Companies should consider including a party's IP address information in the screening process when this information is available and utilising more advanced geolocation and IP spoofing detection tools to ensure that dealings with parties, including the provision of services and payments, do not involve parties in sanctioned jurisdictions. A company may need to implement IP blocking and 'geofencing' measures to prevent sanctioned persons and persons in sanctioned jurisdictions from opening accounts on the company's website or platform that would allow them to access the company's services. Where a company becomes aware that its customers, partners or account holders are located in jurisdictions subject to OFAC sanctions, it may be necessary to promptly put restrictions on those accounts and investigate whether US sanctions have been violated.

Identify, block and report sanctioned digital currency

Companies engaged in or reliant upon digital currency have the same obligations with respect to US sanctions law compliance as those conducting transactions in traditional currencies. OFAC has included certain digital currency addresses associated with blocked persons as part of its set of identifiers on the SDN List, meaning that companies may have obligations to block digital currency payments associated with those digital addresses.[68] Companies that may transact routinely with the digital currency addresses should consider enhancing their screening and compliance processes to account for this information.

Screening a digital currency address is more involved than the screening of ordinary names or physical addresses, but OFAC has provided some guidance on how to search the SDN List for these addresses. OFAC guidance also provides two discrete methods companies may integrate into their compliance programmes to block digital currencies held by sanctioned persons.[69] Companies dealing in digital currencies held by users in regions subject to expanded US sanctions, particularly Russia, will also need to be highly alert to the risk that parties

68 See OFAC, 'Virtual Currency FAQs 562–63, 594', footnote 36. See, generally, OFAC, 'Virtual Currency FAQs', https://ofac.treasury.gov/faqs/topic/1626.

69 See OFAC, 'Cyber-Related Sanctions FAQ 646' (15 October 2021), https://ofac.treasury.gov/faqs/646.

subject to sanctions will try to evade US sanctions and obfuscate their identity or location by using digital currencies. Companies may consider implemented blockchain tracing software to assist in identifying and blocking virtual currency addresses associated with sanctioned persons. As seen in the Bittrex settlement, OFAC considers blockchain tracing as one of the significant remedial measures taken by companies to curtail apparent violations of US sanctions. Companies may block digital wallets associated with digital addresses identified and sanctioned by OFAC or may combine all digital wallets with digital addresses identified by OFAC into one digital wallet. OFAC also requires companies holding wallets with blocked digital addresses to report the digital currency to OFAC within 10 business days and to have a traceable audit trail.

Compliance related to making or facilitating ransom payments

Given the risks associated with ransomware payments and the possibility that sanctioned persons or jurisdictions may be involved in them, sanctions compliance programmes should incorporate risk-based procedures for responding to ransomware attacks, including, at a minimum, thorough enhanced screening procedures. In many cases, companies should strongly consider engaging with relevant law enforcement agencies when ransomware attacks arise, including OFAC if the ransomware attack or a requested ransom payment may potentially involve a sanctioned party or country.

Preventative measures regarding cyber intrusions

In looking to root causes, businesses may also reduce their cyber-related sanctions compliance risks by making efforts to prevent cyber intrusions in the first place. US government agencies, including FinCEN[70] and the US Department of Justice,[71] have provided guidance on best practices for companies to help them protect their systems from cyberattacks. Integrating these considerations into a company's overall approach to risk management and, specifically, its sanctions compliance programme in the first instance can prevent sanctions violations arising from malicious cyber-enabled activities (e.g., ransomware attacks) carried out by a sanctioned party or country.

---

70 FinCEN, 'Advisory on Illicit Activity Involving Convertible Virtual Currency' (9 May 2019), www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf.

71 US Dep't of Justice, et al., 'How to Protect Your Networks from Ransomware: Interagency Technical Guidance Document' (June 2016), www.justice.gov/criminal-ccips/file/872771/download.

Potential benefits of cooperation with the US government in the cybersecurity context

We close by highlighting the strong incentives that US government enforcers provide in exchange for voluntary disclosure and robust cooperation by companies that have committed potential US sanctions violations, which apply equally in the cyber context. For example, in the OFAC ransomware advisories discussed above, OFAC emphasises that it would consider both a 'self-initiated, timely, and complete report of a ransomware attack to law enforcement' and 'full and timely cooperation with law enforcement' to be 'significant' mitigating factors in determining the proper enforcement outcome if a ransom payment is made and 'if the situation is later determined to have a sanctions nexus'.[72] Likewise, in the SAP enforcement matter discussed above, the Department of Justice explained that SAP's penalty 'would have been far worse had they not disclosed, cooperated, and remediated. We hope that other businesses, software or otherwise, we [sic] heed this lesson.'[73] OFAC also touted SAP's 'substantial' cooperation and significant remedial actions, as well as its voluntary disclosure, in explaining why the actual penalty was reduced substantially from the civil penalty recommended under OFAC's enforcement guidelines. Although cooperation with US government enforcers is a complex, risk-based decision that must be considered carefully, the potential benefits are clear under the right circumstances.

72 OFAC, 2020 Ransomware Advisory, footnote 25, at 4.

73 Dep't of Justice, 'SAP Admits to Thousands of Illegal Exports of its Software Products to Iran and Enters into Non-Prosecution Agreement with DOJ' (29 April 2021), www.justice.gov/opa/pr/sap-admits-thousands-illegal-exports-its-software-products-iran-and-enters-non-prosecution.

CHAPTER 22

The Role of Forensics in Sanctions Investigations

Leilei Wu, Bridget Johnson, Christine Sohar Henter and Michelle Rosario[1]

Introduction

The global value chain is a far-reaching system reliant on cross-border transfers of funds, services and goods, which are increasingly subject to economic sanctions law enforcement by the Office of Foreign Assets Control (OFAC), the US Department of Justice and other regulatory authorities. Investigations involving sanctions allegations will continue to be more prevalent as sanctions are a growing foreign and security policy tool used to influence foreign behaviour and mitigate national security risks.

Parties seeking to circumvent the sanctions regulations often go to great lengths to disguise transactions using intricate payment processes, subsidiaries, intermediaries and shell corporations, among other vehicles. To combat these types of deception, organisations should implement effective sanctions compliance programmes and investigate potential sanctions violations. Thus, prudent companies will leverage cutting-edge investigative techniques, tools and consultants with specialised forensic knowledge. The purpose of this chapter is to explain key investigative procedures and best practices from a forensic accounting perspective and highlight the techniques and tools used to uncover facts and patterns in the complex web of transactions designed to circumvent economic sanctions. The

---

1 Leilei Wu is a senior manager and Bridget Johnson is a manager at BDO USA, PA. Christine Sohar Henter is a partner and Michelle Rosario is a law clerk at Barnes & Thornburg LLP. The authors would like to acknowledge the contributions of Linda Weinberg and Roscoe Howard, partners at Barnes & Thornburg LLP, and Nicole Sliger, Anthony Lendez and Pei Li Wong, partners at BDO USA, PA.

chapter provides a combination of best practices, published guidance from OFAC and recent case outcomes to provide insight on the evolving sanctions environment and to support forensic and compliance professionals in creating a sanctions compliance programme (SCP) or enhancing or testing an existing one.

OFAC guidance

OFAC's guidance document, 'A Framework for OFAC Compliance Commitments', encourages companies to 'develop, implement and routinely update' a risk-based SCP.[2] OFAC strongly recommends the adoption of an SCP by all organisations subject to US jurisdiction and foreign entities that conduct business in or with the US or US persons, or that use US-origin goods or services, use the US financial system, or process payments to or through US financial institutions. Forensic methodologies and tools are critical elements of effective compliance measures, such as risk assessments and compliance testing. For the purposes of this chapter, we focus on the two SCP components most relevant to forensics – risk assessment and testing and auditing – and how these components interplay with the factors OFAC considers in administrative enforcement actions.[3]

The risk assessment and testing and auditing components of an SCP should not be viewed in isolation, but rather should inform each other and continue to evolve. Not only is the regulatory environment constantly evolving, so too is the nature of a business. Because each company is unique, the risk assessment and testing and auditing plan should be tailored to each business. Additionally, risk assessments should be refreshed periodically to take into consideration any changes in the organisation. A properly designed risk assessment and testing and auditing cycle should minimise exposure in the event of an apparent violation. Moreover, conclusions should be analysed as part of the testing and auditing process. If testing or auditing reveal that risks are higher than anticipated in one portion of the business, these results should inform the company's overall risk assessment and compliance efforts.

---

2 See https://ofac.treasury.gov/media/16331/download?inline.

3 'A Framework for OFAC Compliance Commitments' states: 'OFAC has generally focused its enforcement investigations on persons who have engaged in wilful or reckless conduct, attempted to conceal their activity (e.g., by stripping or manipulating payment messages, or making false representations to their non-U.S. or U.S. financial institution), engaged in a pattern or practice of conduct for several months or years, ignored or failed to consider numerous warning signs that the conduct was prohibited, involved actual knowledge or involvement by the organization's management, caused significant harm to U.S. sanctions program objectives, and were large or sophisticated organizations.'

As OFAC notes, a risk assessment should consider customers, products, services, supply chain, intermediaries, counterparties, transactions and geographical locations, depending on the nature, size and sophistication of the organisation. These factors should be targeted for assessment during the testing and auditing process. When determining the appropriate administrative action in response to a sanction violation, OFAC will follow and consider certain 'general factors' described in its Economic Sanctions Enforcement Guidelines.[4]

Implementing a testing and auditing plan as part of a risk-based SCP is a mitigating factor. In addition, using key forensic procedures and analytical tools as part of a testing and auditing plan can also help reduce a company's exposure by minimising instances of aggravating conduct. For example, auditing using forensic procedures and data analytical tools on emails and shipping records can help detect and deter non-compliance by employees.

Key forensic procedures and analytical tools

Data analysis

Among the most effective investigative procedures applied in testing or investigating as part of an SCP is a statistical analysis of historical and 'real-time' transactional data. It is critical for a company to be able to identify potentially suspicious transactions and determine the 'who, what, where, when and how' by piecing together a timeline of events.

Statistical data analysis – ranging from basic pivot-table analysis to more advanced software applications and platforms to stratify, synthesise and flag data from a variety of ecosystems – is an invaluable tool. The key to effectively using data analysis is the ability to link transactional evidence buried in a multitude of data fields from disparate sources to identify hidden relationships or correlations.

With the assistance of data analytic tools, robust forensic analyses can be performed to help identify and thwart sanctions violations. The following observations from recent enforcement cases (as discussed in more detail in 'Analysis of recent enforcement cases – a forensics focus' below) could further inform efforts to prevent and detect potentially suspicious activities.

- Use keyword search terms on unstructured data to assist with data analysis. Evidence regarding prohibited transactions is frequently located in unstructured data (e.g., electronic communications, such as email, voicemail and instant messages). Forensic tools can identify suspicious activity using

4 31 C.F.R. Part 501, Appendix A, at www.ecfr.gov/current/title-31/subtitle-B/chapter-V/part-501/appendix-Appendix%20A%20to%20Part%20501.

keywords on these communications, including metadata reviews (e.g., to/from fields). These tools can also analyse system access logs to identify users who accessed the system and can then obtain internet protocol (IP) addresses and GPS coordinates of the users. Further, a company can proactively use keyword search terms across communication channels in the normal course of business to identify suspect transactions or 'code' words in real time and block those communications.

- Anticipate potential compliance risks, especially when entering new business areas, and leverage data and IT systems to automatically block transactions that violate US sanctions. For example, companies engaging in overseas transactions for the first time should proactively identify risks, including the potential for current business partners and the countries in which they operate to become subject to future sanctions. Data analytics can flag transactions and use controls such as automated restricted-party and restricted-country screening, IP address blocking and SWIFT payment analyses to prevent illegal payments, travel, shipments and services in restricted regions. Additionally, companies can improve the effectiveness of IT controls by ensuring data is complete, standardised and used consistently across the enterprise.
- Test and assess IT controls periodically to ensure they remain effective in preventing compliance violations. Compliance control breakdowns can occur as the result of weak or out-of-date algorithms that, for example, can allow close matches to Specially Designated Nationals lists to evade filters, flagged payments to be released without review or failures to flag IP addresses in sanctioned regions. For example, companies can apply text analytics and natural language processing to detect fuzzy matches. OFAC may consider a company's failure to review and improve its compliance procedures to be an aggravating factor in prosecuting compliance violations.
- Require supporting documentation for travel, shipment and payment requests to be submitted through IT approval systems, allowing automated flagging of transactions. Making it mandatory to attach supporting documents to system approval requests, such as employee expense receipts related to travel and entertainment and bills of lading related to invoices, forces requestors and approvers to substantiate the veracity of dates, locations and entity names entered into the approval system. IT systems can then perform automated matching on the verified information. For example, hotel locations supported by lodging bills can be compared to the requested travel destination to verify that travel was not to unapproved or sanctioned regions, and destinations from bills of lading can be compared to invoices to verify that deliveries and

payments did not go to entities other than those on the approved invoices. These controls also leave audit trails that are helpful in detecting trends and isolating questionable transactions.

- Verify accuracy and completeness of customers' data, including their branch information. While customers can be incorporated outside of sanctioned countries, they could maintain branches in sanctioned countries. Companies should consider requesting a complete list of branches, including all the name variations and physical addresses, from each of their customers and conducting additional due diligence on each branch. Data analysis should be considered as a way to identify discrepancies between the actual shipping addresses/payers' names and the documented data of the customer and its branches. Companies can also consider adopting master data management to standardise naming and addresses and facilitate the discrepancy analysis.
- Conduct sanctions-related due diligence prior to acquisitions. Sanctions-related due diligence is critical before acquisition of any entity, especially if the acquisition target is outside the US. Conducting interviews with all levels of employees could help companies to understand the acquisition target's compliance culture and assess employees' knowledge related to sanctions. Companies should also consider analysing all the available data at the acquisition target to detect any potential violation. Identifying violations or potential violations can help companies to voluntarily self-disclose as soon as possible and plan for targeted change in the acquisition targets' compliance governance.
- Automate and customise the training courses received by domestic and international employees. All relevant employees should have the same basic level of awareness in sanctions-related laws and regulations. Companies should consider providing online training courses with exams. Exam-scoring patterns can be analysed so companies can develop customised training programmes for employees at different subsidiaries. For example, international employees may benefit from training courses developed in the local language and extra introductory courses on US laws and regulations.
- Analyse leads from business partners for potential violations. Employees may instruct business partners to modify or hide certain details related to day-to-day transactions, such as shipments, payments and cash receipts, to circumvent compliance controls. Companies should provide channels such as dedicated email addresses, mailboxes and hotlines for business partners to report potential violations. Adopting natural language processing to analyse voice and text received should be considered as a course of action. Companies can check the leads from different channels with the internal structured and unstructured data and verify the authenticity of the leads.

Investigative due diligence

Investigative due diligence typically comprises a set of research tools and approaches that can be applied to a wide range of investigations. In sanctions-related investigations, these tools may consist of (1) documents and electronic records disclosed by a party, (2) public records gathered through desk research or on-site searches, and (3) observational site inspections or human source intelligence. Investigative due diligence arms investigators with additional knowledge to connect dots and enhance understanding of the pool of information gathered about the subject of the investigation.

Additionally, forensics professionals leverage investigative due diligence to combine data analysis with a review of pertinent open-source data about the parties involved in the activity. Open-source data (e.g., public records, such as corporate registry details, litigation records, asset ownership details and social media) can assist with untangling the web of indirect relationships and interrelated connections involved in transactions. Investigators can consider using a case tool to consolidate and analyse all the open-source data. Although the investigative trail often begins with the company's books and records, perpetrators usually engage in a variety of techniques to cover their tracks, such as layering and multiple transfers to intermediaries, shell companies, nominee shareholders and related parties. By using investigative due diligence, including reviews of public records and 'boots on the ground' interviews, investigators can uncover valuable clues regarding ownership structure and executive leadership positions of complex organisational structures.

Perpetrators may go to significant lengths to obscure beneficial ownership of companies or to disguise certain transactions, but these patterns can often be identified with common elements, such as addresses, proxies or nominees in corporate structures, or law firms or accountants used to register companies. Investigators frequently use link analysis and other visualisation tools to track the information uncovered, map the networks of bad actors, and help companies understand the potential exposure to those bad actors. Identifying patterns or connections in voluminous information requires tools to distil the information quickly and clearly into charts or graphs.

Supply chain mapping

Forensic analysis tools also enable the use of models for predictive analysis and present opportunities for global supply chain mapping. This mapping offers the possibility to identify the sanctions risk posed by third parties, such as suppliers,

distributors, agents, sub-agents and customers who may be conducting business directly or indirectly with sanctioned countries or regions or whose activities benefit sanctioned governments or sanctioned parties.

When supply chains extend to countries that actively trade with sanctioned jurisdictions, the sanctions risk may be elevated. Some primary examples of these relationships include Colombia and Venezuela, China and North Korea, and the United Arab Emirates and Iran. Assessing the potential third-party risk of relationships should be a process in which data analysis and models are continually updated with new information taken from the latest enforcement actions, in addition to published advisories from the US State Department, the US Treasury Department or other regulatory authorities.

The investment made to develop a supply chain risk map will produce longer-term benefits, especially for larger, complex enterprises and those with a multinational presence. The insight gained through supply chain mapping for sanctions risk will help in designing effective internal controls, training programmes and due diligence practices.

Predictive analysis

Once a supply chain is mapped for sanctions risk, predictive modelling can be leveraged with a global SCP to identify emerging trends in the evolving global sanctions landscape. For example, enterprises that deliver fourth-party or fifth-party logistics services[5] can enhance their existing contingency plans by incorporating sanctions risks in their supply chain mapping. Predictive analysis can highlight counterparties and relationships that may need to be re-evaluated or replaced in the event of a sanctions-related disruption, such as a sanctions designation or significant enforcement action. Although not widely adopted, a growing number of companies are using predictive analytics.

Leveraging key forensic procedures and analytical tools, such as those described above, will assist in building a 'best-in-class' SCP. Due to the exponential growth of international transactions, reliance on manual compliance controls alone can no longer effectively protect organisations against costly enforcement actions or other risks associated with sanctions violations.

5 In using fourth- and fifth-party logistics service providers, companies outsource a majority of, or nearly all, logistics management activities. As more of the supply chain logistics function is performed by an external party rather than the company itself, compliance risk increases.

On-site interviews and inspections

Forensic investigations rely heavily on historical records to identify relevant facts and support conclusions. Interviews or on-site observations provide additional context on collected data or evidence to validate authenticity and confirm facts and circumstances leading up to the recording of transactions. In-person observation of body language can also be very valuable, especially in potentially sensitive situations involving possible wrongdoing. For this reason, on-site interviews or inspections present unique opportunities for compliance personnel, investigators or those engaged to perform related testing.

In practice, in-person interviews can help investigators evaluate employees' compliance policy knowledge and the effectiveness of training, which may shed light on documented decisions made by those employees. This can potentially distinguish intentional violations of policy from decisions made because of deficient training or human error. These 'in-person' meetings provide first-hand knowledge of how written policies and procedures are operating. In some cases, disparities between the written procedure and its execution might point to gaps in the procedure. Process walk-throughs can also detect procedural steps skipped by employees taking 'shortcuts'. Interviewees can articulate why certain procedures were not performed and describe pain points or process inefficiencies that exist, highlighting the need for policy updates or additional controls.

Field interviews and observations can also detect instances when compliance processes are viewed as unimportant by employees or management or are not adequately supported by funding, necessary equipment, information technology infrastructure or staffing. These observations may indicate an overall lack of management commitment to the programme or a failure to anticipate external stresses. For example, employees in economically developing countries, where disruptions to internet service (or even electrical power) are commonplace, may default to unapproved workarounds or off-system processes, which result in incomplete system data and failures to apply controls.

Irrespective of geography, protracted crisis may result in lengthy business interruption, high staff turnover or absenteeism. Employees may be unable to access their work location because of civil unrest, natural disaster or other widespread disruption, as exemplified by the covid-19 pandemic, the Myanmar military coup in 2021 and the Russian invasion of Ukraine in 2022. Thus, expertise or resources required to fully execute the SCP may not be available, and employees may find themselves under increased pressure to ignore processes for the sake of business continuity. Sanctions compliance should influence the crisis response and business

continuity plans for sophisticated, global organisations. Advanced planning and on-site walk-throughs help to provide a clearer picture in understanding potential risks, which may not be anticipated or detected during a crisis.

In situations where on-site procedures cannot be performed, such as because of travel constraints that were brought on by the covid-19 pandemic, interviews and inspections conducted remotely can provide satisfactory results when investigators adhere to best practices. Video conferencing allows the interviewer to gauge the interviewee's body language and facial expression, may help to put the interviewee at ease and can provide a solution for remote sharing of documents on a shared screen. The use of mobile devices to allow a view of facilities can be effective when an in-person inspection is not possible. However, investigators generally have a limited view when a mobile device is used and the person who holds the mobile devices can manipulate what can be viewed by investigators. Investigators need to be aware of these pitfalls when conducting remote procedures and may want to consider using an independent third-party observer physically on-site when possible. A keen awareness of relevant data protection or privacy laws and regulations, state and commercial secrecy laws and employment regulations is key to successful remote interviews and inspections.

For remote interviews, interviewers should be alert to the possibility of other individuals in the same room who may be listening in or coaching the interviewee. An interviewee may try to avoid being interviewed or answering questions by claiming technical difficulties. Remote interviews also run the risk of being recorded surreptitiously. During virtual tours of facilities and premises, investigators should expect areas of interest to the team to be intentionally excluded from the tour. If permissible, investigators can arrange to have local colleagues be present in person during remote procedures to mitigate these risks.

Data preservation and collection activities are major activities in an investigation. Forensics practitioners collect data from servers and devices, such as smartphones, laptop computers, hard drives and other portable drives (e.g., flash drives). While remote collection of server data is a common industry practice, collecting data from other devices in a forensically sound way may require shipping of these devices and is often challenging and slow, especially in times when global logistics services are overextended; for example, during the covid-19 pandemic.

Many organisations still rely heavily on hard copy documentation to conduct business. Often, the need to maintain a hard copy paper trail is driven by local government requirements and business norms in the country. Organisations may scan hard copy documents for electronic storage, but the quality of the scan is often inconsistent and scanned images are at risk of being altered. Best practice is to follow up with an on-site examination of the original hard-copy

documentation whenever possible. Companies should consider digitising the hard copies used in the business processes and managing the digitised data for easy retrieval and analysis.

One major limitation of remote procedures is the inability to conduct unscheduled interviews or surprise 'spot checks'. These cannot be performed remotely, mainly because of the coordination and logistics arrangements required to organise remote data collection, interviews or facilities inspections.

Ultimately, proper planning is key, and communication of expectations to the subject entity or individual helps reduce misunderstandings over logistics. Where possible, the investigations team should corroborate preliminary results from the remote investigative procedures by supplementing the work conducted with an in-person inspection when travel is feasible.

Potential post-investigation procedures

An investigation should conclude with a final report containing findings. An opportunity exists to convert findings into formalised action plans to remediate any deficiencies. For example, when gaps in compliance knowledge are revealed, the organisation should implement role-specific or targeted training. A finding that screening systems failed to detect name variations may result in adjustments to the configuration of the screening system. Still other findings may require enterprise-wide initiatives and policy development.

Specific compliance errors uncovered through transaction analysis and forensic techniques, such as look-backs, are also useful to isolate incorrect compliance decisions and enhance existing training programmes and materials. The circumstances surrounding the errors are useful in forming situation-based questions and case studies for training materials, internal discussions and employee evaluations. Studying the various types of errors may also be helpful in creating automated system-generated policy reminders to help employees in following the correct steps to avoid future violations.

Action plans should include identification of responsible parties, follow-up timelines, and procedures with features, such as scheduled action plan updates; retraining or retesting of employees; follow-up sampling of transaction activity to test controls; updated or enhanced risk assessments; and targeted disciplinary actions such as probationary periods or re-evaluation of contracts with external parties. Follow-up activities associated with an action plan should also be documented and records retained according to written policy and legal standards.

Analysis of recent enforcement cases – a forensics focus

Examining recent cases and outcomes offers insight into trends within the evolving sanctions landscape. This context is important to demonstrate the application of various forensic investigative methods and best practices, while also highlighting the practices that might have contributed towards the identification of mitigating factors considered by OFAC.

Godfrey Phillips India

On 1 March 2023, Godfrey Phillips India (GPI), a tobacco manufacturer based in Mumbai, India, settled this case[6] with a payment of US$332,500. GPI used the US financial system to receive payments totalling approximately US$360,000 for tobacco it indirectly exported to North Korea in 2017. For the US financial institutions to fulfil the transactions, GPI used several third-country intermediary parties to obscure the connection with North Korea, causing US financial institutions to clear the payments. In an email exchange, GPI employees also decided not to include 'North Korea' or the North Korean customer's details on any trade document, but merely referenced the intermediary with a third country as the generic destination.

The case demonstrates the importance of comprehensive compliance programmes for foreign entities engaging in financial transactions processed through US financial institutions. Robust compliance programmes can help foreign entities understand potential US sanctions risks. The case also highlights the importance of companies using keyword search terms across communication channels to identify and suspend suspicious transactions promptly. Finally, it emphasises the necessity to implement effective compliance training, which keeps employees updated on the rapidly changing risk environment.

Payward, Inc

Payward, Inc (doing business as Kraken), a Delaware incorporated global virtual currency exchange, agreed to pay US$362,158.70 to settle this case[7] in November 2022. Kraken's platform allows users to buy, sell or hold cryptocurrencies, trade those currencies for fiat currency or exchange one cryptocurrency for another. Although Kraken maintained controls designed to prevent users from opening an account while in a sanctioned jurisdiction, it did not implement similar IP address blocking on transactional activity facilitated on its platform,

6 See https://ofac.treasury.gov/recent-actions/20230301_33.

7 See https://ofac.treasury.gov/recent-actions/20221128.

which caused Kraken to process 826 transactions totalling approximately US$1.6 million on behalf of users residing in Iran in apparent violation of the Iranian Transactions and Sanctions Regulations. After identifying this problem, Kraken implemented automated blocking for IP addresses linked to sanctioned jurisdictions and adopted multiple blockchain analytics tools to assist in sanctions compliance.

This case illustrates the importance of using geolocation tools, including IP address blocking and other location verification tools, to identify and prevent illegal transactions in restricted regions. It also demonstrates the importance of regular internal auditing and testing to identify deficiencies in existing compliance policies. Another lesson from this case is that a company should implement robust remedial measures after becoming aware of potential sanctions issues and the shortcomings of data analysis tools and analytics, then commit to continuous sanctions compliance investments as technology evolves.

CA Indosuez (Switzerland) SA and CFM Indosuez Wealth

CA Indosuez (Switzerland) SA (CAIS) and CFM Indosuez Wealth (CFM) are both indirect subsidiaries of Credit Agricole Corporate and Investment Bank. In September 2022, CAIS and CFM agreed to settle their potential civil liability for approximately US$750,000 and US$400,000, respectively, for apparent violations of Cuba, Iran, Syria, Ukraine-related and Sudan sanctions programmes.[8] CAIS and CFM's compliance procedures included collecting customers' data for know-your-customer purposes, which includes address information revealing the location of account holders that reside in sanctioned countries. Despite having this data, from April 2013 to April 2016 CAIS processed a total of 273 transactions (security procurements and commercial transactions), totalling over US$3 million through US banking correspondents, on behalf of the 17 individuals located in Iran, Syria, Sudan, Cuba and the Crimea region of Ukraine. Similarly, CFM also failed to address the known risks from December 2011 to 2016 by allowing 11 individuals residing in Iran, Syria and Cuba to conduct 426 transactions (security procurements and commercial transactions) worth over US$1.2 million. Although both companies implemented internal restrictions designed to prevent certain payments to persons residing in sanctioned regions, they later discovered that their internal restrictions did not prevent securities-related payments from being made to certain accounts. CAIS and CFM later implemented measures to prevent these payments.

8 See https://ofac.treasury.gov/recent-actions/20220926_33.

This case highlights the importance of integrating customer data into companies' compliance screening process to ensure all collected information informs compliance. It also demonstrates the value of testing and auditing controls to identify gaps in controls and compliance policies, and proactively implementing remedial actions.

Banco Popular de Puerto Rico

Banco Popular de Puerto Rico (BPPR), a Puerto Rican bank with branches in Puerto Rico and the Virgin Islands, settled its potential civil liability with OFAC for processing over 300 transactions totalling over US$850,000 on behalf of two low-level government of Venezuela employees in apparent violation of Venezuela-related sanctions in May 2022.[9] On 5 August 2019, Executive Order (EO) 13884 blocked property and interests in property of the Venezuelan government, which included:

- 'any political subdivision, agency, or instrumentality';
- 'any person owned or controlled, directly or indirectly', by the Venezuelan government; and
- 'any person who has acted or purported to act directly or indirectly for or on behalf of' any government entity.

EO 13884 was incorporated into the amended Venezuela Sanctions Regulations (VSR) on 22 November 2019.

Shortly after the issuance of EO 13884, BPPR began reviewing accounts that might be affected by the Order, but it took the bank 14 months to block four personal accounts of two customers employed by the government of Venezuela. When EO 13884 was announced, BPPR identified one customer working in the Diplomatic Representation Office of the Venezuelan government and the other account holder employed by a Venezuelan state-owned entity. BPPR's delay in identifying these customers resulted in the processing of 337 prohibited transactions totalling US$853,126, which violated the VSR. With OFAC's consideration of the aggravating and mitigating factors, BPPR agreed to a settlement payment of over US$255,000.

This case illustrates to financial institutions the importance of taking swift action following the issuance of new sanctions-related prohibitions. While BPPR had documentation of the customers' government connections, the company did not block the accounts for more than a year after the Executive Order was issued.

9 https://ofac.treasury.gov/recent-actions/20220527_33.

To be more agile to an evolving regulatory risk environment, companies should proactively surface key information from documents, such as government relationships, and convert this data into a structured format. Having this information readily available enables companies to perform timely due diligence and respond more rapidly to government sanctions.

Toll Holdings Limited

An international freight forwarding and logistics company headquartered in Australia, Toll Holdings Limited, settled more than 2,000 apparent violations of multiple OFAC sanctions programmes by agreeing to pay a settlement of over US$6 million.[10] For six years, from January 2013 to February 2019, Toll was involved in nearly 3,000 payments related to shipments involving three sanctioned countries – specifically, North Korea, Iran and Syria. Some of these payments also involved the property or interests of property of an entity on OFAC's Specially Designated Nationals and Blocked Persons List. Both types of payments were processed through at least four financial institutions in the US or through foreign branches of US-based financial institutions and totalled approximately US$48 million.

Toll had expanded rapidly through acquisition, and, as a result, the business included numerous legacy freight forwarding companies in regions around the world. Notably, by 2018, Toll had nearly 600 different IT systems spread across its business. The sanctioned activity was commonly initiated by Toll's overseas units, altogether comprising 23 different Toll entities across Asia, Europe, the Middle East and North America. During its normal course of operations, Toll engaged in complex payment practices, such as making or receiving payments for multiple shipments in a single invoice or spreading one shipment across multiple invoices. In these cases, the value of the payment amount associated with a sanctioned country or entity could be a portion of a larger amount comprised of both sanctioned and non-sanctioned parties.

Around May 2015, some Toll personnel were put on notice that the subject payments were in potential violation of US sanctions regulations when one of its banks restricted a Toll subsidiary's use of its US account after identifying a transaction with Syria. However, despite instruction from its compliance office that Toll must not be involved with any shipments to US-sanctioned jurisdictions, the activity continued, and it was not until years later that Toll implemented 'hard controls' to block these illegal shipments and payments. These controls included

10 https://ofac.treasury.gov/recent-actions/20220425.

disabling the country and location codes for ports and cities to or from sanctioned countries in its freight management system, thereby preventing its shipments from transiting in sanctioned countries.

This enforcement action emphasises the necessity for companies to continually examine the effectiveness of their internal controls as their business expands and the crucial role that IT systems play in ensuring compliance. While Toll had compliance policies, sanctioned activity was able to occur in part due to lack of system controls. While policies are a necessary aspect of a compliance programme, companies should also regularly assess whether those policies can be 'hard coded' as part of their IT system configuration. Furthermore, companies should use data analytics to continually monitor the transactional activity that flows through these systems to identify any compliance concerns and address sanctions risks in a timely manner.

British American Tobacco plc

OFAC's largest-ever settlement with a non-financial company was with British American Tobacco plc (BAT), an English tobacco and cigarette manufacturer that agreed to pay over US$500 million to settle alleged violations of sanctions against North Korea.[11] BAT established an elaborate payment scheme for approximately US$250 million in over 200 payments from a North Korea joint venture, through blocked bank accounts in North Korea to BAT's Singaporean subsidiary, which implicated US banks clearing the transactions between 2009 and 2016. BAT's apparent violations occurred because the US-dollar-denominated payments for its exports of tobacco to the North Korean Embassy in Singapore cleared through the US financial system.

The penalty was the maximum statutory civil amount permitted (e.g., twice the value of the sum of transactions), reflecting OFAC's finding that these apparent violations were egregious and not voluntarily disclosed. The main lesson from this case is that companies that knowingly engage in conspiracies that cause US persons to be involved in prohibited transactions, including dealing with blocked persons, risk receiving severe penalties. Further, without a culture of compliance driven by senior management and suitable compliance policies and controls, which must be reassessed when regulations evolve, these companies have heightened risk for potential violations.

11 https://ofac.treasury.gov/recent-actions/20230425.

Sanctions compliance: best practices and lessons learned

Former US Deputy Attorney General Paul McNulty issued a warning at a 2009 conference that has become a popular maxim within compliance circles even more than a decade later: 'If you think compliance is expensive, try non-compliance.'[12] Sanctions compliance violations are among the costliest ways this lesson is learned. OFAC maintains the most active and extensive sanctions programme in the world. OFAC's recent output has included a steady flow of new regulations, guidelines and enhanced reporting requirements for rejected transactions.

It is worthwhile remembering that OFAC considers 'good faith' compliance efforts in the disposition of enforcement matters. OFAC 'will consider favorably subject persons that had effective SCPs at the time of an apparent violation'.[13] However, there is no way to predict how OFAC will apply this principle to individual cases, so compliance professionals and organisational leaders should not assume their efforts will result in mitigation of penalties.

OFAC's advice in the 'Framework for OFAC Compliance Commitments', and echoed here, can be traced to cases in which at least one of the five commitment areas was deficient. Focusing on the forensic and investigatory lessons that can be gleaned from the cases referenced herein, below is a series of emphatic dos and don'ts, from a forensics perspective, for building an effective SCP, testing an existing programme or conducting sanctions investigations.

Do . . .

Sanctions compliance programme:

- conduct comprehensive risk assessments;
- implement risk-based, straightforward policies, procedures and internal controls relevant to day-to-day operations and sanctions concerns; and
- enforce policies and procedures, and identify, document and remediate weaknesses.

12 Rodney T Stamler, Hans J Marschdorf and Mario Possamai, *Fraud Prevention and Detection: Warning Signs and the Red Flag System* (Routledge, 2014), p. 4.

13 See https://ofac.treasury.gov/media/16331/download?inline.

Due diligence and screening:

- conduct due diligence on customers, distributors, suppliers, contractors, logistics providers, financial institutions and other partners;
- use and test automated screening software continuously, being cognisant of filter faults – prioritise alerts by severity and tune configuration of the software as needed;
- utilise systems to track movement of goods and financial transactions from manufacturing to end user;
- deploy blockchain and distributed ledger technologies to improve due diligence records;
- understand circumvention risk;
- monitor recent enforcement actions for effects on operations; and
- establish anonymous reporting channels for employees and policies to ensure non-retaliation for whistle-blowing.

Testing and auditing:

- assess tools, technology and data needed to monitor sanctions compliance;
- consider artificial intelligence to detect red flags – calibrate and test routinely;
- apply forensic investigative techniques on structured and unstructured data and metadata;
- conduct regular internal compliance audits, including at crucial junctures; for example, mergers, acquisitions and management changes;
- conduct supply chain audits with country-of-origin verification; and
- perform supplier and distributor audits.

Don't . . .

- conceal violations;
- facilitate transactions by non-US persons (including through or by non-US subsidiaries or countries);
- utilise US financial systems or process payments to or through US financial institutions for transactions involving sanctioned persons or countries (including US dollar payments); or
- utilise non-standard payments and commercial practices.

Conclusion

The area of sanctions compliance continues to grow in importance and simultaneously challenge the programmes, tools and talents of legal, compliance and forensics professionals. As the international political trends and criminal activities driving the use of sanctions show no signs of disappearing, and worldwide economic instability continues to show vulnerabilities in the global value chain, the advantage of establishing a robust and proactive SCP could provide a significant measure of protection against potential violations. By focusing on the core commitment areas described in the OFAC guidance, drawing from best practices and tools used by forensics professionals, and studying relevant case outcomes, enterprises seeking to mitigate sanctions risk can do so with confidence that those efforts will pay off in the long term.

CHAPTER 23

Representing Designated Persons: A UK Lawyer's Perspective

Anna Bradshaw and Alistair Jones[1]

Introduction

Lawyers advising on sanctions must not only navigate the risks their clients face, but also manage their own risks when providing legal services. Just as professionals must guard against the misuse of legal services in other contexts, sanctions lawyers must take care to understand who their clients are and why they are seeking legal advice. As a general rule, the provision of legal services would not breach sanctions. There are, however, increasing circumstances in which legal services could amount to prohibited or restricted activity and may require a prior licence.

Where legal services are sought for unlawful purposes, such as to commit, conceal or disguise a sanctions breach, it would clearly be improper for the lawyer to act. The general guidance on financial sanctions produced by the UK's Office of Financial Sanctions Implementation (OFSI) warns lawyers to carefully consider whether their legal advice is properly helping a client to comply with sanctions or amounts to improper participation in, or facilitation of, a sanctions breach. To illustrate the point, OFSI distinguishes between permissible advice to a client on the effects on business of prohibitions against raising capital on financial markets and assistance in preparing documents to raise the capital; the latter may amount

1 Anna Bradshaw is a partner and Alistair Jones is a senior associate at Peters & Peters Solicitors LLP.

to an attempt to circumvent sanctions.[2] OFSI's separate enforcement guidance makes it clear that failure by regulated individuals to meet regulatory and professional standards may be considered an aggravating feature of a financial sanctions breach.[3]

The need to combat the perceived involvement of lawyers and other professionals in sanctions evasion and circumvention has emerged as a political priority. In March 2022, a Russian Elites, Proxies and Oligarchs Task Force was set up by the G7 members, the European Union and Australia, to take action against the assets of key Russian elites and proxies and to act against their enablers and facilitators.[4] In support of this initiative, the UK's National Crime Agency has established a Combatting Kleptocracy Cell to investigate sanctions evasion, with a specific focus on professional enablers.[5] The UK's Economic Crime Plan for 2023-2026 identifies driving down sanctions evasion as a key priority, and commits to identifying and disrupting the enablers who are knowingly complicit in assisting elites to evade sanctions.[6] Finally, there have been calls for lawyers to be designated as sanctions targets on account of their provision of legal advice to, and representation of, clients in connection with specific forms of legal

2 Office for Financial Sanctions Implementation (OFSI), 'UK financial sanctions: General guidance for financial sanctions under the Sanctions and Anti-Money Laundering Act 2018', August 2022, paragraph 6.6.1, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1173762/UK_Financial_Sanctions_General_Guidance.pdf.

3 OFSI, 'OFSI enforcement and monetary penalties for breaches of financial sanctions: Guidance' (31 August 2023), paragraph 3.21, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1181296/Monetary_Penalty_and_Enforcement_Guidance__Aug_2023_.pdf.

4 'Russian Elites, Proxies, and Oligarchs Task Force ministerial joint statement', 16 March 2022, available at: https://home.treasury.gov/news/press-releases/jy0663.

5 National Crime Agency, SARs In Action, Issue 15, March 2022, p. 8, available at: https://nationalcrimeagency.gov.uk/who-we-are/publications/591-sars-in-action-march-2022/file.

6 HM Government, 'Economic Crime Plan 2: 2023–2026', paragraph 3.10, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1147515/6.8300_HO_Economic_Crime_Plan_2_v6_Web.pdf.

proceedings.[7] A number of lawyers have already been designated on account of their provision of legal services outside the UK in circumstances that have engaged designation criteria.[8]

When coupled with public criticism of law firms and individual lawyers for acting for specified categories of clients, including sanctioned clients, these developments may discourage law firms and individual lawyers from representing designated persons or advising clients who are located in, or otherwise connected in some way with, sanctioned regimes. A further 'chilling' effect is likely to result from the increase in scrutiny of, and by, professional regulators and representative bodies in this connection. According to a paper published by the Legal Services Board in July 2022, regulators have been encouraged to be more 'curious' about the risks and challenges in their respective sectors, including by 'making appropriate enquiries of those who have been or may be involved in supporting sanctioned individuals and their wider networks'.[9]

In its guidance on the Russian sanctions regime, the Solicitors Regulation Authority (SRA) advises firms that they can decline instructions from clients they do not feel comfortable acting for, provided that the reason is not unlawful, whether under equalities legislation or otherwise.[10] Whether a current retainer is terminated for 'good reason' is ultimately a question of common law for the courts to determine on a case-by-case basis. In the SRA's separate guidance on compliance with UK sanctions, law firms are advised to include, in terms of business or equivalent, 'becoming a designated person' as a valid reason for ending the

---

7 Jonathan Ames, 'Deny visas to oligarchs' British lawyers', *The Times*, 19 April 2022, available at: www.thetimes.co.uk/article/deny-visas-to-oligarchs-british-lawyers-tg5g6dkjj; Stephanie Kirchgaessner and Julian Borger, 'Calls for US to issue visa bans for UK lawyers enabling Russian oligarchs', *The Guardian*, 16 April 2022, available at: www.theguardian.com/us-news/2022/apr/16/calls-for-us-to-issue-visa-bans-for-uk-lawyers-enabling-russian-oligarchs.

8 e.g., Russian lawyers Yulia Mikhailovna Maiorova (UK Sanctions List Ref: GAC0014) and Andrei Alekseevich Pavlov (UK Sanctions List Ref: GAC0007) were both designated on 26 April 2021 as asset freeze targets under the Global Anti-Corruption Sanctions Regulations 2021 for facilitating or providing support for serious corruption, described in the Statement of Reasons as having participated in a fraud through their involvement, in particular, in court processes based on fraudulent claims for damages.

9 Legal Services Board, 'Financial sanctions and legal services', Paper (22) 39, 19 July 2022, available at: https://legalservicesboard.org.uk/wp-content/uploads/2022/07/04.-Paper-22-39-Sanctions-update-.pdf.

10 Solicitors Regulation Authority (SRA), News Release, 'Russian Conflict and Sanctions', 4 March 2022, as updated 15 March 2022, available at: www.sra.org.uk/sra/news/russian-conflict-and-sanctions/.

business relationship and ceasing to provide services.[11] Firms that choose to work in the area of sanctions are warned to seriously consider the risks and how they will address them before offering any services. The guidance further advises firms acting for designated persons to check whether their bank and insurers will continue to provide their services, in addition to considering reputational and regulatory risk.

The ability of a designated person to access legal representation is, however, a fundamental element of the rule of law. Access to legal advice is necessary to ensure that sanctions prohibitions and restrictions are understood and complied with. All asset freezes adopted by the UN, EU and UK to date are understood to have allowed licences or other forms of authorisation to be granted to permit frozen funds to be used by designated persons in payment of their legal fees.[12] The Explanatory Notes to the Sanctions and Anti-Money Laundering Act 2018 (SAMLA) confirm that licensing grounds for the purpose of the UK's new autonomous sanctions may include reasonable professional fees and the reimbursement of reasonable and necessarily incurred expenses associated with the provision of legal services;[13] and all regulations adopted under SAMLA have expressly included provisions to this effect. The types of legal services that can be licensed for this purpose are unrestricted under SAMLA, but OFSI's general guidance states that legal fees and disbursements must relate specifically to the provision of legal advice or involvement in litigation or dispute resolution.[14] A further, more recent, policy decision announced on 30 March 2023 now also restricts the types of contentious legal advice and representation available to persons designated as asset freeze targets. Following an internal review by HM Treasury, the UK government has concluded that in most cases, the use of frozen funds for payment of legal professional fees for defamation cases is not an appropriate use of funds, and in many cases will be against the public interest.[15] While OFSI will continue to review individual applications on a case-by-case basis for both appropriateness

11 SRA, Guidance, 'Complying with the UK Sanctions Regime', 28 November 2022, available at: www.sra.org.uk/solicitors/guidance/financial-sanctions-regime/.

12 See, e.g., the Council of the European Union, 'Guidelines on Implementation and Evaluation of Restrictive Measures (Sanctions) in the Framework of the EU Common Foreign and Security Policy', as updated 8 December 2017, at paragraph 25.

13 Sanctions and Anti-Money Laundering Act 2018 (SAMLA), Explanatory Notes, Paragraph 65(c), available at: www.legislation.gov.uk/ukpga/2018/13/notes.

14 id., Paragraph 6.5.

15 UK Parliament, Written questions, answers and statements, '[OFSI] update: Statement made on 30 March 2023', Statement UIN HLWS686, available at: https://questions-statements.parliament.uk/written-statements/detail/2023-03-30/hlws686.

and compliance with the right to a fair hearing, it will now apply a presumption that applications for legal fees licences relating to defamation and similar cases will be rejected.[16] In accordance with this policy, OFSI's general licence for the purposes of the Russia and Belarus sanctions regimes excludes fees and disbursements incurred in connection with the provision of legal advice or representation in court, anywhere in the world, in relation to a claim for defamation or malicious falsehood.[17]

The legal services that designated persons are expected to seek fall into three broad categories. First, designated persons will seek legal advice for the same reasons as anyone: to exercise their legal rights and to protect their lawful interests, which may be unrelated to their status as designated persons. Second, designated persons would be expected to seek sanctions compliance advice to understand their obligations under the prohibitions and restrictions that apply to them, and to obtain assistance with licence applications. Finally, designated persons may seek legal advice and representation in order to request a variation to, or a revocation of, their designation.

This chapter identifies some of the main issues that are likely to arise in the legal representation of designated persons in the UK.

Legal services prohibition

Trade sanctions now directly target the provision of legal services under one of the SAMLA sanctions regimes, following the introduction of Regulation 54D to the Russia (Sanctions) (EU Exit) Regulations 2019.[18] With effect from 30 June 2023, any person subject to UK sanctions jurisdiction is prohibited from directly or indirectly providing non-contentious legal services to any person who is not a UK person, which relates to activity that would breach any specified provisions of the Russia sanctions regime if carried out by a UK person or taking place in the UK (regardless of whether there is such a jurisdictional nexus to the activity). On 11 August 2023, a general trade licence was adopted by the Department of Business and Trade to clarify that the exception for compliance advice also applies

16 Letter from Baroness Penn to Alicia Kearns MP, chair of the Foreign Affairs Committee, House of Commons, 18 April 2023, available at: https://committees.parliament.uk/publications/39307/documents/192902/default/.

17 OFSI General Licence under the Russia Regulations and the Belarus Regulations, INT/2023/2954852, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1153971/Legal_Services_GL_INT20232954852.pdf.

18 Russia (Sanctions) (EU Exit) (Amendment) (No. 3) Regulations 2023, S.I. 2023/713.

where it relates to the sanctions laws and criminal laws imposed by any jurisdiction, including Russian counter-sanctions. Anyone seeking to rely on it must register via the online export licensing system, SPIRE, within 30 calendar days, and relevant records (other than privileged information) must be kept and made available on request for a period of four years. For prohibited legal advice falling outside the scope of the general trade licence, a standard individual export licence may be granted if licensing grounds would apply to the activity in relation to which the legal advice is being given. Applicants are advised to explain how the continued provision of otherwise prohibited legal services is consistent with the aims of the sanctions, and the impact or implications if the services could not be provided.[19]

The legal services prohibition is not likely to be engaged in connection with work for designated persons because it does not apply to any representation, advice, preparation or verification of documents undertaken as part of legal representation services provided in, or in anticipation of, any proceedings before administrative agencies, courts or other duly constituted official tribunals or arbitral or mediation proceedings.[20] Legal representation services are defined to include advice given in relation to a dispute or potential dispute, and on the settlement of a dispute, whether or not proceedings are commenced in relation to the dispute. The press release accompanying the introduction of the provision confirmed that legal representation of Russian nationals using UK legal expertise remains permitted, ensuring that allowing everyone to access legal support remains a core aspect of the rule of law across the UK.[21] Nonetheless, the prohibition is likely to exert a further 'chilling' effect on the willingness of UK lawyers to act for designated persons. The stated objective of the prohibition reinforces the perception of lawyers as enablers of sanctions evasion and circumvention. When the government first announced its intention to restrict access to 'transactional

19 Department of Business and Trade (DBT), 'Guidance: Complying with professional and business services sanctions related to Russia', updated 30 June 2023, available at: www.gov.uk/government/publications/professional-and-business-services-to-a-person-connected-with-russia/professional-and-business-services-to-a-person-connected-with-russia.

20 Russia (Sanctions) (EU Exit) Regulations 2019, Paragraph 8A of Schedule 3J.

21 Press Release, HM Government, 'New law imposes fresh sanctions on Russia using UK legal expertise', 29 June 2023, available at: www.gov.uk/government/news/new-law-imposes-fresh-sanctions-on-russia-accessing-uk-legal-expertise.

legal advisory services for certain commercial activity' on 30 September 2022,[22] the aim was described as hampering the ability of Russia's businesses to operate internationally. When the prohibition was adopted nine months later, it was presented as plugging a perceived loophole that would otherwise potentially permit UK legal services providers to support commercial activity that advances the interests of Russia where those activities are not conducted in the UK or by UK persons.[23] The statutory guidance on the Russia sanctions regime similarly describes the legal services prohibition as supplementary to the prohibitions on circumventing financial and trade sanctions,[24] and the separate guidance on the professional and business services prohibitions also refers to the limitations on ancillary services more broadly.[25]

Legal fees licences

A legal fees licence is not a prerequisite for legal advice or assistance to be provided to a designated person. The provision of legal services cannot directly or indirectly make economic resources available to a designated person in breach of an asset freeze if the designated person is not likely to exchange legal services for, or use legal services in exchange for, funds, goods or services.[26] It is equally difficult to see how the provision of legal services, in itself, could be considered to make economic resources available for the benefit of a designated person, in the sense that the designated person thereby obtains (or is able to obtain) a significant financial benefit, including the discharge (or partial discharge) of a financial obligation for which they are wholly or partly responsible.

---

22 Press Release, HM Government, 'Sanctions in response to Putin's illegal annexation of Ukrainian regions', 30 September 2022, available at: www.gov.uk/government/news/sanctions-in-response-to-putins-illegal-annexation-of-ukrainian-regions.

23 Explanatory Memorandum to the Russia (Sanctions) (EU Exit) (Amendment) (No. 3) Regulations 2023, available at: www.legislation.gov.uk/uksi/2023/713/pdfs/uksiem_20230713_en_001.pdf.

24 HM Government, 'Statutory guidance, Russia sanctions: guidance', updated 11 August 2023, available at: www.gov.uk/government/publications/russia-sanctions-guidance/russia-sanctions-guidance.

25 DBT, 'Guidance: Complying with professional and business services sanctions related to Russia' (footnote 19).

26 Section 60(2) of SAMLA defines 'economic resources' as assets of every kind, whether tangible or intangible, movable or immovable, which are not funds but can be used to obtain funds, goods or services.

OFSI's general guidance confirms that a licence is not required to provide legal advice to, and act for, a designated person; although lawyers are strongly encouraged to apply for a licence in advance of providing substantive legal services to have certainty as to the fees that will be recoverable while the designated person remains listed.[27] The SRA's compliance guidance similarly advises that unpaid work can be undertaken provided it does not circumvent the sanctions regime or provide financial advantage to the designated person.[28]

The only exception to this general rule is where legal services are paid for and provided 'on credit', which in OFSI's view would require a licence.[29] In the absence of any explanation it is unclear what is meant by the provision of legal services on credit. OFSI's guidance is clearly predicated on the assumption that licences will be sought and granted for legal services already rendered, and OFSI routinely grants legal fees licences to permit lawyers to issue bills on this basis.

A legal fees licence permits the use of frozen assets as payment for legal services or the use of unfrozen funds as payment for legal services rendered to a designated person. In other words, regardless of who pays, a licence is required to receive payment for any work on behalf of a designated person and any related disbursements. Interestingly, although court fees will ordinarily be considered a disbursement related to the provision of legal services, OFSI's general guidance suggests that a licence is only required if court fees are 'significant', which is a question of fact. By contrast, OFSI expects a legal fees licence to be sought before any payment is made into court as security for costs. OFSI takes the view that some licensing ground other than legal fees needs to be identified to pay security for damages into court, and the ground that will apply depends on the specific circumstances of the case.[30]

The issues that typically arise in practice include the considerable length of time it can take for legal fees licence applications to be processed, the amount of information that must be disclosed to OFSI as part of the application process and the ongoing compliance risks once the licence has been issued. Breaches of licence conditions are strict liability criminal offences and any ongoing reporting requirements imposed in a legal fees licence must be carefully monitored.

---

27 OFSI, 'UK financial sanctions: General guidance for financial sanctions under the Sanctions and Anti-Money Laundering Act 2018' (footnote 2), paragraph 6.5.

28 SRA, Guidance (footnote 11).

29 OFSI, 'UK financial sanctions: General guidance for financial sanctions under the Sanctions and Anti-Money Laundering Act 2018' (footnote 2), paragraph 6.6.1.

30 id., paragraph 6.6.2.

Further issues are likely to arise following a policy position adopted by OFSI on 12 July 2023 to no longer engage with applicants where it considers an application to contain insufficient details or evidence. Applications that do not demonstrate that the criteria of the licensing grounds have been met or provide sufficient evidence will be deemed incomplete and returned to the applicant for resubmission.[31] OFSI's blog post clarifies that applicants will be able to reapply, but this will be treated as a new application and will not be prioritised purely because it has been resubmitted.[32] OFSI's blog post further advises applicants to consider taking independent legal advice before applying, especially for complicated matters. A separate policy position adopted by OFSI on 26 July 2023 removes the option for applicants to request OFSI to review a decision to refuse a licence.[33] The only remaining options for unsuccessful applicants are to apply to challenge OFSI's decision in court under Section 38 of SAMLA or to reapply for a licence, with new or supplementary evidence and new supporting documents or on different licensing grounds.

General legal fees licences

There is likely to be a considerable amount of preliminary work involved in identifying the activities that would need to be licenced and preparing the corresponding application, in circumstances where there is no applicable general legal fees licence already in place. OFSI has been reluctant to grant general legal fees licences, and has, at the time of writing, done so on a few occasions only.

- Legal aid payments for representation of clients designated under antiterrorist sanctions: the first general licence issued by OFSI under SAMLA for legal services was limited to legally aided work for clients sanctioned under antiterrorist sanctions regimes.[34] A general licence issued at the beginning of 2021[35] authorises the government agencies involved in administering legal aid

31 id., amended paragraph 6.9.

32 OFSI, 'An Update to our Licensing Process: Returning Incomplete Applications', 12 July 2023, available at: https://ofsi.blog.gov.uk/2023/07/12/an-update-to-our-licensing-process-returning-incomplete-applications/.

33 OFSI, 'UK financial sanctions: General guidance for financial sanctions under the Sanctions and Anti-Money Laundering Act 2018' (footnote 2), amended paragraph 6.12.

34 The ISIL (Da'esh) and Al-Qaida (United Nations Sanctions) (EU Exit) Regulations 2019, the Counter-Terrorism (International Sanctions) (EU Exit) Regulations 2019 and the Counter-Terrorism (Sanctions) (EU Exit) Regulations 2019.

35 GENERAL LICENCE INT/2020/G1, 11 January 2021 (as amended), available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/988364/General_Licence_-_INT2020G1_-_As_amended.pdf.

to make payments to solicitors acting for clients designated under any of the specified regimes, and for the solicitors to receive these payments, provided that no funds are paid directly or indirectly to the designated person. It replaced a broader general licence, which extended to private third-party payments for the representation of persons designated under the UK's domestic antiterrorism legislation, together with a parallel general licence for insurance (both now revoked).

- Payments by specified entities or their subsidiaries: in March 2022, OFSI, for the first time, issued a general licence authorising specific entities – UK subsidiaries of designated persons VTB Capital plc and Sberbank CIB (UK) Ltd – to make payments of reasonable professional fees for the provision of legal services or reasonable expenses associated with the provision of legal services.[36] Notification must be provided to OFSI within seven days of any payments made in reliance on the licence, and supporting records must be kept for a minimum of six years.
- A further general legal fees licence permits legal fees to be paid by an interim manager or a trustee when acting as receivers and managers in respect of the property and affairs of a charity.[37] Records of any activity conducted in reliance on the licence must be kept for a minimum of six years.
- As from 28 October 2022, a general licence permits payments for legal fees and disbursements incurred in connection with the representation of persons designated under the Russian and Belarusian sanctions regimes.[38] There are separate conditions for payment obligations that predate designation and those that post-date designation. Both categories are subject to a total cap on professional legal fees (including counsel's fees) of £500,000 (inclusive of VAT) for the duration of the licence. Related expenses cannot

36 GENERAL LICENCE – Russian Banks – UK subsidiaries – Basic needs, routine holding and maintenance, the payment of legal fees and insolvency related payments, INT/2022/1280876, 1 March 2022 (as amended 1 April 2022 and 22 April 2022), available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1070607/INT.2022.1280876_GL.pdf.

37 GENERAL LICENCE – Russia Designated Persons – Charities and Interim Managers and trustees, INT/2022/1834876, 30 May 2022, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1079599/GENERAL_LICENCE_CC_20220530_.pdf.

38 The current version of this licence is OFSI General Licence under the Russia Regulations and the Belarus Regulations, INT/2023/2954852, 29 April 2023, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1153971/Legal_Services_GL_INT20232954852.pdf.

exceed 5 per cent of the amount payable for professional legal fees or, if lower, £25,000. Reports (on forms provided for this purpose) must be made within seven days of completing the legal services or, if sooner, the licence coming to an end. Under the current version of this general licence, legal services are defined as legal services provided to a designated person, including legal advice and representation in court, whether provided within the UK or another jurisdiction, in relation to any matter except a claim for defamation or malicious falsehood.[39]

Specific legal fees licences

Applications for specific legal fees licences are made using the general form for licence applications.[40] The reason why these applications tend to be time consuming is the requirement to demonstrate the reasonableness of any amounts sought to be licensed. As explained by OFSI in a June 2021 blog post,[41] OFSI is legally obliged under SAMLA to ensure that legal fees and expenses are 'reasonable'. The requirement of reasonableness is in fact imposed in the regulations adopted under SAMLA rather than in SAMLA itself. However, neither SAMLA nor the regulations define what is to be considered reasonable for this purpose. Instead, OFSI's general guidance explains that the burden of demonstrating reasonableness of legal fees and disbursements falls on the applicant and that OFSI will take as its benchmark or starting point the rates applied when costs orders are made in civil proceedings, as governed by the Supreme Court Cost Guidelines.[42] The blog post expands further on this general guidance by warning that OFSI will require a significant level of evidence when scrutinising the reasonableness threshold, and will consider the following factors: (1) whether the work has already taken place or if it is anticipated; (2) what the work will involve or has involved; (3) which fee earners will be, or have been, involved in the work (and their positions or roles within the firm, including relevant experience); (4) the fee earners' hourly rates; (5) how many hours each fee earner will be estimated to spend, or has already spent, on each work stream; (6) any supporting evidence as to why the involvement or the number of hours of the particular fee earner is reasonable or

39 ibid.

40 OFSI, Guidance, 'Licences that allow activity prohibited by financial sanctions', available at: www.gov.uk/guidance/licences-that-allow-activity-prohibited-by-financial-sanctions.

41 OFSI, 'Reasonableness in Licensing', 30 June 2021, available at: https://ofsi.blog.gov.uk/2021/06/30/reasonableness-in-licensing/.

42 OFSI, 'UK financial sanctions: General guidance for financial sanctions under the Sanctions and Anti-Money Laundering Act 2018' (footnote 2), paragraph 6.5.

proportionate to the nature and complexity of the work; (7) any expenses that are expected and have been paid out; and (8) if any expenses are expected, why they are necessary. Applicants are also warned to not assume that OFSI understands the process and practice of the legal profession. The obvious difficulty for many applicants, however, will be to provide all the details sought by OFSI without disclosing information protected by legal professional privilege (LPP). The blog post pre-empts this issue by confirming that OFSI does not generally consider fee notes and narratives of work (in generic terms) to be privileged, as they do not constitute the giving or obtaining of legal advice, stressing that OFSI will be unable to undertake a reasonableness assessment without having a breakdown of the legal costs for each area of work. It is not clear why OFSI has chosen to publish its policy position in the form of a blog post or how it is compatible with judicial authorities on the circumstances in which fee notes can attract LPP.[43] What is clear, however, is that OFSI will not issue a legal fees licence unless the specified details are disclosed. This potentially creates a conflict with the duty of regulated legal professionals to advise their clients on their entitlement to assert LPP, which is recognised under English law as a fundamental common law right as well as a human right.

Processing time for licence applications

The time taken by OFSI to process legal fees licence applications can be considerable. OFSI's general guidance previously stated that it aimed to 'engage' on the substance of a completed application in four weeks, but now states that all new licensing applications are reviewed 'as soon as practicable'.[44] There are no publicly available statistics on the average processing times for licence applications, and ministerial responses to questions in Parliament have confirmed that no distinction is drawn by OFSI when processing applications between legal fees licences and other categories of licences. The current version of OFSI's general guidance states that urgent and humanitarian cases (i.e., cases that involve a risk of harm or a threat to life) will be prioritised.[45] At times of high demand, OFSI will also prioritise applications where there are issues of personal basic needs or wider humanitarian issues at stake that are of material impact or urgency. It is not, however, clear whether legal fees licence applications would be considered of

43 See, e.g., the summary of the relevant judicial authorities in Colin Passmore, *Privilege*, 4th edition (Sweet & Maxwell, 2020), at 2-209 to 2-216.

44 OFSI, 'UK financial sanctions: General guidance for financial sanctions under the Sanctions and Anti-Money Laundering Act 2018' (footnote 2), paragraph 6.10.

45 id., at paragraph 6.10.1.

material impact or urgency. A response to a Freedom of Information Act request reported by *The Law Society Gazette* in April 2022 revealed that OFSI had granted no legal fees licences between 1 January and 10 March 2022, despite having received 15 applications relating to Russian individuals and entities.[46] The time taken for legal fees licence applications to be processed will clearly bear directly on access to justice, and specifically the designated person's access to the courts as a fundamental right protected by the common law as well as under the Human Rights Act 1998 (HRA). The hurdles created for designated persons to access legal services are compounded by the limitations imposed by OFSI on the duration and amounts authorised by licences, which means that multiple consecutive licence applications may need to be submitted for the same legal proceedings or the performance of the same instructions, adding not just to the length of time spent on making applications but also to the costs of legal representation.

In January 2023, HM Treasury commissioned an internal review of its approach to specific and general licences, to see if any changes were required to OFSI's licensing practice in relation to legal fees licence applications. On 30 March 2023, Parliament was informed that the review had confirmed that OFSI's decision-making on legal fees licence applications:

> *must carefully balance between the right to legal representation – which is a fundamental one – with wider issues, including the aim and the purpose of the sanctions. While some legal claims may be unfounded, it is for the Courts to decide whether their claims should be permitted to succeed – not the Government.*[47]

Challenges to licensing decisions

It is, in theory, possible to judicially review OFSI's refusal to process or grant a legal fees licence application or its failure to consider it within a reasonable period. However, a legal fees licence would be required to enable payment of lawyers for advising on and bringing the challenge. Unsurprisingly, the UK courts have heard very few challenges to licence determinations to date, even though these

46 John Hyde, 'Sanctioned clients in limbo as Treasury fails to grant "reasonable fees" licences', *The Law Society Gazette* (10 April 2022), available at: www.lawgazette.co.uk/news/sanctioned-clients-in-limbo-as-treasury-fails-to-grant-reasonable-fees-licences/5112164.article.

47 UK Parliament, Written questions, answers and statements, '[OFSI] update, Statement made on 30 March 2023' (footnote 15).

challenges would have been possible prior to the expiry of the Brexit transition period, as licensing decisions are always made by the national competent authorities rather than at EU level.

Instead, it has fallen to the EU court to clarify the obligations of the national licensing authorities. In *Peftiev*,[48] the Court of Justice of the European Union (CJEU) identified the considerations that would arise if a legal fees licence were refused altogether by a national licensing authority, specifically on account of concerns that the frozen funds might represent the proceeds of crime. The court concluded that the licensing authority's discretion was tempered by the obligation to respect the fundamental human rights of the applicant, which, in the case of a target of EU sanctions, included the indispensable nature of legal representation in bringing an action challenging their lawfulness. The court rejected the suggestion that a lawyer could be paid what they are owed once sanctions have been lifted, finding that it was not open to Member States to require a legal services professional to bear such a risk and financial burden. The court also rejected the suggestion that the designated person could be forced to resort to legal aid instead. As for the suggestion that the funds in question had been unlawfully acquired, the court stressed that the nature of an asset freeze is different in kind from seizure or confiscation and the purpose of sanctions is not to penalise the unlawful acquisition of funds. This is why there is no carve out from the right to apply for a legal fees licence, whether on account of the origin of the funds in question or their possible unlawful acquisition.

The position is the same for UK licensing bodies, even after the UK's departure from the EU. As 'public authorities' for the purposes of Section 6 of the HRA, they are obliged to act compatibly with rights afforded under the European Convention on Human Rights (ECHR) when processing and determining legal fees licence applications.

Representing a designated person in applications for revocations of or variations to a UK designation

The legal work that a legal fees licence is typically sought for includes requests for a ministerial revocation or variation of a designation, or, for UN designations, a request that the Secretary of State use their best endeavours to request a reconsideration. The requirement to periodically review designations was repealed by the Economic Crime (Transparency and Enforcement) Act 2022 (ECTEA) on 15 March 2022. However, Section 22 of SAMLA enables a minister to consider

48 Case C-314/13, *Užsieno reikalu ministerija & Ors v. Vladimir Peftiev & Ors*.

whether the required conditions of a designation are met; and Section 23 of SAMLA confers a right on a designated person to request variation or revocation at any time. The process for submitting representations to a minister for this purpose is governed by the Sanctions Review Procedure (EU Exit) Regulations 2018 and supported by guidance and a standard sanctions review request form published by the Foreign, Commonwealth and Development Office (FCDO).[49] Section 40 of SAMLA confers a right to apply for a court review of ministerial decisions to refuse requests made under Sections 23 and 25 of SAMLA. The procedure is governed by the Civil Procedure Rules 1998 and related Practice Directions.[50]

A preliminary issue that typically arises in connection with these challenges is whether legal advice and assistance is necessary in the first place. There is no procedural requirement for legal representation, whether at the ministerial review stage or at the court stage, and the standard form is clearly intended to enable designated persons to apply without recourse to legal advice and assistance. However, designated persons are typically located outside the UK and are unlikely to be familiar with the UK's autonomous sanctions regime. While litigants in person can ordinarily represent themselves in any court and in any case, sanctions designation challenges will inevitably raise complex issues of public law. Article 6 of the ECHR confers a right to legal representation in the determination of civil rights and obligations, in circumstances where a lawyer is indispensable for effective access to a court.[51] The ability of a designated person to obtain legal representation of their choosing is also key to the legitimacy of any sanctions regime. It is therefore important that this right is effective and available in practice.

There is still limited experience of ministerial reviews of UK autonomous designations or judicial challenges to ministerial decisions. While the UK was an EU Member State, requests for reconsideration would need to be addressed to the Council and applications to annul a designation directed to the General Court of the CJEU. Challenges to EU sanctions would not be heard by the UK

---

49 Foreign, Commonwealth and Development Office, 'Guidance – How to request variation or revocation of a sanctions designation or review of a UN listing', updated 2 February 2023, available at: www.gov.uk/government/publications/making-a-sanctions-challenge-how-to-seek-variation-or-revocation-of-a-sanctions-designation/making-a-sanctions-challenge-how-to-seek-a-variation-or-revocation-of-a-sanctions-designation.

50 Practice Direction Part 79 – Proceedings under the Counter-Terrorism Act 2008, Part 1 of the Terrorist Asset-Freezing Etc. Act 2010 and Part 1 of the Sanctions and Anti-Money Laundering Act 2018, available at: www.justice.gov.uk/courts/procedure-rules/civil/rules/part79.

51 See, e.g., *Airey v. Ireland* (1979-90) 2 EHRR 305.

courts unless they involved a decision by a UK public authority – such as a decision to request a person's designation or a refusal to request the removal of a designation. In one of the earliest, unsuccessful, examples, a minister's refusal to request a delisting was considered a matter of foreign policy and, as such, unsuitable for judicial review.[52] A subsequent judicial authority concluded that it would be possible, albeit difficult, to challenge ministerial decisions to designate as well as to refuse to seek the removal of a designation.[53]

The new regime created by SAMLA for challenging UK autonomous sanctions has not improved the prospect of judicial scrutiny of designation decisions, which is the only mechanism available to ensure that ministers exercise their powers to designate lawfully. Court applications are likely to remain infrequent for the following reasons.

- No variation or revocation can be made by a UK minister in relation to designations based on UN listings. An early challenge to the compatibility of this restriction with the designated person's Convention rights was rejected by the High Court in *Youssef*,[54] despite a precedent seemingly to the contrary from the European Court of Human Rights in *Al-Dulimi*.[55] Instead, the only remedy available for UN designated persons is to request the Secretary of State to use their best endeavours to secure their removal from the UN list, and any refusal to do so can be challenged on judicial review principles.[56]
- In accordance with a partial 'ouster clause' in SAMLA, no court can hear a delisting application until the ministerial review process has been exhausted. There are no time limits for ministerial decisions on revocation requests beyond a general requirement that they are to be made as soon as reasonably practicable on receipt of the information needed for making them.[57] SAMLA also prohibits repeated requests, unless there is a significant matter that has not previously been considered by the minister.[58]

52 *R (El-Maghraby and El Gazaerly) v. HM Treasury and Foreign and Commonwealth Office* [2012] EWHC 674 (Admin).

53 *R (Bredenkamp) v. Secretary of State for Foreign and Commonwealth Affairs* [2012] EWHC 3297 (Admin).

54 *Youssef v. the Secretary of State for Foreign, Commonwealth and Development Affairs and HM Treasury* [2021] EWHC 3188 (Admin).

55 *Al-Dulimi and Montana Management Inc. v. Switzerland*, Application 5809/08) (2016) 42 BHRC 163.

56 SAMLA, Section 25(2).

57 The Sanctions Review Procedure (EU Exit) Regulations 2018, Regulation 7.

58 SAMLA, Sections 23(2) and 25(3).

- A prerequisite to challenging any public act is the ability to understand the case against the designated person. Yet, they may not know the basis for their designation. There is a duty on the minister to provide a statement of reasons for designating a person by name under the standard procedure, which would ordinarily be reproduced in the Consolidated List of Financial Sanctions Targets in the UK (the Consolidated List). This is not, however, a substitute for the evidence relied on in support of the designation, which must be sought separately from the FCDO. SAMLA does not require designated persons to be informed about the existence of the Sanctions Designation Form Evidence Pack (SDFE) or how to request access to it. There are no time limits governing the production of the SDFE or any means of understanding whether a disclosure is incomplete. Designated persons may invoke their rights as data subjects to obtain copies of their personal data, but this is an entirely separate process governed by data protection legislation. The FCDO routinely invokes exemptions in the UK General Data Protection Regulation and the Data Protection Act 2018 to resist disclosure of information over which it considers a claim to LPP could be maintained and to safeguard national security.
- The designated person may not always be in a position to understand why a revocation request has been refused by the minister. It is at the minister's discretion whether to publish a decision and the reasons for it. Although the designated person must be given a reason for the refusal, the minister can exclude any matters in the interests of national security or international relations, for reasons connected with the prevention or detection of serious crime or in the interests of justice.[59] The courts may similarly hear sensitive evidence not disclosed to the applicant, in a 'closed material' procedure imported from domestic antiterrorist legislation.[60]
- Even where the designated person is in possession of the evidence relied on in support of their designation as well as the full reasons for the minister's refusal of a revocation request, the grounds for challenge are limited. Although a minister may vary or revoke a designation at any time, there is only an obligation to do so if the necessary conditions cease to be met.[61] Those necessary conditions have been further limited by amendments to SAMLA introduced by ECTEA, which enable ministers to conclude that any sanctions adopted for a discretionary purpose are appropriate without first satisfying themselves

59 The Sanctions Review Procedure (EU Exit) Regulations 2018, Regulation 8.

60 SAMLA, Section 40.

61 id., Section 22(3).

that there are good reasons to pursue the purpose for which the sanctions are to be adopted and that the imposition of sanctions is a reasonable course of action for that purpose.[62]

- Court proceedings are expensive to bring. Following amendments to SAMLA by ECTEA, the ability of a court to order damages in the event of a successful challenge is now confined to circumstances where a designation is found to have been adopted in bad faith.[63] Any damages award made may also not exceed any amount specified by a minister in regulations adopted for this purpose.[64]
- Finally, there appears to be nothing in SAMLA to prevent a designation from being remade on different grounds, even after it has been revoked by the minister or declared unlawful by a court.

Concurrent designations in multiple jurisdictions create additional issues that need to be factored in when advising designated persons, particularly in connection with legal and administrative challenges to designation decisions. The proliferation of sanctions designations worldwide has increased the likelihood of the same person being designated in more than one jurisdiction. Indeed, the recently introduced 'urgent' procedure for temporary UK designations is predicated on a prior designation by one of the specified jurisdictions.[65] Simultaneous designation challenges raise complex strategic considerations as well as practical coordination challenges, not least as legal fees licences may need to be sought from multiple authorities.

General considerations arising in all legal work for designated persons

Any legal work for designated persons will expose a lawyer to a heightened risk of committing financial sanctions breaches, including by participating in or facilitating circumvention offences. It may not always be clear, however, what activities could potentially amount to unlawful facilitation and circumvention. OFSI's enforcement guidance explains that facilitation of a financial sanctions breach is a form of circumvention, and that individuals who act on behalf of or provide advice to others as part of their job may be considered professional facilitators. In

62 Economic Crime (Transparency and Enforcement) Act 2022 (ECTEA), Section 57(2), repealing SAMLA, Section 1(4); ECTEA, Section 57(3), repealing SAMLA, Section 2.

63 SAMLA, Section 39(2).

64 id., Section 39(2A).

65 id., Section 11(1A)(b).

OFSI's view, simply discovering a potential sanctions breach when acting for a client does not automatically make a professional adviser party to it, but they may become so if their subsequent actions amount to collusion in the breach.[66]

Lawyers are also exposed to criminal liability for failing to comply with their reporting obligations in connection with the representation of designated persons. In addition to any reporting obligations imposed under legal fees licences, firms and sole practitioners providing legal or notarial services to other persons, by way of business, are 'relevant firms' obliged under each SAMLA regulation, in accordance with information provision obligations adopted pursuant to Section 16 of SAMLA, to inform the Treasury as soon as practicable if they know, or have reasonable cause to suspect, that a person is a designated person or has committed a criminal breach of financial sanctions. Where a designated person is a client, relevant firms are also required to report on the nature and extent of any frozen assets held on that client's behalf. OFSI has published a standard 'compliance reporting form' on its website for this purpose. Where the designated person is a client, the obligation to report knowledge that a person is a designated person and the obligation to report on the nature and extent of any frozen assets held would in any event be discharged when submitting a legal fees licence application or, where reliance is placed on a general licence, when complying with reporting conditions.

If there is no general licence in place, the SRA's compliance guidance advises firms to also consider making the SRA aware that a client is a designated person regardless of whether this information relates to any reportable conduct to ensure that the SRA has a record of what has happened and why, in case of any future queries or concerns.[67]

The SRA has separately and more recently confirmed that it expects firms to 'screen' not only their clients but also any counterparties against the Consolidated List at the outset of a matter, and to conduct more in-depth due diligence and regular ongoing monitoring for riskier counterparties and transactions.[68] The SRA warns that reliance on another party's screening systems is unlikely to provide a complete defence in the event of a breach of the sanctions regime.

---

66 'OFSI enforcement and monetary penalties for breaches of financial sanctions' (footnote 3), paragraph 3.37.

67 SRA, Guidance (footnote 11).

68 SRA, Questions and answers, updated 28 July 2023, available at: www.sra.org.uk/solicitors/resources/money-laundering/guidance-support/aml-questions-answers/.

Relevant firms are also separately obliged to provide information about frozen funds in response to OFSI's annual frozen assets reviews. This is an exercise of the broad powers conferred by SAMLA on the Treasury to request any person to provide specified information or to produce specified documents, in any manner specified, for a specified purpose. A failure to comply with any information provision obligation, without reasonable excuse, is a criminal offence and the obligation may be enforced by court order.

There is a limited carve out from the information provision obligations in SAMLA regulations for information that is protected by LPP, when it is in the possession of a person who has acted or is acting as counsel or solicitor for any person. The identity of a client may, in certain circumstances, be protected by LPP.[69] However, the requirement to report knowledge or reasonable cause to suspect that a person is a designated person is in any event understood to be confined to individuals and entities on the Consolidated List (as opposed to entities owned or controlled by designated persons) and directed at circumstances where the designated person in question is seeking to disguise their identity and designated status. It would present an obvious obstacle to access to justice if lawyers were required to report the fact that they had been approached by a designated person lawfully seeking legal assistance, in circumstances where they decline instructions or are not retained to act.

69 *SRJ and persons unknown* [2014] EWHC 2293 (QB).

CHAPTER 24

Representing Designated Persons: A US Lawyer's Perspective

Farhad Alavi and Sam Amir Toossi[1]

Over the past 20 years, the United States has increasingly leveraged its economic power by implementing sanctions to effectuate foreign policy objectives.[2] As a result, more and more parties operating in sanctioned countries or labelled as sanctions violators face significant limitations in their day-to-day international dealings.

This chapter details the authorisations and prohibitions commonly seen in the representation of persons subject to US sanctions, be they designated as such by the US Department of the Treasury's Office of Foreign Assets Control (OFAC) or parties based in a jurisdiction subject to a broader economic embargo. This chapter also provides an outline of: the scope of representation authorised for sanctioned individuals; OFAC's policy and position on payments to counsel, related costs and judicial award transfers; the processes by which parties can seek authorisation to conduct transactions that would otherwise be prohibited by US sanctions; the process by which a sanctioned individual may seek to have sanctions lifted; and reputational issues counsel can face when representing sanctioned individuals.

---

1 Farhad Alavi is the managing partner and Sam Amir Toossi is a partner at Akrivis Law Group, PLLC. The authors wish to thank associates Ziad El Oud and Hope Mirski for their contributions to the chapter.

2 Between 2000 and 2021, the number of sanctions authorities nearly tripled, and, in the same period of time, the number of sanctioned individuals and entities grew from 912 to 9,412. See US Dep't of Treasury, 'The Treasury 2021 Sanctions Review', 18 October 2021.

Scope of representation of parties in sanctioned countries and parties that are sanctioned

The SDN List

OFAC 'administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States'.[3] Sanctions 'can be either comprehensive [i.e., targeting specific countries] or selective [i.e., targeting specific entities and individuals]'.[4]

With respect to selective sanctions:

> *As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called 'Specially Designated Nationals' or 'SDNs.'*[5]

When OFAC adds individuals and entities to the Specially Designated Nationals and Blocked Persons List (the SDN List),[6] '[t]heir assets are blocked and U.S. persons are generally prohibited from dealing with them'.[7] 'In making a listing

---

3 US Dep't of Treasury, 'Office of Foreign Assets Control – Sanctions Programs and Information', https://ofac.treasury.gov/office-of-foreign-assets-control-sanctions-programs-and-information; see also US Dep't of Treasury, Office of Foreign Assets Control (OFAC), Frequently Asked Questions (FAQs) (released on 10 September 2002), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1501.

4 US Dep't of Treasury, FAQs (footnote 3).

5 US Dep't of Treasury, 'Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists' (last updated 9 May 2023), https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists; see also US Dep't of Treasury, FAQs, Question #56 (released on 30 January 2015), https://ofac.treasury.gov/faqs/56.

6 Note that: 'OFAC also administers several other sanctions lists including the Foreign Sanctions Evaders (FSE) List and the Sectoral Sanctions Identifications (SSI) List. U.S. persons are not required to block the property of individuals and entities on these FSE and SSI lists (unless the targets are also on the SDN list), but other prohibitions and investment restrictions apply.' OFAC, FAQs, Question #56 (footnote 5). Separately, '[t]he Bureau of Industry and Security . . . of the U.S. Department of Commerce maintains separate lists for the purposes of the programs that it administers'. ibid.

7 US Dep't of Treasury, SDN List (footnote 5); see also OFAC, FAQs, Question #56 (footnote 5).

determination, OFAC draws on information from many sources, including but not limited to relevant United States government agencies, foreign governments, United Nations expert panels, and press and other open source reporting.'[8] OFAC will then conduct an investigation and will document its findings in an evidentiary memo and a proposed listing action, which is then reviewed by the relevant US agencies.[9] Individuals and entities can also be added to the SDN List via secondary sanctions, where applicable.[10]

Parties cannot merely rely on the SDN List to determine which entities they should not conduct business with. As OFAC has explained:

> *any entity owned in the aggregate, directly or indirectly, 50 percent or more by one or more blocked persons is itself considered to be a blocked person. The property and interests in property of such an entity are blocked regardless of whether the entity itself is listed in the annex to an Executive order or otherwise placed on OFAC's list of Specially Designated Nationals.*[11]

A party sanctioned by the United States and, therefore, effectively shut off from the US economy, may still have significant financial and legal interests subject to US jurisdiction. Moreover, in many instances, the very basis for many OFAC designations is grounded in the harm these parties are alleged to have committed against US persons or US interests, which may be litigated in US courts or other tribunals and require the sanctioned individuals to obtain legal counsel. And some citizens and residents of sanctioned jurisdictions (i.e., territories subject to comprehensive US sanctions) may have substantial touchpoints outside their home country, such as owning businesses in third jurisdictions not subject to sanctions, having personal affairs in the United States and having US or third-country

8 US Dep't of Treasury, Filing a Petition for Removal from an OFAC List, https://ofac.treasury.gov/specially-designated-nationals-list-sdn-list/filing-a-petition-for-removal-from-an-ofac-list.

9 ibid.

10 See, e.g., Executive Order 13810 of September 20, 2017, 82 Fed. Reg. 184 (25 September 2017), https://ofac.treasury.gov/system/files/126/13810.pdf (authorising secondary sanctions in relation to North Korea).

11 US Dep't of Treasury, 'Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property Are Blocked' (13 August 2014), https://ofac.treasury.gov/media/6186/download?inline.

passports.[12] Broadly speaking, OFAC regulations authorise US counsel to provide many types of legal services to parties that are subject to sanctions. A party might, therefore, require an attorney to:

- counsel the targeted persons on the requirements of US laws and regulations;
- represent the person before US federal, state and local agencies, whether they have been named a party to such a case or have initiated it themselves;[13]
- represent the person in litigation and other dispute resolution in the US;
- apply for OFAC licences to engage in otherwise unauthorised transactions;
- seek removal from the SDN List;[14] or
- represent the person in cases where US laws require access to legal counsel at the public's expense,[15] such as in a criminal matter where parties can be represented by a court-appointed attorney.

Because legal representation increasingly relies on the support of non-lawyer experts, including expert witnesses, electronic discovery specialists, investigators, forensic accountants and IT experts, these types of engagements are generally authorised by OFAC, although many may be prohibited outside the litigation context. As further described below, however, receiving payment for these legal and related services could require a specific licence.[16]

---

12 Beyond sanctioned parties, OFAC also regulates the legal representation by US counsel of persons in sanctioned jurisdictions, such as individuals residing in Iran or Cuban nationals residing anywhere outside the United States. See 31 Code of Federal Regulations (C.F.R.) § 560.525 of the Iranian Transaction and Sanction Regulations and 31 C.F.R. § 515.512 of the Cuban Assets Control Regulations.

13 See, e.g., *American Airways Charters Inc. v. Regan*, 746 F.2d 865, 866–67 (D.C. Cir. 1984) ('We hold that although government permission, in the form of an Office of Foreign Assets Control license, is required prior to the execution of any transaction reaching the assets of a designated Cuban national, the Office of Foreign Assets Control lacks authority to condition the bare formation of an attorney-client relationship on advance government approval.').

14 OFAC makes clear, however, that those filing a petition for removal from the SDN List do not need to hire an attorney, as 'OFAC accepts petitions directly from listed persons or from their representatives'. US Dep't of Treasury, Filing a Petition for Removal from an OFAC List (footnote 8).

15 See, e.g., 31 C.F.R. § 515.512.

16 See, e.g., 31 C.F.R. § 515.512(d)(1) (stating, in a regulation relating to the Cuba sanctions programme, that '[a]ll receipts of payment of professional fees and reimbursement of incurred expenses for the provision of [authorized] legal services . . . must be specifically licensed or otherwise authorized pursuant to § 515.512(e)').

Although every US sanctions programme is unique and designed to effectuate distinct policy ends, the scope of OFAC authorisations for the provision of legal services to sanctioned parties and parties in sanctioned jurisdictions is generally consistent across sanctions programmes, albeit with some variation and nuance. These provisions – predominantly found in the Code of Federal Regulations (CFR) or OFAC-issued general licences[17] – not only authorise the representation of these parties by US counsel, but also cover ancillary issues such as paying attorneys' fees and reporting obligations. Of course, US counsel are, however, prohibited from assisting clients in circumvention of sanctions laws, such as structuring transactions in a manner aimed at keeping them outside the purview of US jurisdiction, as these acts could violate provisions of OFAC regulations prohibiting US persons from engaging in unlawful facilitation.[18]

Despite the broad flexibility afforded US counsel and supporting parties, there may be times when general licences do not suffice, requiring the US counsel to apply for a specific licence to engage in certain representation. These can be issues such as representing a sanctioned party in litigation or arbitration outside the United States, acting as expert witness or counsel in a dispute abroad, or merely advising on contractual matters. For example, providing expert witness services as a US legal expert may be intrinsically legal in nature but viewed under OFAC regulations as a general service, given that the expert would not be providing legal representation per se. Separately, if US counsel is advising on a commercial transaction for a foreign party that is subsequently designated by OFAC, there may be a need for a specific licence to continue providing advice or engage in a wind-down of legal services.

17 See US Dep't of Treasury, Filing a Petition for Removal from an OFAC List (footnote 8) ('In almost all of its sanctions programs, OFAC has issued general licenses . . . authorizing the provision of certain legal services to SDNs, including representation of SDNs in connection with delisting requests'); see also 31 C.F.R. § 515.512 (listing, in a regulation relating to the Cuba sanctions programme, the 'legal services to or on behalf of Cuba or a Cuban national' that are 'authorized').

18 See, e.g., 31 C.F.R. § 560.525(a)(1).

Licensing

According to OFAC, '[a] license is an authorisation from OFAC to engage in a transaction that otherwise would be prohibited.' OFAC's regulations establishing sanctions programmes generally include language authorising OFAC to issue licences to effectuate the intent of sanctions programmes, 'ensuring that those transactions consistent with U.S. policy are permitted'.[19]

OFAC issues two different types of licences: general licences and specific licences. General licences authorise 'a particular type of transaction for a class of persons without the need to apply for a license'.[20] OFAC issues general licences to authorise activities that would otherwise be prohibited with regard to sanctioned countries and entities. These broad authorisations allow all US persons to engage in the activity described thereof without applying for specific authorisation issued on a case-by-case basis.

A specific licence, by contrast, 'is a written document issued by OFAC to a particular person or entity, authorising a particular transaction in response to a written license application'.[21] When a contemplated activity falls outside the scope of a general licence, a party can request a specific licence authorising both US and non-US persons to engage in the activity. After receiving a licence application, OFAC will issue a written response approving or denying the request. If approved, an OFAC licence is issued to a particular person or entity and authorises a particular transaction[22] for a set term. Importantly, persons engaging in transactions pursuant to general or specific licences must strictly comply with the terms and scope of the licences.[23]

Requests for interpretive guidance

Although a general or specific licence may be clear on its face, certain activities may warrant seeking interpretive guidance from OFAC, as it may not be clear whether the proposed activities fall within the scope of the licence. In these circumstances, sanctioned individuals and entities, or those conducting business with these entities, are well advised to, at a minimum, seek interpretative guidance from OFAC.

---

19 Press Release, OFAC, 16 June 2004, https://home.treasury.gov/news/press-releases/js1729.

20 ibid.

21 ibid.

22 OFAC, FAQs, Question #74, https://ofac.treasury.gov/faqs/74.

23 ibid.

Interpretative guidance may also be sought when there are sudden political or economic shifts and resulting conditions that the original sanctions programme did not contemplate. For example, when the Taliban took control of the Afghan government in August 2021, it created the unusual circumstance where a sanctioned entity was the controlling entity in a nation that was not under a country-wide embargo. This led to considerable confusion as to whether certain activities that required interaction with the local government were allowed or prohibited. In these circumstances where the political shift has created a disconnect from previously issued licences, written guidance from OFAC can provide clarity to entities operating within these environments and can be used as a reference by counterparties. Further, if this guidance is provided publicly, it could potentially stave off similar requests to OFAC by parties performing similar transactions.

Payment for legal services and related expenses

Even where the provision of legal advice is allowed by a general licence, payment for these services often still requires a specific licence. For example, the Weapons of Mass Destruction Proliferators Sanctions Regulations[24] state, in relevant part:

> *The provision of the following legal services to or on behalf of persons whose property and interests in property are blocked pursuant to §544.201(a) is authorised, provided that all receipts of payment of professional fees and reimbursement of incurred expenses must be specifically licensed.*[25]

Even where a specific licence is obtained for payment of legal services, the relevant CFR sections will often dictate that payments to the licensee of professional fees and expenses authorised by the licence must not originate from a source within the United States, or from any source outside the United States within the possession or control of a US person, or from any other entity or individual

24 31 C.F.R. § 544.507.

25 31 C.F.R. § 544.507(a). The Syrian Sanctions Regulations (31 C.F.R. §542.507), the Iranian Sector And Human Rights Abuses Sanctions Regulations (31 C.F.R. § 562.506), the Global Terrorism Sanctions Regulations (31 C.F.R. § 594.506) and the Foreign Terrorist Organisations Sanctions Regulations (31 C.F.R. § 597.505) have similar authorisations with regard to legal representation, and as a general matter, 'all receipts of payment of professional fees and reimbursement of incurred expenses must be specifically licensed' (see 31 C.F.R. §542.507(d)(1), 31 C.F.R. § 562.506(a), 31 C.F.R. § 594.506(a) and 31 C.F.R. § 597.505), and there are reporting requirements for receipts of payment (see 31 C.F.R. §542.508(c), 31 C.F.R. § 562.101, 31 C.F.R. § 594.517(a)(3) and 31 C.F.R. § 597.513(a)(3)).

whose property and interests in property are blocked pursuant to any executive order.[26] This requirement for parties to pay their legal fees from outside the United States can prove difficult given that SDNs and parties in comprehensively sanctioned territories are generally barred from the US banking system. To effectuate payment in these circumstances, each regulatory framework has its own requirements, with some requiring prior notification to OFAC, some requiring prior specific licensing[27] and some requiring periodic reporting.[28] Where a sanctions regime provides no guidance with respect to legal representation or payments for representation, parties should seek interpretative guidance, and in the alternative, a specific licence for legal representation and payment for the same.

Finally, the receipt of payment based on awards of judgments and settlements generally requires a specific licence.[29] Even entering into a settlement agreement may, under certain sanctions programmes, require licensing, and efforts to pre-emptively obtain pre-approval to collect payment on a court award or settlement amount may prove difficult, given the time it takes for OFAC to evaluate and approve licence applications.

Applications for general and specific licences

While US persons can submit specific licence applications to OFAC for any type of transaction, counsel should first assess the likelihood of receiving a licence. This means assessing the proposed activity and the policy interests of OFAC and, more broadly, the United States in relation to the involved parties and the proposed activity. To illustrate, a licence application enabling US counsel to engage in proactive representation – such as representing sanctioned persons on international, non-US matters such as a contract or structuring of a financial transaction – is arguably less likely to be seen as consistent with US interests than engaging in an activity that would be subject to a general licence if in the United States, such as serving as counsel or a US law expert in a dispute abroad where the US lawyer's or law firm's services are critical to the representation.

Although OFAC does not provide standard forms for most of these licence applications, its website states that licence applications should include 'all necessary information as required in the application guidelines or the regulations pertaining to the particular embargo program'.[30] Applications for licences must

26 See, e.g., 31 C.F.R. §§ 583.506 and 590.508.
27 See, e.g., 31 C.F.R. § 594.506.
28 See, e.g., 31 C.F.R. § 560.553(b).
29 See, e.g., 31 C.F.R. §§ 515.512(c) and 560.525(c).
30 OFAC, FAQs, Question #75, https://ofac.treasury.gov/faqs/75.

include 'all information specified by relevant instructions and/or forms and must fully disclose the names of all parties who are concerned with or interested in the proposed transaction'.[31] Furthermore, OFAC asks that licence applications include 'a detailed description of the proposed transaction, including the names and addresses of any individuals/companies involved'.[32] After receiving a licence application, OFAC will issue a written response approving or denying the licence request or return it without action if it finds a given general licence or other authorisation to apply.

Evidence and documentation

There is no established burden of proof for OFAC's consideration of applications for specific licences. However, because the success of the application is heavily fact- and policy-specific, it is critical to include detailed, accurate and verifiable information so that OFAC can make an informed decision regarding the application. Parties seeking these licences should be clear in their request and explain not only the rationale underpinning their applications, but also the policy justification warranting the issuance of a specific licence. Supporting documentation should be provided to the extent that it is available and responsive.

In terms of the criteria for evaluating applications, OFAC has stated that its licensing determinations are 'guided by US foreign policy and national security concerns' and that '[e]ach application is reviewed on a case-by-case basis and often requires interagency consultation'.[33] For this reason, certain public comments by the leaders of other federal agencies explaining or defining the US government's foreign policy objectives can be useful in advocating for the approval of a specific licence. Additionally, although OFAC will disclaim any precedential value to the approval of any given licence, it nonetheless strives to achieve consistency across its evaluations of licence applications, meaning that it will consider its prior decisions in similar matters.

Beyond the basic facts and circumstances of a given transaction, as well as the involved parties, counsel can and should make active arguments justifying approval. Counsel should advance arguments as to why the proposed transaction aligns with or does not contravene US foreign policy objectives. For example, if US policy favours divestment from a sanctioned country, counsel should highlight how the transaction that is the subject of the counsel's representation advances

31 31 C.F.R. § 501.801(b)(2)(ii).

32 OFAC, FAQs, Question #75 (footnote 30).

33 OFAC, FAQs, Question #58, https://ofac.treasury.gov/faqs/58.

that policy. Similarly, if a proposed transaction has at least some humanitarian objectives, counsel should stress them. A frequent criticism of sanctions regimes is that their impact is felt predominantly by the ordinary people living in the heavily sanctioned country rather than by the governing regimes, especially where the sanctioned country is ruled by an autocratic government where the population has no say in its government or its conduct. OFAC often attempts to address these concerns by issuing general licences directed at humanitarian efforts, particularly in the supply of food and medicine. Still, these general licences do not contemplate all aspects of humanitarian aid, including legal representation, and to the extent possible, applicants for specific licences should emphasise the humanitarian objectives within the proposed transaction.

Challenging OFAC's denial of a specific licence

OFAC licensing decisions are considered 'final' agency actions. Thus, to appeal OFAC's denial of a licence request to provide legal services, the applicant would have to demonstrate some 'good cause', such as changed circumstances or additional relevant information that is outcome-determinative.[34]

Alternatively, applicants denied OFAC licences can file a lawsuit against the agency. This option can be costly, and a successful challenge to 'final agency action' requires a litigant to show that the agency's decision was 'arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law', a very high standard in the US legal system.[35] Furthermore, because US courts afford tremendous deference to government agencies charged with making decisions that affect national security, it is imperative that OFAC licence applicants ensure that the application is accurate and exhaustive prior to submitting it for OFAC's consideration.

Precedential value

Even when OFAC agrees that a proposed activity is within the scope of a general licence or grants a specific licence, it will often also state that its response has 'no precedential effect' and is 'based on the facts and circumstances of the application'. Nevertheless, OFAC states that part of its evaluation of any given application includes its prior determination in similar situations. Because OFAC does not publish its grants of specific licences, it can be challenging for applicants and counsel to cite other applications for any guidance. For that reason, it is important

34 OFAC, FAQs, Question #76, https://ofac.treasury.gov/faqs/76.

35 5 U.S.C. § 706(2)(A).

for an applicant to hire counsel with experience in making licensing applications for transactions affecting sanctioned persons or in the sanctioned country at issue because that counsel will be able to draw upon similar cases and previous OFAC decisions to support the application.

Timing considerations

There are no set timetables for OFAC to respond to a request for a specific licence to conduct any activity. OFAC can take months or even years to respond to a given request, but, as a general matter, it will respond to routine requests within several months, and more complex transactions can potentially take over a year to obtain a response. OFAC's ability to respond expeditiously to each request may be thwarted by major sanctions events, such as the Taliban takeover of Afghanistan or the Russian invasion of Ukraine. The Ukraine invasion has arguably made any prediction on agency timing even more difficult, especially given the scores of parties sanctioned and the presumably high number of parties petitioning before the agency for various reasons.

Consequently, applicants for specific licences should clearly state the time sensitivity of the request, including all relevant deadlines for the transactions or legal proceedings. Where humanitarian interests are involved, the applicant should unambiguously request and emphasise the importance of an expeditious review, as well as the detrimental consequences of denial of the application or non-action. If OFAC has failed to respond to a given application, the applicant or counsel can call the agency and speak with an information specialist who can update them on the status of the application. In some circumstances, the applicant or counsel may be able to speak directly with the licensing officer assigned to the application.

Confidentiality

Finally, to the extent that a licence application contains extremely confidential and business proprietary information as well as certain commentary that could potentially endanger the party making the application, its owners and any affiliates and contractors if released to the public, the applicant should so note and request confidentiality pursuant to the Freedom of Information Act and 5 USC Sections 552(b)(4) and (b)(7)(F), which prevents the release of the information to the public, even when requests for this information are made pursuant to other laws and regulations. Certain parts of an application, even if released, can be redacted under these provisions.

Obtaining delisting

As part of its guidance, OFAC explains that the 'power and integrity' of its sanctions stem not only from its 'ability to designate and add persons to the Specially Designated Nationals and Blocked Persons List (SDN List), but also from its willingness to remove persons from the SDN List consistent with the law'.[36] OFAC guidance further explains that '[t]he ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior'.[37] Notably, while designations have often focused on ongoing activity by the targeted party, past activity may also provide an adequate basis for designation, as demonstrated by OFAC's enforcement patterns and the text of certain executive orders in recent years.[38]

To petition for removal from the SDN List – that is, to 'seek administrative reconsideration of his, her or its designation or that of a vessel as blocked'[39] – a listed party should submit to OFAC '[a] request for the reconsideration of OFAC's determination, including a detailed description of why the listed person should be removed'.[40] While the regulations prescribe an official 'gatekeeper' function for OFAC with respect to delistings, this traditional role is not exclusive to the agency.[41]

---

36 US Dep't of Treasury, Filing a Petition for Removal from an OFAC List (footnote 8).

37 ibid. OFAC continues that, '[e]ach year, OFAC removes hundreds of individuals and entities from the SDN List. Each removal is based on a thorough review by OFAC. Maintaining the integrity of U.S. sanctions is a high priority for OFAC and is the driving principle behind its rigorous review process that evaluates every request for removal individually on its merits and applies consistent standards to all of them.'

38 See, e.g., *Olenga v. Gacki*, 507 F. Supp. 3d at 264 ('the President has broad authority under [the International Emergency Economic Powers Act (IEEPA)] and could reasonably conclude that the deterrence of international bad actors, at least at times, requires the imposition of sanctions on those who have retired or moved on to other pursuits'); *Karadzic v. Gacki*, 2022 U.S. Dist. LEXIS 82768 at *18,3 (D.D.C. 2022) (finding that OFAC could sanction someone found to 'have actively obstructed' and that delisting by OFAC for changed circumstances fell under permissible rather than obligatory language with the use of the word 'may'); Executive Order 14024, 31 C.F.R. Appendix A to Part 587 (2021); Executive Order 14046, 31 C.F.R. Part 550 (2021); Executive Order 14038, 86 Federal Register 43,905 (11 August 2021).

39 31 C.F.R. § 501.807.

40 US Dep't of Treasury, Filing a Petition for Removal from an OFAC List (footnote 8).

41 For example, Section 8 of Executive Order 14024 delegates to the Secretary of the Treasury all powers granted to the President by the IEEPA, and it authorises the Secretary to re-delegate all those functions and powers to other agencies within the Department of the Treasury. Furthermore, the Secretary of the Treasury's delegation authority expands beyond

Pursuant to 31 CFR Section 501.807, '[a] person blocked . . . or a person owning a majority interest in a blocked vessel may submit arguments or evidence that the person believes establishes that insufficient basis exists for the designation.' 'A request for reconsideration – also sometimes called a delisting request – may include arguments or evidence rebutting [OFAC's] "basis . . . for the designation," or "assert that the circumstances resulting in the designation no longer apply."'[42] In other words, the designated person must argue that 'whatever rationale led to the designation was never true or is no longer true'.[43] A blocked person may also propose remedial steps, such as corporate reorganisation or the resignation of persons from positions in a blocked entity, that may negate the basis for designation.[44]

OFAC guidance[45] further lists circumstances that could lead to an entity's or individual's removal from the SDN List: 'the death of an SDN';[46] the fact that a

---

the Department of the Treasury, and, pursuant to Section 587.802 of the Russian Harmful Foreign Activities Sanctions Regulations, the Secretary of the Treasury may delegate to 'any person', any action the Secretary is authorised to take pursuant to Executive Order 14024 and any further executive order issued pursuant to the emergency declared within.

42 *Zevallos v. Obama*, 793 F.3d 106, 110 (D.C. Cir. 2015) (citing 31 C.F.R. § 501.807).

43 ibid.

44 Letter from US Dep't of Treasury to Senator Mitch McConnell, 19 December 2018, p. 2, at https://ofac.treasury.gov/system/files/126/20181219_notification_removal.pdf.

45 US Dep't of Treasury, Filing a Petition for Removal from an OFAC List (footnote 8).

46 See, e.g., Press Release, US Dep't of Treasury, 'Treasury Delists Former Honduran Money Launderer and Associated Companies' (25 August 2020), https://home.treasury.gov/news/press-releases/sm1106 (announcing the delisting of, inter alia, an individual who died subsequent to being added to the SDN List).

'designation was based on mistaken identity';[47] 'a positive change in behavior';[48] or the fact that 'the basis for the designation no longer exists'.[49]

After a party has petitioned for removal from the SDN List, OFAC reviews the petition and 'may request clarifying, corroborating, or other additional information'.[50] OFAC guidance states that '[i]f needed, OFAC typically

47 See, e.g., Daphne Psaledakis and Luc Cohen, 'Cooking oil or crude? Italian restaurant owner was mistaken target of U.S. sanctions', Reuters (1 April 2021), www.reuters.com/article/us-usa-sanctions-venezuela/cooking-oil-or-crude-italian-restaurant-owner-was-mistaken-target-of-u-s-sanctions-idUSKBN2BO6V8; see also Press Release, US Dep't of Treasury, 'Venezuela-related Designations Removals' (31 March 2021), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210331.

48 See, e.g., Press Release, US Dep't of Treasury, 'Treasury Delists Former Honduran Money Launderer and Associated Companies' (footnote 46) (announcing the delisting of, inter alia, five companies and stating that '[t]his delisting serves as a successful example of the ultimate goal of the Administration's use of sanctions as a tool – to bring about a positive change in behavior' where, '[f]ollowing OFAC's designation, Honduran authorities seized or took control over multiple entities and properties owned by' a 'Money Laundering Organization'); Press Release, US Dep't of Treasury, 'Treasury Removes Sanctions Imposed on Former High-Ranking Venezuelan Intelligence Official After Public Break with Maduro and Dismissal' (7 May 2019), https://home.treasury.gov/news/press-releases/sm684 (announcing delisting of a Venezuelan former government official who 'broke ranks with the Maduro regime and rallied to the support of the Venezuelan constitution and the National Assembly', explaining that '[t]oday's action, taken in consultation with the U.S. Department of State, demonstrates that U.S. sanctions need not be permanent and are intended to bring about a positive change of behavior').

49 See, e.g., Press Release, US Dep't of Treasury, 'OFAC Delists En+, Rusal, and EuroSibEnergo' (27 January 2019), https://home.treasury.gov/news/press-releases/sm592 (removing companies from the SDN List where, per the terms of their removal, the companies reduced a designated individual's 'direct and indirect shareholding stake in these companies and severed his control'); Press Release, US Dep't of Treasury, 'Treasury Amends Burmese Sanctions Regulations, Identifies Blocked Companies Owned By Designated Persons, And Delists Several Burmese State-Owned Entities' (17 May 2016), https://home.treasury.gov/news/press-releases/jl0458 (announcing the delisting of several state-owned entities where '[t]hese removals support U.S. foreign policy goals and acknowledge the changing circumstances in Burma. The entities being removed are organized under civilian line ministries or no longer exist'); see also Press Release, US Dep't of Treasury, 'Treasury Removes Sanctions on Latvia's Ventspils Freeport Authority' (18 December 2019), https://home.treasury.gov/news/press-releases/sm860 (announcing delisting of an entity that OFAC had designated for being owned or controlled by a Global Magnitsky-designated individual where, '[f]ollowing the designation of [the individual] and [the entity], the Latvian government passed legislation effectively ending [the individual's] control of the [entity]'. Following the designation, the individual also resigned from the entity.).

50 31 C.F.R. § 501.807(b).

endeavors to send the first questionnaire within 90 days from the date the petition is received by OFAC'.[51] Because these requests for information may result in further questions, 'it is not uncommon for OFAC to send one or more follow-up questionnaires and to engage in additional research to verify claims made by a petitioner'.[52] Parties seeking removal may also request a 'meeting' with OFAC, although these meetings are not required and OFAC is not required to grant a meeting request.[53] Further, '[a]s part of the agency's reconsideration process, designated individuals may request disclosure of the administrative record supporting the designation decision'.[54] OFAC ultimately renders a decision in writing.[55]

The length of the removal process is case-specific, and there is no prescribed review period for rendering a decision. OFAC guidance states that:

> *Though each case is unique, OFAC applies the same standards to petition reviews across all sanctions programs. The timing of a review depends upon a range of factors including whether OFAC needs additional information, how timely and forthcoming the petitioner is in responding to OFAC's requests, and the specific facts of the case. Incomplete answers to questionnaires or incomplete documentation often cause delays.*[56]

If OFAC rejects a petition for removal, a party may reapply – although, without new arguments or evidence, or a change in circumstances, the outcome will, in the absence of an independent decision to delist, remain the same.[57] '[T]here is "no limit on the number of times a designated person can request delisting."'[58]

---

51 See US Dep't of Treasury, Filing a Petition for Removal from an OFAC List (footnote 8).

52 ibid.

53 31 C.F.R. § 501.807(c).

54 *Fares v. Smith*, 901 F.3d 315, 319 (D.C. Cir. 2018).

55 See 31 C.F.R. § 501.807(d).

56 See US Dep't of Treasury, Filing a Petition for Removal from an OFAC List (footnote 8).

57 ibid. ('You may reapply using the same process as for the original petition. If you present new arguments and evidence, OFAC may reach a different conclusion. However, if you fail to present new arguments or evidence, and there has been no change in circumstances, OFAC will again deny your application.').

58 *Fares v. Smith*, 901 F.3d at 326 (quoting *Zevallos*, 793 F.3d at 115 (citing 31 C.F.R. § 501.807)); see also *Zevallos*, 793 F.3d at 110 ('A designated person can request delisting as many times as he likes' (citing § 501.807)); *Rakhimov v. Gacki*, No. 19-2554, 2020 US Dist. LEXIS 68764, at 2 (finding, in addressing the plaintiff's Administrative Procedure Act (APA) claims, that the agency's initial designation of the plaintiff was reasonable and that his procedural challenges were unavailing, but noting that he was 'free to pursue the available administrative reconsideration process and to obtain judicial review of Defendants' ensuing decision' (citations omitted)).

Listed parties may have a statutory right to seek judicial review.[59] Thus, '[i]f OFAC denies a request for reconsideration, the blocked person may challenge that determination under the [Administrative Procedure Act] in federal court.'[60] A listed party may 'bypass the administrative-delisting process altogether and immediately challenge the agency's designation'.[61] Listed parties pursuing delisting litigation should, however, be aware that the relevant judicial standard of review in cases challenging an OFAC designation decision is a very deferential one. Courts will 'set aside OFAC's designation only if it is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law."'[62] Thus, where the evidence 'provides adequate basis to justify Treasury's determination',[63] courts will deny the petitioner's application for delisting. However, where OFAC refuses to provide reasons for the investigation and designation – if, for example, the evidence is classified – courts have found a due process violation.[64] Similar constitutional violations have been found where OFAC fails to obtain a warrant before seizing assets, violating the Fourth Amendment.[65] However, with respect to constitutional claims, the government's motion to dismiss has been granted where the court finds that a foreign national lacks standing to assert these claims.[66]

---

59 See, e.g., 5 USC § 702 ('A person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action within the meaning of a relevant statute, is entitled to judicial review thereof.').

60 *Rakhimov*, 2020 US Dist. LEXIS 68764, at 5 (D.D.C. 20 April 2020) (citations omitted); see also *Al Haramain Islamic Foundation, Inc v. U.S. Dep't of Treasury*, 686 F.3d 965, 1027 (9th Cir. 2011) (noting that the plaintiff-appellant (unsuccessfully) challenged OFAC's 'specially designated global terrorist' designation in court after receiving no response from OFAC to its request for administrative reconsideration); *Rakhimov*, No. 19-2554, at 5 (stating that the plaintiff initially requested the rescission of his designation; he later (1) requested a temporary stay of his delisting request and (2) filed suit, 'arguing, inter alia, that OFAC's failure to provide him with the administrative record underlying his designation violated the APA' (citations omitted)).

61 *Rakhimov*, 2020 US Dist. LEXIS 68764, at 4; see *Olenga v. Gacki*, 507 F. Supp. 3d 260, 264 (D.D.C. 2020) (stating that the SDN-listed plaintiff filed a lawsuit while the administrative reconsideration process was ongoing); *Holy Land Foundation v. Ashcroft*, 333 F.3d 156, 160 (D.C. Cir. 2003), cert. denied, 540 US ___ (2004) (stating that, soon after being designated as a Specially Designated Terrorist and as a Specially Designated Global Terrorist, an entity filed a lawsuit challenging its designations and the seizure of its assets, and alleging violations of, inter alia, its constitutional rights and its rights under the APA).

62 See, e.g., *Al Haramain Islamic Foundation*, 686 F.3d, at 1029; see also 5 USC § 706.

63 *Zevallos*, 793 F.3d, at 114.

64 *Al Haramain Islamic Foundation*, 686 F.3d, at 1027.

65 ibid.

66 *Fulmen Co. v. Office of Foreign Assets Control*, 547 F. Supp. 3d 13, 14 (D.D.C. 2020), at 10.

Public relations and reputational issues for both the client and the lawyer

Sanctioned individuals and their attorneys both face unique reputational and public relations issues. For sanctioned individuals, the reputational harm associated with being designated is often catastrophic to their business and personal interests, as fear of being blocked from the US economy can trigger their counterparties to engage in de-risking activity, meaning that many counterparties that may legally transact business with the sanctioned party may nonetheless choose to end the relationship merely because of the perceived risk of running afoul of the sanctions. Counterparties may cease all transactions and cancel contracts and financial institutions may close accounts, even if they are not subject to US sanctions. For those clients engaged in authorised business with a sanctioned party or in a sanctioned country, the reputational risks of being associated with a sanctioned person are also quite high, especially given that OFAC has been known to designate persons based on open-source reporting, and the mere association with a sanctioned person could result in a designation.

Even when sanctions are lifted, the stigma of a listing can linger. Once publicly associated with the activity that led to the listing, formerly sanctioned parties and parties operating in sanctioned countries may face public demands for counterparties to cancel contracts or for local partners to divest from their investments.

Legal counsel can assist in alleviating many of these reputational harms. For example, counsel can interface with counterparties that are skittish about continuing to transact with the sanctioned party and potentially provide comfort that proposed activity is, in fact, not prohibited by the sanctions listing. Counsel can also advise on the legality of divestments and corporate reorganisations to allow entities that are majority owned by a sanctioned party to continue their business in accordance with the sanctions. To the extent that a sanctioned party is cut off by financial institutions, US counsel can advise on securing financing from other institutions to ensure compliance with the sanctions regime that led to the listing. And, of course, counsel can advise and represent the sanctioned person in obtaining delisting.

Lawyers, too, face reputational risks for representing sanctioned parties. Although the American Bar Association, which publishes Model Rules of Professional Conduct for attorneys, states in Model Rule 1.2(b) that '[a] lawyer's representation of a client, including representation by appointment, does not constitute an endorsement of the client's political, economic, social or moral views or activities', it is not unusual for lawyers to be publicly criticised for representing unpopular or controversial clients. This consideration is particularly acute when representing sanctioned persons, largely because sanctions regimes are inherently

political and often exist at the cross section of foreign policy and national security, and an attorney for a sanctioned person may be perceived as operating contrary to the national interest or be labelled 'un-American'.

This desire to dissociate with sanctioned bad actors may also be brought on by economic concerns on the part of the attorney. Specifically, a law firm risks losing or failing to retain clients that may not want to be represented by a firm representing sanctioned persons. This loss may extend to employees as well, who may shift to a competing firm following a decision of the initial firm to represent a particularly controversial client.

These issues can be particularly difficult to navigate when there are sudden political shifts or unforeseen international crises. For example, after Russia annexed Crimea in 2014, the United States instituted a sanctions regime on Russia, yet many US law firms continued to represent Russian nationals (including Russian 'oligarchs') and operate offices in Russia. But when Russia invaded Ukraine in February 2022, the international outrage caused an unprecedented number of multinational law firms to shutter offices in Moscow, dissociate with Russian clients and refuse to onboard new clients associated with the Russian economy or regime.

Fear of reputational harm may lead attorneys to terminate sanctioned clients, even mid-litigation.[67] If a case is pending in court, a lawyer's effort to withdraw from a client's case may require court approval.[68] In other legal matters that do not require court approval, lawyers who wish to withdraw from representation of a client must ensure that they are complying with ethics rules in their jurisdiction and that clients will not face a 'material adverse effect' from their withdrawal.[69] Failure to do so could lead to disciplinary complaints and malpractice lawsuits, although the latter is less likely in the absence of evidence of actual harm to the client.

67 www.reuters.com/legal/transactional/some-law-firms-dropping-russian-clients-us-courts-have-final-say-2022-03-15/.

68 American Bar Association (ABA) Model Rule 1.16(c) ('A lawyer must comply with applicable law requiring notice to or permission of a tribunal when terminating a representation.').

69 ABA Model Rule 1.16(b(1) ('a lawyer may withdraw from representing a client if . . . withdrawal can be accomplished without material adverse effect on the interests of the client.').

It is therefore imperative for any sanctions attorney to weigh the advantages and disadvantages of representing a sanctioned client. It is also critical to do a thorough background check as due diligence and vetting are critical in assessing whether a sanctioned client's case presents reputational issues that are insurmountable. Beyond what the client discloses, a comprehensive dive into the potential client's past and records may turn up information that affects the lawyer's decision to represent the party.

APPENDIX 1

Comparison of Select Sanctions Regimes

The following table provides a high-level comparison of the thematic sanctions regimes of the United Nations, the United States, the European Union and the United Kingdom. Although the purpose, details and targets of each jurisdiction's programmes may vary, there is a high degree of overlap between the four jurisdictions when it comes to the themes that are addressed by sanctions. This table is up to date as at August 2023.

Type of sanction	United Nations	United States	European Union	United Kingdom
Afghanistan (including Taliban)	X	X	X	X
Anti-boycott (i.e., blocking statutes)				
– of Cuba			X	X
– of Iran			X	X
– of Israel		X		
Balkans (Bosnia and Herzegovina[1])		X	X	X
Belarus		X	X	X
Burundi			X	X
Central African Republic	X	X	X	X
Chemical weapons		X	X	X
Chinese military companies		X		
Counter narcotics		X		
Cuba		X		
Cyber-related		X	X	X
Democratic Republic of Congo	X	X	X	X

1 The EU and UK sanctions are limited to Bosnia and Herzegovina while the US sanctions are wider.

Type of sanction	United Nations	United States	European Union	United Kingdom
Democratic People's Republic of Korea (North Korea)	X	X	X	X
Ethiopia (including Eritrea)		X		
Foreign interference in elections		X		
Foreign sanctions evaders		X		
Guinea			X	X
Guinea-Bissau	X		X	X
Haiti	X		X	X
Hong Kong		X		
Hostages/wrongfully detained nationals		X		
Human rights/corruption (Magnitsky)		X	X[2]	X
Iran	X	X	X	X
Iraq	X	X	X	X
Lebanon	X	X	X	X
Libya	X	X	X	X
Mali	X	X	X	X
Moldova			X	
Myanmar (Burma)		X	X	X
Nicaragua		X	X	X
Non-proliferation		X		
Russia		X	X	X
Secondary sanctions[3]				
– re: Hezbollah		X		
– re: Hong Kong		X		
– re: Iran		X		
– re: North Korea		X		
– re: Russia/Ukraine		X		

2 The EU sanctions are limited to human rights.

3 While the EU and UK are not generally considered to have secondary sanctions regimes, the designation criteria under the UK Sanctions and Anti-Money Laundering Act may be applied to a person 'acting on behalf of or at the direction of' or who 'is a member of, or associated with' a person subject to designation, which could provide a basis for the development of UK secondary sanctions.

Type of sanction	United Nations	United States	European Union	United Kingdom
– re: Syria		X		
– re: terrorism		X		
Somalia	X	X	X	X
South Sudan	X	X	X	X
Sudan (including Darfur)	X	X	X	X
Syria	X	X	X	X
Terrorism (including ISIL/Daesh and Al-Qaida)	X	X	X	X
Transnational criminal organisations		X		
Tunisia			X	
Turkey		X[4]	X	X
Ukraine (including Crimea, Donetsk, Kherson, Luhansk and Zaporizhzhia)		X	X	X
Venezuela		X	X	X
Yemen	X	X	X	X
Zimbabwe		X	X	X

4 The US sanctions are applied through the Countering America's Adversaries Through Sanctions Act-related sanctions programme, rather than a Turkey-specific sanctions programme.

APPENDIX 2

About the Authors

Ama Adams

Ropes & Gray LLP

Ama Adams is managing partner of the Washington, DC, office in the firm's litigation and enforcement practice. She has over 20 years of experience advising clients on international transactions and the US government's regulation of trade and investment. Most notably, this includes export controls, economic sanctions, anti-corruption and anti-money laundering, foreign direct investment and customs laws and regulations. She advises clients on these complex issues in a range of industries, including the financial services, aviation, biotechnology, life sciences, oil and gas, manufacturing, technology and chemical sectors.

In addition to advising clients on the application of international trade regulations to their global business operations, Ama also assists clients in developing compliance programmes, handling pre- and post-acquisition due diligence, conducting internal investigations relating to potential violations of trade laws and representing clients before the US government agencies in connection with licence requests, enforcement matters and government inquiries. She also advises clients on cross-border investment and national security matters, including national security reviews and investigations before the Committee on Foreign Investment in the United States (CFIUS). Ama has successfully represented a number of foreign and domestic clients through the CFIUS clearance process and regularly advises clients on managing CFIUS risks across investment scenarios.

Farhad Alavi
Akrivis Law Group, PLLC

Farhad Alavi's practice focuses on complex trade issues related to compliance with and enforcement of US national security, including sanctions, export controls, customs and anti-corruption, as well as cross-border transactions, investment and banking matters. He represents clients around the world, such as major multinationals, middle market businesses and high net worth individuals.

Mr Alavi regularly represents clients before the US Department of the Treasury's Office of Foreign Assets Control, the Department of Commerce's Bureau of Industry and Security and Customs and Border Protection on sanctions, export controls and customs compliance and enforcement matters. He also represents clients before the Department of Justice on white-collar criminal defence issues related to national trade laws.

Renato Antonini
Steptoe & Johnson LLP

Renato Antonini is the managing partner of Steptoe's Brussels office.

For over 20 years Renato has represented clients on global trade legal and regulatory issues, in particular advising on EU trade matters, such as EU trade remedies investigations, sanctions, export controls and customs, as well as World Trade Organization trade law and trade remedies investigations in other jurisdictions.

He has a track record of achieving successful outcomes for clients before EU courts, the European Commission and national regulators. Renato successfully assisted Jinan Meide Casting Co Ltd, one of the largest manufacturers in the world, in two landmark judgments of the EU General Court concerning imports of threaded tube or pipe cast fittings, of malleable cast iron, originating in China. He also represented Jindal Saw Ltd, an international manufacturer headquartered in India, in two landmark judgments concerning imports of tubes and pipes of ductile cast iron originating from India.

Renato advises international companies operating globally, and across all industries, including steel manufacturing, chemicals, energy and financial services, as well as sovereign states.

Sophie Armstrong
Baker McKenzie

Sophie Armstrong is an associate in the London office and joined Baker McKenzie in 2018. Her practice focuses on compliance with EU and UK sanctions, export controls and customs regulations, as well as compliance with the UK Bribery Act. Sophie advises clients in a number of sectors, including energy, manufacturing, telecoms, retail, financial services and consumer goods.

Rachel Barnes KC
Three Raymond Buildings

Dr Rachel Barnes KC is a dual-qualified US attorney and English barrister. She is recognised as a leading practitioner in the area of sanctions, as well as corruption, financial and corporate crime, international crime, extradition and mutual legal assistance, and proceeds of crime and asset recovery.

Rachel has a wealth of sanctions experience as a practitioner, academic and expert witness. She is 'one of the best navigators of the complex financial and trade sanctions regime' (*Chambers UK* 2018), 'go-to counsel on matters with a transatlantic element' (*Chambers UK* 2019), 'pragmatic, hands-on, easy to work with, always available' and 'devastatingly well prepared in court' (*Chambers UK* 2020), 'the first and last stop for financial sanctions advice' (*Chambers UK* 2021) and 'has a specialist [sanctions] practice, is very knowledgeable and has excellent judgement' (*Chambers UK* 2022).

Rachel regularly acts in both domestic and international sanctions cases. As an English barrister, Rachel both prosecutes and defends in criminal cases, and civil and public law crime-related matters. Her clients include governments, corporations, non-governmental organisations and individuals. She is prosecuting counsel for the UK's Serious Fraud Office and Financial Conduct Authority and appointed to the Attorney General's specialist panel of public international law counsel. Rachel appears in cases in the Crown Court, the High Court, the Court of Appeal and the UK's Supreme Court, as well as acting for a number of successful petitioners before the UN Ombudsperson. Rachel previously taught law at Cambridge University and the London School of Economics and Political Science. After graduating from Harvard Law School, Rachel began her legal career as a litigation attorney at Shearman & Sterling, New York. She was awarded her doctorate in public international law from Cambridge University.

Julie Bastien

Bonifassi Avocats

Julie Bastien specialises in international and European law. Her practice focuses on litigation related to international sanctions and in proceedings concerning the recognition and enforcement of arbitral awards and foreign judgments. Her experience also includes criminal law cases in the cross-border context.

Elissa N Baur

McGuireWoods LLP

Elissa Baur focuses her practice on white-collar and antitrust criminal defence matters, including internal investigations, litigation and regulatory enforcement actions. She has defended clients in numerous government investigations before the Department of Justice, the United States Office of Special Counsel, the Securities and Exchange Commission, the Department of Treasury's Financial Crimes Enforcement Network, the Office of the Comptroller of Currency and the Federal Reserve Board, among others.

Elissa is a member of McGuireWoods' government investigations and white-collar litigation department, which was recognised by *Law360* as a Practice Group of the Year. She has particular experience conducting internal investigations and advising clients on compliance with the US Foreign Corrupt Practices Act and other anti-corruption laws. Her practice also includes representing companies and financial institutions in connection with regulatory, civil and criminal enforcement actions arising from US anti-money laundering laws and regulations. She speaks Spanish and Portuguese and uses her language skills regularly in her practice.

John Bedford

Dechert LLP

John Bedford is an experienced litigator and investigations lawyer who advises leading financial institutions, corporations and high net worth individuals on financial crime compliance, commercial litigation, white-collar investigations and international arbitration. He has over a decade of experience representing clients in domestic and international disputes and investigations covering a wide range of industries, including financial services, e-commerce, payment services, manufacturing and life sciences.

Mr Bedford has advised corporations and board committees on the conduct of investigations into allegations of bribery, corruption, money laundering, fraud and breach of domestic and international sanctions or export controls. These matters have involved prosecutors, regulators and enforcements agencies, including the Financial Conduct Authority, the Serious Fraud Office, the National Crime

Agency, the US Department of Justice, the Securities and Exchange Commission, the Office of Foreign Assets Control and the Parquet National Financier. He also has extensive experience in corporate compliance monitorships.

Mr Bedford regularly undertakes financial crime compliance advisory work, including drafting and implementing policies and procedures and advising money laundering reporting officers on their reporting obligations under the suspicious activity reports regime. He also conducts training sessions for clients on these topics.

Stéphane Bonifassi

Bonifassi Avocats

Stéphane Bonifassi represents individuals and companies accused of international corruption and business crime in multiple jurisdictions. He is a go-to litigator with decades of experience, and the majority of his cases involve mutual assistance, criminal freezing orders, sanctions and extradition.

Mr Bonifassi is a co-founder of the International Academy of Financial Crime Litigators, a collaboration of experienced public and private litigation professionals and distinguished academics working with the Basel Institute on Governance to expand worldwide access to solutions in economic crime cases.

James Bowen

Linklaters LLP

James Bowen is a solicitor at Linklaters with broad experience in sanctions, white-collar crime, investigations and commercial dispute resolution. Since February 2022, he has been extremely involved in advising a broad range of corporate and financial institution clients on the United Kingdom's Ukraine-related sanctions regime, and on winding down their operations in Moscow, with previous sanctions experience covering the 2014 Russia restrictions and the Iran regime. Recent sanctions work has included advising a range of financial institutions on the application of the oil price cap and advising a number of funds on the UK professional and trust services restrictions. James has a particular interest in the interaction of sanctions and litigation/restructuring.

Alex J Brackett

McGuireWoods LLP

Alex Brackett is a member of the government investigations and white-collar litigation department, and co-head of McGuireWoods' strategic risk and compliance team. His practice focuses primarily on advising and supporting corporate and individual clients in the areas of white-collar criminal defence and internal

investigations. He has a particular focus on financial industry investigations and anti-corruption laws such as the US Foreign Corrupt Practices Act, export control laws and sanctions and trade restrictions, including those administered by the Office of Foreign Assets Control, in addition to general white-collar defence and corporate compliance matters. His client work has taken him to 21 countries on six continents.

Alex has participated in numerous internal investigations for large corporate clients and in the defence of criminal and regulatory investigations involving alleged violations of export control laws, healthcare fraud, mortgage fraud, securities fraud, financial fraud, environmental crimes and bribery. He also has experience in related civil litigation, including the defence of False Claims Act/qui tam litigation from initial Department of Justice investigations to resolution, and the defence of claims arising under Title III of the Helms–Burton Act.

Anna Bradshaw

Peters & Peters Solicitors LLP

Dr Anna Bradshaw is a partner in the business crime team at Peters & Peters Solicitors LLP, where she advises on sanctions and trade controls as part of her wider financial crime practice. In addition to compliance advice, she assists with investigations into suspected breaches and related reporting obligations and represents individuals and corporates in contentious proceedings. She also acts for designated persons in legal and administrative challenges to sanctions listings. Anna regularly publishes and speaks in the United Kingdom and abroad on topics relating to sanctions and financial crime. She is an Associate Fellow of the Royal United Services Institute and assists its Centre for Financial Crime and Security Studies with its research on US, EU and UK sanctions.

John D Buretta

Cravath, Swaine & Moore LLP

John D Buretta, a former senior US Department of Justice (DOJ) official, focuses his practice on advising corporations, board members and senior executives with respect to internal investigations, criminal defence, regulatory compliance and related civil litigation. His clients have included global companies, boards of directors, audit committees, individual board members, company owners, senior management of public and private companies, general counsel and other in-house counsel of public companies, law firms and former US and foreign government officials. Mr Buretta has handled a variety of sensitive investigative matters concerning the Foreign Corrupt Practices Act (FCPA), antitrust laws, securities fraud and disclosure regulations, money laundering and anti-money laundering

controls, trade sanctions, export controls, cyber intrusion and tax compliance. Mr Buretta completed his time at the DOJ as the number two ranking official in the Criminal Division as Principal Deputy Assistant Attorney General and Chief of Staff.

Mr Buretta also served as Deputy Assistant Attorney General for the DOJ Criminal Division, when he oversaw the Criminal Division's Fraud Section, among others, including the DOJ's FCPA Unit. In 2011, Mr Buretta was appointed Director of the Deepwater Horizon Task Force. Prior to joining the Criminal Division, Mr Buretta served for eight years as an Assistant US Attorney in the US Attorney's Office for the Eastern District of New York, and was Chief of the Office's Organized Crime and Racketeering Section from 2008 to 2011.s

Ali Burney

Steptoe & Johnson HK LLP

Ali Burney is a partner in Steptoe & Johnson's Hong Kong office. Ali's practice focuses on representing US and non-US clients in the Asia-Pacific region on matters related to US economic sanctions, export controls, the US Foreign Corrupt Practices Act and anti-money laundering laws.

Ali has extensive experience representing clients in front of the US Department of Justice, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) and the US Department of Commerce's Bureau of Industry and Security (BIS). His experience includes conducting cross-border investigations, filing voluntary self-disclosures, responding to subpoenas, obtaining OFAC licences, conducting risk assessments and representing individuals and companies seeking removal from OFAC's Specially Designated Nationals and Blocked Persons List and the BIS Entity List.

He also frequently advises companies investing in high-risk sectors and countries on sanctions, anti-bribery and corruption and export control-related pre-acquisition due diligence and post-acquisition compliance programme implementation.

Orga Cadet

Baker & Hostetler LLP

Orga Cadet is an associate in BakerHostetler's international trade and national security team. His practice focuses on the intersection of trade, technology and national security. Specifically, Mr Cadet advises clients on complex trade and national security statutes and regulations, including in the context of US sanctions, export controls and defence security matters, as well as on reviews by the

Committee on Foreign Investment in the United States. He draws from his prior experience as an international trade attorney with the US Department of Commerce and as a legal adviser on international conflict resolution.

Mr Cadet is a vice chair of the American Bar Association's Section of International Law National Security Committee. He also currently serves on Law360's International Trade Editorial Advisory Board.

Jona Boscolo Cappon

Forensic Risk Alliance

Jona Boscolo Cappon is a director based in FRA's London office. He has over 10 years' experience in applying data analytics, information technology and novel computational methods to solve complex business problems and drive data-informed decisions. He specialises in delivering analytics-driven solutions to global financial and non-financial institutions to help them respond to business-critical events by identifying, quantifying and mitigating risks. Jona has led forensic technology teams to design fraud detection analysis, develop monitoring capabilities and support clients across the public, corporate and financial sectors to respond to global regulators. He has experience in leading forensic investigations and complex regulatory compliance projects covering issues relating to fraud, bribery, anti-money laundering, sanctions violations, customer contract breaches and other complex financial crimes. While at FRA, Jona has focused on network analytics, graph databases and natural language processing techniques to automate the analysis and linking of a variety of data sets and uncover entities with sophisticated organisational structures involved in money laundering. Prior to joining FRA, Jona spent six years in the forensic technology team of a Big Four firm, where he led teams with disparate backgrounds to investigate regulatory breaches through the development of tailor-made software and interactive visualisations.

Edwin O Childs, Jr

McGuireWoods LLP

Edwin Childs is a government contract and investigations and enforcement attorney who represents companies across a wide range of sectors, including the defence, services, technology and aerospace industries. His practice, spanning more than a decade in Washington, DC, encompasses a broad array of legal services, including government contract investigations, disclosures and regulatory enforcement actions; bid protests and government contract disputes; government

contract counselling; export licensing and enforcement; prime contractor–subcontractor disputes; corporate ownership and acquisition issues; and election law investigations and enforcement matters.

Ned advises clients on legal issues affecting national security. He represents clients in matters before the Defense Security Service, the US Department of Commerce's Bureau of Industry and Security, the US Department of State's Directorate of Defense Trade Controls and the US Department of the Treasury's Office of Foreign Assets Control, as well as the Committee on Foreign Investments in the United States and its stakeholder agencies.

Jason H Cowley

McGuireWoods LLP

Jason Cowley is a member of McGuireWoods' government investigations and white-collar litigation department and its securities enforcement and litigation practice group. He principally represents financial institutions (including investment funds), corporations and executives in criminal investigations and trials, regulatory enforcement proceedings and complex civil litigation. Jason has particular expertise in matters involving securities and commodities fraud, cross-border enforcement issues, anti-money laundering issues and criminal and civil asset forfeiture.

Before joining McGuireWoods, Jason served for over 13 years in the US Department of Justice as an Assistant United States Attorney in the Southern District of New York (SDNY) and, prior to that, the Eastern District of North Carolina. In the SDNY, he held key leadership positions, serving for over three years as co-chief of the Securities and Commodities Fraud Task Force and as chief of the Money Laundering and Asset Forfeiture Unit. During his tenure as chief of the Money Laundering and Asset Forfeiture Unit, Jason was the office's principal adviser on money laundering and asset forfeiture issues and oversaw the investigation and prosecution of various money laundering offences, Bank Secrecy Act and anti-money laundering violations, and sanctions violations involving the illicit transfer of funds through the US financial system.

Nikki Cronin

Willkie Farr & Gallagher LLP

Nikki Cronin is an associate in Willkie's global trade and investment group in Washington, DC. Nikki advises clients on government regulations related to international trade and investment, with a particular focus on US economic sanctions. She regularly advises both domestic and foreign clients on compliance and

enforcement matters relating to US economic sanctions and export controls, including financial institutions, private equity firms and media companies, and in various industries, including oil and gas.

Samuel Cutler

Miller & Chevalier Chartered

Samuel Cutler is an associate in Miller & Chevalier's international department. He focuses his practice on export controls, economic sanctions, anti-money laundering, the Committee on Foreign Investments in the United States and other national security matters. He regularly advises clients on issues concerning the US Department of the Treasury's Office of Foreign Assets Control and the US Department of Commerce's Bureau of Industry and Security.

Prior to joining the firm, Mr Cutler worked as an associate at an *Am Law 50* law firm where he advised clients on economic sanctions, bank regulation and other corporate matters. He has experience in assisting with internal investigations, representation before federal agencies and compliance programme development.

Mr Cutler received his JD from the American University Washington College of Law and served on the *American University Law Review*. During law school, he held several roles concerning national security and trade, including a clerkship at the Department of Commerce in the Office of the Chief Counsel for Industry and Security.

Prior to law school, Mr Cutler spent several years consulting on US economic sanctions.

Robert Dalling

Jenner & Block London LLP

Robert Dalling is a partner in Jenner & Block's investigations, compliance and defence practice. Formerly a trial advocate with 10 years' courtroom experience, he has represented global financial institutions, multinational corporates and individuals in high-profile and high-value internal and external investigations involving a wide range of financial crime and other regulatory issues.

Rob has advised some of the world's largest financial institutions on financial sanctions, often in connection with complex and sophisticated financial products and transactions. He has experience in applying for licences from sanctions authorities in the United Kingdom. He advises companies on the development of internal policies (including on anti-bribery, anti-fraud, anti-money laundering and terrorist financing, conflicts of interest, gifts and hospitality, and supply chain

and modern slavery issues) and associated procedures, controls and training. He has assisted several clients with complex anti-money laundering issues and has dealt with the National Crime Agency on a large number of consent applications.

Prior to moving into private practice, Rob spent several years practising as a barrister in white-collar criminal litigation. Market commentators for *Chambers and Partners* 2020 describe him as an 'excellent' lawyer who is 'incredibly clever and very tactical'.

Sterling Darling

Linklaters LLP

Sterling Darling is a counsel in the Washington, DC, office, in the litigation, investigations and arbitration department. He regularly advises financial institutions, state-owned entities and multinational corporations on US sanctions issues and compliance with other US laws and regulations. As a litigator, Sterling's background is in structured product, securities and banking litigation, and his sanctions-related advice has a particular focus on the application of sanctions regulations to derivatives, structured products and other complex financial product transactions.

Stéphane de Navacelle

Navacelle

Stéphane de Navacelle practises corporate litigation, predominantly in criminal law, regulatory, internal investigations, compliance, complex commercial litigation, international arbitration and mediation, in New York, London and Paris.

With over 15 years' experience in investigations in France and abroad, led in part in connection with French, foreign or international organisations (at Engel & McCarney and Debevoise & Plimpton LLP), Stéphane advises entities in rolling out and auditing ethics and compliance programmes. As such, he has been appointed as an independent expert monitor in compliance (2017–2019, 2019–2021 and 2022–2024) by European groups operating globally, based on negotiated settlement agreements of the World Bank and the Inter-American Development Bank.

He is a former member of the Paris Bar Council (2017–2019) and has been secretary of the ethics commission and a member of the disciplinary reviews board of the Paris Bar. He is currently appointee for influence through law of the Paris Bar.

Stéphane was appointed as observer by the prosecutor for the international criminal tribunal for Rwanda (2009), and was a member of the board of directors of the Fondation de Coubertin (a French public interest Foundation, 2010–2016),

a fellow of the American Bar Foundation (2016), a member of the Recognition and Reparation Commission (a French independent committee on sexual abuse in the Catholic Church, 2019–2021), and a member of the French Health Ministry Commission for the fight against ill treatment and abuse and the promotion of fair treatment.

Satindar Dogra

Linklaters LLP

Satindar Dogra is widely acknowledged as an expert in sanctions, corporate crime and fraud. He leads the firm's sanctions practice and has developed the market standard in relation to Russian sanctions. He regularly advises clients on governmental investigations, including by the UK's Serious Fraud Office, the National Crime Agency and the Office for Financial Sanctions Implementation.

Ahmad El-Gamal

Willkie Farr & Gallagher LLP

Ahmad El-Gamal is an associate in Willkie's global trade and investment group in Washington, DC. Ahmad provides advice to both domestic and foreign clients on government regulation of international trade and investment, particularly with regard to the Committee on Foreign Investment in the United States, economic sanctions and export controls.

Paul Feldberg

Jenner & Block London LLP

Paul Feldberg is a partner in Jenner & Block's investigations, compliance and defence practice. Paul's practice is concentrated on advising and defending companies and individuals in matters relating to sanctions, export controls, criminal fraud, corruption, money laundering, insider trading and other regulatory actions. His experience includes working on some of the highest-profile UK Serious Fraud Office (SFO) cases, either as a prosecutor with the SFO or, more recently, in private practice, where he has acted for companies or individuals subject to investigations or prosecutions by the SFO and Financial Conduct Authority. Paul is also a highly experienced trial lawyer, having conducted trials and other court work on behalf of both corporations and individuals since 1997.

Paul previously served as a prosecutor at HMRC and at the SFO. He appeared as counsel in the House of Lords extradition case of *Re Gilligan, Re Ellis* ((2000) 1 All ER 113). He has been cited in *The Legal 500: UK* as a 'key figure who brings

significant private sector and fraud regulatory experience', while *Chambers and Partners* 2020 market commentators describe him as 'a pleasure to work with' and 'great at helping clients understand things from both sides of the fence'.

Anna Gaudoin

Jenner & Block London LLP

Anna Gaudoin is a senior associate in Jenner & Block's investigations, compliance and defence practice. Her practice focuses on white-collar criminal defence and investigations, regulatory enforcement and internal investigations. She has represented both individual and corporate clients in respect of investigations and enforcement proceedings initiated by, among others, the Serious Fraud Office, the Financial Conduct Authority, the National Crime Agency and the US Department of Justice. These matters often involve allegations of bribery and corruption, market abuse and various regulatory breaches, as well as reputational risk.

Tristan Grimmer

Baker McKenzie

Tristan Grimmer advises clients on the management and mitigation of risks under anti-bribery and corruption, international trade (trade sanctions and export controls) and competition laws. He focuses on providing compliance counselling and advising clients on the design and implementation of their corporate compliance programmes. Tristan also supports clients in the management of internal and external investigations.

Tristan has significant experience in the management of internal and external investigations by government authorities, regulators and prosecutors. He has advised clients on investigations by the Serious Fraud Office, the National Crime Agency, the European Commission, the Competition and Markets Authority and His Majesty's Revenue and Customs.

Brendan Hanifin

Ropes & Gray LLP

Brendan Hanifin provides clients with comprehensive regulatory and transactional counsel across a range of international risks, including foreign direct investment regulations, economic sanctions, anti-money laundering laws and anti-corruption laws. Clients value Brendan's breadth of regulatory knowledge, transactional proficiency and ability to forge practical solutions tailored to their business and strategic goals.

Brendan represents clients in national security reviews before the Committee on Foreign Investment in the United States (CFIUS), including reviews of non-notified transactions and negotiation of national security agreements. He routinely provides CFIUS-related advice and counselling to private equity sponsors, venture capital firms, sovereign wealth funds and US businesses throughout all stages of the investment life cycle.

Brendan also represents clients in multi-jurisdictional internal investigations and government enforcement actions. He has helped numerous clients to prepare and resolve disclosures to the Office of Foreign Assets Control, the Bureau of Industry and Security, the Directorate of Defense Trade Controls, the Department of Justice and the Securities and Exchange Commission.

Christine Sohar Henter

Barnes & Thornburg LLP

Christine Sohar Henter is a partner in Barnes & Thornburg LLP's Washington, DC, office. She specialises in international trade law with over 20 years of private and public legal experience. Christine represents US importers and exporters before federal agencies that administer international trade regulations, including the US Department of Commerce's Office of the Chief Counsel for Trade Enforcement and Compliance and the Bureau of Industry and Security, US Customs and Border Protection, the Census Bureau, the State Department's US Directorate of Defense Trade Controls, the US International Trade Commission (ITC) and the Office of Foreign Assets Control. She also advocates for clients on agency enforcement, whether in the context of investigations, penalties or voluntary disclosures, or as due diligence for mergers, acquisitions and investment transactions. She litigated a rare trade remedy case, *Eurodif v. US*, before the US Supreme Court.

Before joining Barnes & Thornburg, Christine was a senior attorney in the Office of the Chief Counsel for Trade Enforcement and Compliance at the US Department of Commerce, where she litigated numerous anti-dumping, countervailing duty and safeguard cases before the US Court of International Trade, the US Court of Appeals for the Federal Circuit, the US Supreme Court, World Trade Organization panels and Appellate Body, and North America Free Trade Agreement panels. Prior to working at the Department of Commerce, Christine served as a legal adviser for a commissioner and chairperson at the ITC and she assisted numerous companies with their export business through the Denver US Export Assistance Center.

Patrick Hill
Three Raymond Buildings

Patrick Hill represents and advises companies and individuals in matters relating to asset forfeiture, sanctions, complex fraud, money laundering and regulatory offences. He has acted in applications for delisting to the European Commission, the United Nations Security Council and the UN Ombudsperson.

Ningxin Huo
Global Law Office

Ningxin Huo is an associate at Global Law Office, Beijing. She specialises in international trade law, antimonopoly law and dispute resolution.

Ms Huo has advised a number of leading domestic and foreign companies in aerospace, banking, machinery, electronics, internet, AI and other sectors on export controls and economic sanctions.

Andris Ivanovs
Dechert LLP

Andris Ivanovs is a white-collar crime and international regulatory compliance lawyer who advises financial institutions, corporations and senior executives on regulatory and internal investigations and financial crime compliance matters. He regularly advises clients on government-initiated and internal multi-jurisdictional investigations into alleged violations of sanctions or export controls, bribery, corruption, money laundering, fraud and other sensitive matters. Mr Ivanovs has experience in acting for clients facing investigations and proceedings brought by UK, US and European enforcement or regulatory authorities.

In addition, Mr Ivanovs regularly counsels clients on proactive compliance and risk management under UK, EU and US anti-money laundering, anti-corruption and sanctions and export control laws, including in the context of cross-border transactions and business agreements. He has advised clients operating in the banking, private equity, defence, pharma, energy and other industries on developing and implementing best-practice anti-corruption, sanctions and export control, and anti-money laundering compliance programmes.

Karam Jardaneh
Jenner & Block London LLP

Karam Jardaneh is a senior associate in Jenner & Block's investigations, compliance and defence practice. Karam has experience in advising clients on internal investigations and external investigations conducted by the Serious Fraud Office and the Financial Conduct Authority. She also has extensive experience in advising

corporate and financial institutions in navigating UK and EU sanctions as well as export controls. This includes advice on policies and procedures to mitigate against the risks of breaching sanctions, and advice in connection with complex and sophisticated transactions. Karam has utilised her sanctions expertise in her pro bono practice, which includes providing advice in relation to sanctions and counterterrorist financing risks in relation to the provision of aid in conflict-affected areas.

Bridget Johnson
BDO USA, PA

Bridget Johnson is a manager in the data forensics practice at BDO USA, PA. She has significant experience applying data analytics to a range of compliance, legal and regulatory challenges. Bridget concentrates on architecting and operationalising data-driven solutions for large-scale monitorship and settlement programmes. Leveraging her experience on reactive matters, Bridget also develops proactive compliance analytics and fraud detection programmes for clients across a range of industries.

Bridget is a member of the team assisting the special compliance coordinator appointed by the US Department of Commerce to report on Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd's compliance with US export control laws and regulations. She focuses on the analytics and forensics testing aspect of this client project with a particular emphasis on supply chain.

Alistair Jones
Peters & Peters Solicitors LLP

Alistair Jones is a senior associate in the business crime and investigations team at Peters & Peters Solicitors LLP, specialising in sanctions delisting cases and sanctions compliance work. Alistair advises on a broad range of criminal and regulatory matters, including high-profile financial crime investigations and related requests for extradition, mutual legal assistance and INTERPOL notices. He trained and qualified into the international department of a top-tier firm where he acted in complex, multi-jurisdictional civil litigation, working on a number of cases that went to the Supreme Court. During this period, he was seconded to the UK Parliament, where he acted as the legal adviser to the Shadow Attorney General.

Eric J Kadel, Jr
Sullivan & Cromwell LLP

Eric Kadel is a partner in Sullivan & Cromwell's financial services group and is co-head of the firm's foreign investment and trade regulation, and economic sanctions and financial crime groups. He is a recognised leader advising clients on US economic sanctions and foreign investment issues in a wide variety of corporate, transactional and regulatory matters. Mr Kadel's expertise includes sanctions administered by the Treasury Department's Office of Foreign Assets Control, anti-money laundering laws under the Bank Secrecy Act, the Foreign Corrupt Practices Act and the transaction review process administered by the Committee on Foreign Investment in the United States. His practice also includes analysis of proposed transactions and business relationships, due diligence and design and review of compliance procedures and strategies, and internal investigations, voluntary disclosures and government enforcement actions.

Junsuk Lee
Ropes & Gray LLP

Junsuk Lee is an associate in Ropes & Gray's litigation and enforcement practice group. Junsuk focuses his practice on representing clients in relation to laws and regulations governing international trade and cross-border investment. He regularly advises clients on various US trade laws, including economic sanctions and export controls. He also advises regulatory compliance matters in connection with trade laws and assists with clients' internal investigations, as well as with investigations by various US governmental agencies related to those laws. In addition, he assists clients in navigating complex laws and regulations related to the Committee on Foreign Investment in the United States and anti-corruption matters.

Manuel Levitt
Miller & Chevalier Chartered

Manuel (Manny) Levitt is a senior associate in Miller & Chevalier's international department. He focuses his practice on economic sanctions and export controls.

Prior to joining the firm, Mr Levitt gained experience in international trade at an *Am Law 100* firm, where he helped global businesses address a wide variety of legal and regulatory challenges affecting their cross-border supply chains, transactions and operations. He has advised clients on matters related to regulations administered by US Customs and Border Protection, the Treasury Department's Office of Foreign Assets Control, the Commerce Department's Bureau of Industry and Security and the State Department's Directorate of Defense Trade

Controls. He also has experience helping clients comply with anti-corruption and anti-forced labour laws, assisting with internal investigations and representing clients before federal agencies.

Mr Levitt graduated with honours from the George Washington University Law School, where he was a member of the *Public Contracts Law Journal* and the Anti-Corruption and Compliance Association. He was awarded a Foreign Language and Areas Studies Fellowship, during which he studied Mandarin Chinese and took courses on Chinese legal institutions and Chinese business law.

Megan Y Lew

Cravath, Swaine & Moore LLP

Megan Y Lew is of counsel in Cravath's litigation department. Her practice focuses on internal and government investigations, civil litigation and regulatory compliance, including matters concerning the Foreign Corrupt Practices Act, fraud, money laundering and anti-money laundering controls, trade sanctions and export controls. Ms Lew has represented a wide range of clients, including AerCap Holdings NV, American Express, Computer Sciences Corporation, Mylan NV and Credit Suisse AG. She has also served on the attorney team supporting partner John D Buretta in his role as compliance monitor for TK Holdings, Inc (Takata) in connection with the recall of certain of Takata's airbag inflators.

She received a BS *magna cum laude* from Cornell University in 2004 and a JD *cum laude* from New York University School of Law in 2010, where she was a notes editor of the *Law Review*. Following her graduation, Ms Lew served as a law clerk to the Honourable Frank Maas of the US District Court for the Southern District of New York.

Barbara D Linney

Baker & Hostetler LLP

Barbara D Linney is a co-leader of the BakerHostetler international trade and national security team and has spent nearly three decades advising clients on international trade and business issues. Her multinational practice spans numerous industries, notably including the defence, aerospace, oil and gas, maritime, logistics and medical device industries. Ms Linney practises before various US federal agencies, including the Directorate of Defense Trade Controls, the Bureau of Industry and Security, the Office of Foreign Assets Control and the Committee on Foreign Investment in the United States. Licensed to practise law in three countries (the United States, Canada and the United Kingdom), she provides practical, business-oriented advice on a wide range of complex cross-border regulatory

requirements, from US and international export and import controls, anti-boycott rules and defence security requirements, to international economic sanctions and embargoes, foreign investment reviews and anti-corruption legislation.

Ms Linney serves as an adjunct professor at the Georgetown University Law Center, is frequently invited to speak on international trade and business issues at national and international conferences and is the author of numerous articles on international trade and business issues. She is a member of the American Bar Association's Section of International Law (SIL) and currently serves as a co-chair of the SIL National Security Committee. Ms Linney is also a member, a past president and pro bono general counsel of the Association of Women in International Trade (WIIT), as well as a recipient of the WIIT Lifetime Achievement Award. In addition, Ms Linney was named the WorldECR Practitioner of the Year in 2021.

Byron Maniatis

Steptoe & Johnson LLP

Byron Maniatis is a senior associate at Steptoe & Johnson. His practice focuses on several areas of EU and international trade law, including anti-dumping and anti-subsidy investigations, economic sanctions, export controls, customs law, free trade agreements, trade negotiations, EU internal market law and World Trade Organization dispute settlement. He frequently works with clients on matters before the European Commission and has assisted clients in the context of more than two dozen cases before the Court of Justice of the European Union.

In the field of trade remedies, Byron has assisted clients in several high-profile anti-dumping, anti-subsidy and safeguard investigations across the world. He regularly advises clients on compliance with economic sanctions, export controls and customs law, as well as on the EU Blocking Statute.

Byron also devotes a substantial part of his practice to pro bono initiatives.

Jacob M Marco

Sullivan & Cromwell LLP

Jacob Marco is an associate in Sullivan & Cromwell's general practice group. He represents clients in a wide range of corporate, transactional and regulatory matters, and focuses his work on economic sanctions, foreign investment reviews, anti-money laundering and financial regulatory and enforcement matters.

Laura C Marshall
McGuireWoods LLP

Laura Marshall is a partner in McGuireWoods' nationally recognised government investigations and white-collar litigation practice. She advises clients on a wide range of criminal, civil and regulatory enforcement matters. She has successfully defended companies and executives facing high-stakes investigations, criminal exposure and reputational risk. She also advises on compliance issues and has extensive experience managing risks associated with corruption, money laundering and economic sanctions.

Laura is ranked in *Chambers USA* for white-collar crime and government investigations in Virginia, and she was named a *National Law Journal* 'Criminal Law Trailblazer' and a *Benchmark* 'Local Litigation Star'. She has been consistently recognised for her work by Global Investigations Review, including as one of the top 100 'Women in Investigations' 'who are achieving great things in a competitive and notoriously tough area of law'.

Prior to joining McGuireWoods, Laura was the head of the white-collar defence and internal investigations team for an *Am Law 100* international firm. She also served for 15 years as an Assistant United States Attorney in the Eastern District of Virginia, handling numerous federal jury trials and successfully arguing five cases before the Fourth Circuit Court of Appeals.

Eva Monard
Steptoe & Johnson LLP

Eva Monard is a partner at Steptoe & Johnson. Her practice focuses on EU trade and customs law, World Trade Organization (WTO) disputes, trade remedies such as anti-dumping and anti-subsidy investigations, EU sanctions and trade controls, and EU internal market law. Eva represents international companies, associations and governments. She represents clients before EU institutions, including the European Commission, and before customs authorities of various EU Member States. Eva has extensive experience in litigating trade and internal market cases before the EU courts.

In the trade remedy area, she has assisted clients in more than 80 anti-dumping, anti-subsidy and safeguard investigations in various jurisdictions, and has obtained annulments of trade remedies imposed on imports. She also advises clients on their obligations under EU export control laws and sanctions by preparing compliance policies and by conducting due diligence of proposed transactions to ensure that clients meet their obligations on EU trade controls (e.g., in relation to military or dual-use items) and sanctions.

Eva advises clients on EU customs law, on issues such as classification, origin and valuation. She has guided several companies through pan-European customs investigations.

She assists governments at all stages of WTO dispute settlement proceedings, before panels and the Appellate Body. She also advises clients on the compatibility of national legislation with WTO trade laws and free trade agreements.

Navpreet Moonga

Dechert LLP

Navpreet Moonga is a dual qualified (US and UK) lawyer (working in Dechert's London and Washington, DC, offices) whose practice focuses on national security and international trade issues. She advises clients on economic sanctions laws (including programmes administered by the US Office of Foreign Assets Control), provisions of the US Foreign Corrupt Practices Act and the UK Bribery Act, export controls (the Export Administration Regulations and the International Traffic in Arms Regulations), and trade compliance with respect to international agreements and World Trade Organization provisions. Ms Moonga has experience interacting with US government agencies and developing anti-bribery, sanctions and export controls compliance programmes.

Ms Moonga also has litigation experience, having advised domestic companies and foreign entities on trade remedies proceedings before the US Department of Commerce and International Trade Commission, as well as appeals before the US Court of International Trade and Court of Appeals, Federal Circuit.

David Mortlock

Willkie Farr & Gallagher LLP

David Mortlock is a partner and chair of the global trade and investment group at Willkie Farr & Gallagher LLP in Washington, DC. David provides clients with guidance on compliance and enforcement on national security-related issues, including sanctions and export controls, anti-money laundering and reviews by the Committee on Foreign Investment in the United States. He helps clients to build and implement compliance programmes, conducts internal investigations and responds to government inquiries and enforcement actions. From October 2013 to November 2015, David was director for international economic affairs at the White House National Security Council, where he was responsible for coordinating inter-agency work on sanctions, anti-corruption and other illicit finance issues.

From August 2009 to October 2013, he held a number of roles at the Department of State, including attorney-adviser for sanctions and terror finance and deputy coordinator for sanctions policy. David was centrally involved in developing or easing the sanctions programmes for Russia, Iran, Cuba, Myanmar and Venezuela, among others.

Britt Mosman

Willkie Farr & Gallagher LLP

Britt Mosman is a partner and vice chair of the global trade and investment group at Willkie Farr & Gallagher LLP in Washington, DC. Britt has advised global financial institutions and leading multinational companies on complex, international compliance and enforcement matters, particularly economic sanctions, anti-money laundering and anti-corruption laws, as well as transaction reviews by the Committee on Foreign Investment in the United States. Britt has deep experience with economic sanctions laws and regulations, having served as an attorney-adviser in the Office of the Chief Counsel (Foreign Assets Control) advising the Treasury Department's Office of Foreign Assets Control, prior to joining Willkie. In this capacity, she focused on economic sanctions and national security issues, including as a lead attorney on the Iran, Ukraine/Russia, Cuba, Syria, election interference and cyber-related sanctions programmes.

Juliette Musso

Navacelle

Juliette Musso assists clients on complex white-collar and commercial litigation in relation to disputes on unfair competition, banking law and international sanctions. She also represents companies and other entities in the implementation of anti-corruption and money laundering compliance programmes.

After gaining extensive experience with various international law firms in Paris, including one year with an international arbitrator, Juliette has also been involved in commercial, construction and investment arbitration cases conducted under various arbitration rules.

Weng Yee Ng

Forensic Risk Alliance

Weng Yee Ng is a partner at FRA. She holds almost 20 years of experience in external and internal audit and forensic accounting. She specialises in investigations from their initiation to settlement, evaluating and building compliance programmes, risk assessments and litigation support (both civil and criminal).

Weng Yee has conducted work globally – including more than six years working in Malaysia – leveraging her language skills, industry knowledge and cultural understanding to achieve success for her international clients. Over her extensive track record of complex global matters, she has built particular expertise in US Foreign Corrupt Practices Act monitorships, disgorgement and penalty calculations, procurement fraud matters, third-party due diligence, and pre- and post-acquisition transaction, anti-bribery and corruption reviews.

Recognised as a 'Global Leader' in *Who's Who Legal: Investigations*, Weng Yee is described as 'a fantastic forensic investigator', as well as 'very personable and able to build meaningful relationships with stakeholders at all levels of the company'.

Timothy O'Toole

Miller & Chevalier Chartered

Timothy O'Toole is the leader of Miller & Chevalier's economic sanctions and export controls practice group. Mr O'Toole focuses his practice on defending enforcement actions and conducting investigations involving the economic sanctions, export controls and anti-money laundering laws. Recognised as one of the leading international trade lawyers in the US by *Chambers USA*, *The Legal 500*, *Who's Who Legal* and Global Investigations Review, Mr O'Toole provides companies and individuals with advice on compliance with the US economic sanctions, export controls and anti-money laundering laws, and interacts regularly with the US Department of Justice, the Treasury Department's Office of Foreign Assets Control, the State Department's Directorate of Defense Trade Controls and the Commerce Department's Bureau of Industry and Security in that capacity.

Mr O'Toole frequently writes and speaks about white-collar defence and international trade issues at global venues and media outlets. He is a past co-chair of the National Association of Criminal Defense Lawyers (NACDL) West Coast White Collar Crime Conference in Santa Monica and a past co-chair of the NACDL's White Collar Crime Committee. Mr O'Toole also hosts the firm's economic sanctions and export controls podcast, 'EMBARGOED!'.

Ryan Pereira

Steptoe & Johnson LLP

Ryan Pereira is an associate in Steptoe's international trade and regulatory compliance practice group. He counsels clients on compliance with US export controls and economic sanctions laws in addition to handling reviews and investigations by the Committee on Foreign Investment in the United States.

His experience includes representing clients in industries such as aerospace and defence, automotive, financial services, cryptocurrency, insurance, oil and gas, and metals and mining. He has focused on issues concerning Russia, Ukraine, China, Iran, North Korea, Syria, Myanmar, Afghanistan, Venezuela and Cuba.

Ciju Puthuppally

Three Raymond Buildings

Ciju Puthuppally has a broad practice in financial crime, public law and regulatory matters. He is frequently instructed on complex sanctions cases for high net worth individuals and companies. He also acts regularly in asset forfeiture proceedings on behalf of both public authorities and the defence.

Meredith Rathbone

Steptoe & Johnson LLP

Meredith Rathbone chairs Steptoe's international trade and regulatory compliance practice group. She counsels clients on compliance with US export controls and economic sanctions laws and United Nations sanctions and arms embargoes, as well as defence before relevant US government authorities and United Nations sanctions panels.

Her experience includes assisting clients in resolving politically sensitive matters under the joint administration of various government agencies, including navigating the requirements of the Export Administration Regulations, the International Traffic in Arms Regulations and US sanctions laws and regulations administered by the US departments of Commerce, State and the Treasury.

Meredith is experienced in supporting clients with internal investigations, voluntary disclosures and subpoena responses, and export and technology transfer authorisations, undertaking product classification and jurisdiction assessments, and establishing compliance programmes. Meredith regularly advises companies on export controls and sanctions considerations in the context of mergers and acquisitions. She has represented individuals and companies facing civil and criminal investigations in this area, as well as clients seeking to be removed from the United States Department of the Treasury's Office of Foreign Assets Control SDN List through the delisting process.

Meredith currently serves on the US Department of State's Advisory Committee on International Economic Policy, Sanctions Subcommittee.

FeiFei Ren
Miller & Chevalier Chartered

FeiFei (Andrea) Ren is counsel in Miller & Chevalier's international department. Ms Ren focuses her practice on government enforcement actions, internal investigations, international corporate compliance, economic sanctions and export controls and white-collar defence for a wide range of domestic and international clients. She regularly conducts anti-corruption and anti-money laundering investigations, risk assessments and due diligence in countries throughout Asia-Pacific, Europe, Africa and the Middle East for multinational clients across different industries, including oil and gas, pharmaceutical, telecommunications, technology, industrial engineering and equipment, and financial services. Ms Ren's compliance practice also includes helping clients design, implement and improve their corporate compliance programmes.

As a Mandarin speaker, Ms Ren regularly advises on legal matters in both English and Chinese.

Qing Ren
Global Law Office

Qing Ren is a partner at Global Law Office, Beijing. As a leading international trade lawyer recommended by *Chambers and Partners* and *The Legal 500*, Mr Ren has extensive experience in export control and economic sanctions. He has advised, represented or defended many renowned Chinese and foreign companies across various sectors, such as machinery, telecommunications, aerospace, military, semiconductor, AI, internet, automotive, engineering, energy, chemicals, pharmaceuticals, banking, insurance, investment banking, finance leasing and shipping. He also advises government authorities on free trade agreement negotiations and once represented the China Chamber of International Commerce in response to the United States Trade Representative's 301 investigation against China. He was consulted by legislative and administrative authorities during the legislative process of the Export Control Law and related regulations. Being proficient in World Trade Organization (WTO) law, Mr Ren has been elected as an executive director of the WTO Law Research Society of China Law Society.

Mr Ren is on arbitrator panels of the main arbitral institutions in China, including the China International Economic and Trade Arbitration Commission, the China Maritime Arbitration Commission, the Beijing Arbitration Commission, the Shanghai International Arbitration Centre and the Shenzhen Court of International Arbitration.

Prior to practising as a private lawyer, Mr Ren worked at the Department of Treaty and Law in the Ministry of Commerce of China, as deputy director.

Michelle Rosario
Barnes & Thornburg LLP

Michelle Rosario is a law clerk in the international trade practice at Barnes & Thornburg LLP. She will be joining the firm as a full-time associate in autumn 2023 following her graduation from Georgetown University Law Center in May. Prior to joining Barnes & Thornburg, Michelle worked as an intern for the International Trade Administration branch of the US Department of Commerce. She has also served as a judicial for Judge Rudolph Contreras in the District Court for the District of Columbia. When she is not working on trade matters with Barnes & Thornburg, Michelle is a Moot Court competitor and journal editor for the *Georgetown Law Journal for Law and Public Policy*.

J Patrick Rowan
McGuireWoods LLP

Patrick Rowan's practice focuses on criminal and civil enforcement proceedings and internal investigations. He has substantial experience in federal law enforcement, as well as international and national security matters. He also advises corporate clients on compliance with the Foreign Corrupt Practices Act, the International Traffic in Arms Regulations, the Export Administration Regulations and Office of Foreign Assets Control regulations.

Pat spent 18 years in the US Department of Justice (DOJ), where he oversaw the DOJ's review of foreign acquisitions of US companies through the inter-agency Committee on Foreign Investment in the United States. He previously served as the Principal Deputy Assistant Attorney General for the National Security Division, where he managed the DOJ's national security investigations and prosecutions. In both positions, Pat was responsible for supervising all of the DOJ's prosecutions of export violations. As a result, he has particular experience in the application of the material support statutes, the Arms Export Control Act, the International Emergency Economic Powers Act and statutes relating to economic espionage or disclosure of classified information. As the Principal Deputy, he directed the launch and implementation of a nationwide export enforcement initiative, an inter-agency effort to target the illegal export of sensitive technology and weapons components. Pat continued to lead this initiative as Assistant Attorney General.

Gerben Schreurs
Forensic Risk Alliance

Gerben Schreurs is a partner in FRA's Zurich office and has over 25 years of experience solving technical challenges on complex problems requiring insight into large structured and unstructured data sets, including matters relating to investigations, risk management and compliance. He leads high-profile and confidential cases in the areas of money laundering, disputes, fraud, information leakage and regulatory breaches.

Prior to joining FRA, Gerben served as the global head of systems and controls for financial crime compliance at a major Swiss bank. Gerben managed a team of over 50 people internationally and was responsible for the operations and uplifts to compliance systems (transaction surveillance, name screening, sanctions and know-your-customer) with the aim of making processes more efficient and reducing regulatory risks by applying a consistent approach globally. Gerben qualified as a Certified IT Auditor in the Netherlands in 2011.

Emerson Siegle
Ropes & Gray LLP

Emerson Siegle focuses his practice on US regulations governing trade and foreign investment. He routinely counsels clients on the Committee on Foreign Investment in the United States (CFIUS), including by helping clients to navigate the CFIUS review process, assess CFIUS risk in connection with particular investments and assess the CFIUS impact of various transactional and fund structures. Emerson also regularly advises clients on the full scope of US trade laws, including economic sanctions regulations, export controls, import laws and anti-boycott laws. As a trade lawyer, Emerson both advises on regulatory compliance matters and assists with internal and government investigations related to these laws and regulations. Emerson writes frequently about CFIUS, economic sanctions and other international risk topics.

Ben Smith
Baker McKenzie

Ben Smith joined Baker McKenzie in London in 2007 and is a partner in the international trade team. He has worked in the Baker McKenzie San Francisco, Palo Alto and Brussels offices, and on secondment for three FTSE 100 UK plcs. Ben's work focuses on EU and UK export control and sanctions law, as well as anti-bribery and corruption, and antitrust.

Ben advises clients in a number of sectors, with particular focus on technology, energy and energy services, financial services, defence, transport and consumer goods. Ben has significant experience in advising and assisting with risk assessments, compliance programmes, investigations, licence applications, export control classification and voluntary disclosures.

Christopher Stagg

Miller & Chevalier Chartered

Christopher Stagg is a counsel at Miller & Chevalier. He was heavily involved in writing US export control laws, and now companies turn to him to provide practical and strategic counsel to resolve complex export control issues.

Mr Stagg brings special insight into export controls and national security issues by drawing on his substantial experience within government at the State Department's Directorate of Defense Trade Controls (DDTC). He was deeply involved as DDTC's deputy lead in rewriting the International Traffic in Arms Regulations and the Export Administration Regulations, including the revisions to the US Munitions List and Commerce Control List. He was an active participant in related inter-agency policy subcommittees chaired by the National Security Council.

Mr Stagg helps clients navigate export controls by providing regulatory interpretations and clear guidance, rendering jurisdiction and classification determinations, seeking the reversal of unfavourable agency actions through reconsiderations and appeals, advocating before the government for regulatory revisions to advance client interests, developing effective policies and procedures, conducting internal investigations and risk assessments, and advising on consent agreements and enforcement actions. He also advises companies on issues involving economic sanctions and the Committee on Foreign Investment in the United States.

Charlie Steele

Forensic Risk Alliance

Charlie Steele is a partner in FRA's Washington, DC, office with more than 30 years of government and private-sector experience in civil and criminal compliance, investigations, enforcement and litigation matters, in a variety of industries and sectors. In recent years, he has specialised in economic sanctions and Bank Secrecy Act/anti-money laundering (BSA/AML) matters. He is a former senior US Treasury Department and Department of Justice official, serving most recently as chief counsel for the Office of Foreign Assets Control (OFAC). In that role, he led the team of lawyers providing legal advice and support to OFAC

and other Treasury Department personnel in the formulation, implementation and enforcement of economic sanctions. Charlie has also served in a number of other senior positions in the Treasury Department: associate director for enforcement in OFAC, deputy director of the Financial Crimes Enforcement Network (FinCEN, the US government's principal BSA/AML agency and the US Financial Intelligence Unit) and deputy chief counsel in the Office of the Comptroller of the Currency (the US supervisor and regulator of national banks). Charlie earned his JD from the Georgetown University Law Center and a BA in economics from the University of Virginia.

Ben Summers

Three Raymond Buildings

Ben Summers provides advice and representation in a wide range of business settings, including sanctions, fraud, anti-bribery and corruption, and antitrust/cartel investigations and prosecutions brought by bodies including the UK's Serious Fraud Office, Competition and Markets Authority, Office of Financial Sanctions Implementation, National Crime Agency, Department for Business and Trade, Crown Prosecution Service and His Majesty's Revenue and Customs, the US Department of Justice and Securities and Exchange Commission, and the European Union. He is experienced in cross-jurisdictional investigations and mutual assistance requests made by, and of, the United Kingdom. He advises corporate and individual clients subject to Financial Conduct Authority enforcement activity and in relation to non-contentious Financial Services and Markets Act issues, including advice on decisions by the Regulatory Transactions Committee and the Regulatory Decisions Committee. Ben also has a specialist practice in data protection matters.

Ben has worked as a barrister for over 25 years, and as a solicitor at Peters & Peters and, more recently, at Hogan Lovells. In 2019, Ben was named by *The Legal 500* as the 'Crime Junior of the Year'. In *The Legal 500* (2022), his clients describe him as 'an experienced and calm advocate and a fantastic negotiator'; 'he is very client focused and gives a lot of thought to strategy' and he 'combin[es] practicality with deep insight, making him a natural choice for difficult cases'. In *Chambers UK* 2022, his clients say, 'he has brilliant judgement'.

Anahita Thoms

Baker McKenzie

Anahita Thoms heads Baker McKenzie's international trade practice in Germany and is a member of the firm's EMEA steering committee for compliance and investigations. Anahita is global lead sustainability partner of Baker McKenzie's industrials, manufacturing and transportation industry group and a member of the American Bar Association (ABA) International Human Rights Committee. She also served for three consecutive terms as co-chair of the Export Controls and Economic Sanctions Committee of the ABA.

Anahita has won various accolades for her work, including being named 'International Trade Lawyer of the Year (Germany)' at the 2020 ILO Client Choice Awards and 'International Trade Lawyer (New York)' at the 2016 ILO Client Choice Awards, being listed in the '100 Most Influential Women in German Business' by *Manager Magazin* and in *Capital's* 40 under 40, and being a Young Global Leader of the World Economic Forum. She is regularly interviewed as an expert on trade and business and human rights issues, such as by the BBC, the *New York Times*, *Handelsblatt* and *Börsen-Zeitung*.

Anahita focuses her practice on global investigations, particularly in the fields of international trade law, business and human rights, and data protection. She has significant experience in advising on internal compliance programmes, accompanying internal and external investigations and self-disclosures in cases of breaches of sanctions, export control and foreign investment review, closely collaborating with the competent authorities.

Sam Amir Toossi

Akrivis Law Group, PLLC

Sam Amir Toossi is a partner in Akrivis Law Group's New York office and heads the firm's white-collar defence and commercial litigation practice. He has nearly 20 years of litigation experience as a commercial litigator, a state and federal prosecutor and an in-house attorney at a major company. Mr Toossi represents individual and corporate clients in internal and government investigations and white-collar criminal defence, with a particular focus advising on sanctions and export control matters, anti-money laundering, bribery and corruption matters.

For seven years, Mr Toossi was an Assistant United States Attorney in the United States Attorney's Office for the Eastern District of New York, where he served as deputy chief of the office's International Narcotics and Money Laundering Section. In 2015, he received the Attorney General's Award for Exceptional Service, which is the Department of Justice's highest award for

employee performance. In 2014, he received the Federal Law Enforcement Foundation Federal Prosecutor Award, which is among the most prestigious law enforcement awards in the New York region.

Victoria Turner

Eversheds Sutherland

Victoria Turner is a principal associate in the corporate crime and investigations team at Eversheds Sutherland. She has more than 10 years' experience in financial crime, with a specific focus on financial sanctions. She primarily advises a range of global top-tier financial institutions and regulated and unregulated corporate entities in relation to sanctions compliance and is the lead lawyer on a number of large-scale global sanctions investigations into historic EU, UK and US sanctions breaches.

Victoria advises UK-based clients in relation to Office of Foreign Assets Control enforcement cases and settlements. She also advises regulated institutions in connection with establishing and maintaining effective sanctions compliance programmes.

Victoria is a member of the UK Finance Associate Members Sanctions Panel and the deputy chair of the Women in Sanctions Forum. She regularly provides training in respect of sanctions and speaks at a number of industry events.

Zia Ullah

Eversheds Sutherland

Zia Ullah is a partner and co-global head of corporate crime and investigations at Eversheds Sutherland. With more than 20 years' experience as a criminal lawyer, Zia has acted in prosecutions brought by a number of leading enforcement agencies, in addition to being lead lawyer on a number of internationally led investigations, including those involving US regulators such as the US Treasury's Office of Foreign Assets Control (OFAC). He is a globally recognised specialist in international sanctions and anti-money laundering. Zia is a Financial Conduct Authority Skilled Person for Financial Crime and advises on all aspects of corporate and financial crime. He was previously the global head of sanctions at Barclays.

Zia advises global top-tier financial institutions and other regulated entities in connection with sanctions compliance and has led a number of large-scale investigations into historic breaches in relation to sanctions imposed by the European Union, the United Kingdom and the United States. He advises UK-based clients in relation to OFAC enforcement cases and settlements. Zia regularly provides training in respect of sanctions and regularly presents to a number of financial

services industry bodies, including the UK Association of Foreign Banks and the Anti-Money Laundering Professionals Forum, and is co-chair of the Associate Members Sanctions Panel at UK Finance.

Caroline Watson
Miller & Chevalier Chartered

Caroline Watson is a senior associate in Miller & Chevalier's international department. She focuses her practice on international trade, with emphasis on export and import controls, economic sanctions and customs.

Growing up in the Middle and Far East and travelling extensively around the world, Ms Watson brings a keen understanding of international issues and cross-cultural communication to serve clients in international trade-related matters. She counsels clients on issues concerning imports and exports (including in relation to the International Traffic in Arms Regulations and the Export Administration Regulations), the Foreign Corrupt Practices Act, customs, free-trade zones, economic sanctions and defence article operations. Ms Watson has experience in developing compliance programmes, conducting internal investigations and regulatory compliance audits and representing clients in government inspections and investigations. She also advocates clients' interests regarding compliance issues in submissions to and conferences with various government agencies, including the Directorate of Defense Trade Controls, the Office of Foreign Assets Control, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, the Alcohol and Tobacco Tax and Trade Bureau, the Bureau of Industry and Security, US Customs and Border Protection and the US Department of Justice.

Kerstin Wilhelm
Linklaters LLP

Kerstin Wilhelm is a highly accomplished litigation and investigations practitioner and co-head of the German crisis management and compliance group. She focuses her practice on internal and government investigations, both domestic and cross-border, with extensive experience in dawn raids. During a secondment to the investigations in-house team of a large US-based international technology company, she gained additional experience in conducting internal investigations into sensitive matters in several jurisdictions. Kerstin has in-depth experience advising clients on white-collar crime, as well as in compliance matters, including advice on corporate criminal liability and public procurement law implications. She has advised a wide range of financial and corporate clients on EU sanctions risks focusing on, inter alia, Russia-related sanctions. Her advice also extends

to the EU Blocking Regulation and sanctions screening processes. In addition, Kerstin has many years of experience in complex civil litigation proceedings with a focus on banking and capital markets litigation, in particular mass litigation.

Leilei Wu

BDO USA, PA

Leilei Wu is a senior manager in the legal, monitorships and investigations practice at BDO USA, PA, with over 15 years of experience in forensic accounting, auditing and consulting. She is a member of BDO's Asia Forensic Desk, where she works with law firms and companies on international forensic investigations, including financial statement fraud, employee misconduct, corruption and other global white-collar matters.

Leilei has extensive knowledge and experience in advising clients in the prevention and detection of violations of the Foreign Corrupt Practices Act. She conducts internal investigations, evaluates compliance risks and helps clients design and implement compliance programmes that are customised according to their specific risks. Her experience also includes providing monitoring services for companies to comply with consent orders and settlement terms. She has assisted multinational companies within various industries, including manufacturing, healthcare, telecommunications, automotive, banking, technology, pharmaceuticals, real estate and hospitality.

Wendy Wysong

Steptoe & Johnson HK LLP

Wendy Wysong is the managing partner of Steptoe & Johnson's Hong Kong office and co-chair of the firm's investigations and white-collar defence group. She focuses her practice on regulatory compliance and white-collar defence of international laws, including the Export Administration Regulations, US sanctions laws and regulations administered by the Office of Foreign Assets Control, the International Traffic in Arms Regulations and US anti-boycott laws, as well as the US Foreign Corrupt Practices Act.

As a former Assistant US Attorney in Washington and Deputy Assistant Secretary for Export Enforcement in the Department of Commerce's Bureau of Industry and Security, Wendy offers clients a unique combination of experience and insight as both a prosecutor and regulator before courts and agencies.

Ranked as a Band 1 practitioner by *Chambers Asia-Pacific* and *Chambers Global*, Wendy is described by clients as having 'unrivalled expertise in the investigations and regulatory space. Her experience in the US government and clout in the industry has been extremely valuable in helping us navigate the ever-changing

regulatory landscape. She provides invaluable insights into the mindsets and policy directions of regulators, prosecutors and other investigative bodies, and is able to advise us based on the breadth of knowledge and experience over decades of her career.'

Elli Zachari

Steptoe & Johnson LLP

Elli Zachari is a legal consultant at Steptoe & Johnson. She advises multinational companies, financial institutions and governmental bodies on EU trade remedies matters, including World Trade Organization (WTO) dispute settlements, EU trade negotiations, and export controls and sanctions.

Before joining Steptoe, Elli interned at the WTO Legal Affairs division. She has also worked at the European Union Intellectual Property Office as a trainee in its operations department.

Deming Zhao

Global Law Office

Dr Deming Zhao is a partner at Global Law Office, Shanghai. His practice covers corporate and regulatory compliance, dawn raid defence, customs and trade compliance, export control and shipping litigation. He is one of the pioneers who has developed the legal practice of customs and trade compliance in China, which has won wide recognition among multinational clients. Dr Zhao was named in 'Client Choice – Top 20 Lawyers in China', the first survey of its kind by *ALB* in 2012, and was ranked as a highly recommended lawyer (Band One) for customs, export control and economic sanctions (PRC firms) by *Chambers Global* 2021, 2022 and 2023.

As a leading lawyer in customs and trade compliance practice, Dr Zhao has advised, represented or defended many renowned multinational companies in administrative and criminal customs audit and investigation cases, and has led many projects in respect of trade compliance internal control systems, health checks and training for multinational clients in China.

Dr Zhao advises and trains many clients on export control or economic sanctions, and frequently gives talks on China export control and customs supervision practice at symposiums or seminars in Europe. In 2019, he was invited by the International Anti-Corruption Academy to lecture on China and US export control practices in Seoul to professional audiences from Asia.

In an administrative review case, Dr Zhao successfully defended a multinational client against the export licensing requirement for a given chemical product. From 2020 to 2021, he was the leading lawyer supervising a global export control

compliance programme for a leading Chinese company. In 2022, Dr Zhao also advised clients on issues concerning sanctions and export controls against Russia and Belarus.

Julie Zorrilla

Navacelle

Julie Zorrilla is a partner at Navacelle with over 10 years' experience assisting clients in complex cross-border financial and criminal matters, including embargoes, index manipulation (LIBOR and SSA), asset recovery and large-scale corruption cases involving senior executives and major French and foreign financial institutions.

She handles large-scale corruption and compliance matters, advising on both legal and crisis management for corporations with global operations. She is involved in assisting Stéphane de Navacelle in connection with his appointment as expert pursuant to a World Bank negotiated resolution agreement. Julie participates in determining the strategy for and the implementation of internal investigations, and she assists companies with activities on a global scale at all procedure stages, by advising on both legal and communication strategy. She also has expertise in compliance.

Julie leads the firm's extradition and Interpol practices, advising both individuals and states in connection with European arrest warrants, international arrest warrants and red notices.

She previously worked at the Legal Affairs Department of the Ministry of Economy and Finance in 2012, and as an intern auditor at the Paris Court of Appeal in 2011. Julie has been distinguished in *The Legal 500: EMEA*, *Who's Who Legal*, *Best Lawyers* and Global Investigations Review ('Top 100 Women in investigations') in the areas of criminal law, litigation, compliance and investigations.

APPENDIX 3

Contributors' Contact Details

Akrivis Law Group, PLLC

747 Third Avenue
32nd Floor
New York, NY 10022
United States
Tel: +1 646 517 0687
atoossi@akrivislaw.com

5335 Wisconsin Avenue, NW
Suite 440
Washington, DC 20015
United States
Tel: +1 202 730 1271
falavi@akrivislaw.com

www.akrivislaw.com

Baker & Hostetler LLP

1050 Connecticut Avenue, NW
Suite 1100
Washington, DC 20036-5318
United States
Tel: +1 202 861 1500
blinney@bakerlaw.com
ocadet@bakerlaw.com
www.bakerlaw.com

Baker McKenzie

Friedrichstraße 88/Unter den Linden
10117 Berlin
Germany
Tel: +49 30 2 20 02 81 0
Fax: +49 30 2 20 02 81 199
anahita.thoms@bakermckenzie.com

100 New Bridge Street
London EC4V 6JA
United Kingdom
Tel: +44 20 7919 1000
tristan.grimmer@bakermckenzie.com
ben.smith@bakermckenzie.com
sophie.armstrong@
bakermckenzie.com

www.bakermckenzie.com

Barnes & Thornburg LLP

555 12th Street, NW
Suite 1200
Washington, DC 20004
United States
Tel: +1 202 289 1313
christine.sohar-henter@btlaw.com
www.btlaw.com

BDO USA, PA

100 Park Avenue
New York, NY 10017
United States
Tel: +1 212 885 8000
lwu@bdo.com

799 9th Street, NW
Suite 710
Washington, DC 20001
United States
Tel: +1 202 644 5400
bejohnson@bdo.com

www.bdo.com

Bonifassi Avocats

34 boulevard Haussmann
75009 Paris
France
Tel: +33 1 82 28 10 80
s.bonifassi@bonifassi-avocats.com
j.bastien@bonifassi-avocats.com
www.bonifassi-avocats.com

Cravath, Swaine & Moore LLP

Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
United States
Tel: +1 212 474 1000
jburetta@cravath.com
mlew@cravath.com
www.cravath.com

Dechert LLP

160 Queen Victoria Street
London EC4V 4QQ
United Kingdom
Tel: +44 20 7184 7000
john.bedford@dechert.com
andris.ivanovs@dechert.com
navpreet.moonga@dechert.com
www.dechert.com

Eversheds Sutherland

1 Wood Street
London EC2V 7WS
United Kingdom
Tel: +44 20 7919 4500
ziaullah@eversheds-sutherland.com
victoriaturner@eversheds-sutherland.com
www.eversheds-sutherland.com

Forensic Risk Alliance

Löwenstrasse 53
Zurich 8001
Switzerland
Tel: +41 795 002 991
gschreurs@forensicrisk.com

Audrey House
16–20 Ely Place
London EC1N 6SN
United Kingdom
Tel: +44 20 7831 9110
wng@forensicrisk.com
jcappon@forensicrisk.com

2550 M Street, NW
Washington, DC 20037
United States
Tel: +1 202 235 5770
csteele@forensicrisk.com

www.forensicrisk.com

Global Law Office

15th and 20th Floors, Tower 1
China Central Place
No. 81 Jianguo Road
Chaoyang District
Beijing 100025
China
Tel: +86 10 6584 6688
renqing@glo.com.cn
huoningxin@glo.com.cn

35th and 36th Floors,
Shanghai One ICC
No. 999 Middle Huai Hai Road
Xuhui District
Shanghai 200031
China
Tel: +86 21 2310 8288
zhaodeming@glo.com.cn

www.glo.com.cn

Jenner & Block LLP

Jenner & Block London LLP
Level 10, 10 Exchange Square
London EC2A 2BR
United Kingdom
Tel: +44 330 060 5400
pfeldberg@jenner.com
rdalling@jenner.com
kjardaneh@jenner.com
agaudoin@jenner.com
www.jenner.com

Linklaters LLP

Prinzregentenplatz 10
81675 Munich
Germany
Tel: +49 89 41808 0
kerstin.wilhelm@linklaters.com

One Silk Street
London EC2Y 8HQ
United Kingdom
Tel: +44 20 7456 2000
satindar.dogra@linklaters.com
james.bowen@linklaters.com

601 Thirteenth Street, NW
Suite 400 South
Washington, DC 20005
United States
Tel: +1 202 654 9200
sterling.darling@linklaters.com

www.linklaters.com

McGuireWoods LLP

Gateway Plaza
800 East Canal Street
Richmond, VA 23219-3916
United States
Tel: +1 804 775 1000
abrackett@mcguirewoods.com
prowan@mcguirewoods.com
jcowley@mcguirewoods.com
lmarshall@mcguirewoods.com
echilds@mcguirewoods.com
ebaur@mcguirewoods.com
www.mcguirewoods.com

Miller & Chevalier Chartered

900 16th Street, NW
Black Lives Matter Plaza
Washington, DC 20006
United States
Tel: +1 202 626 5800
totoole@milchev.com
cstagg@milchev.com
fren@milchev.com
cwatson@milchev.com
mlevitt@milchev.com
scutler@milchev.com
www.millerchevalier.com

Navacelle

60 rue Saint-Lazare
75009 Paris
France
Tel: +33 1 48 78 76 78
sdenavacelle@navacelle.law
jzorrilla@navacelle.law
jmusso@navacelle.law
www.navacelle.law

Peters & Peters Solicitors LLP

15 Fetter Lane
London EC4A 1BW
United Kingdom
Tel: +44 20 7822 7777
abradshaw@petersandpeters.com
ajones@petersandpeters.com
www.petersandpeters.com

Ropes & Gray LLP

32nd Floor, 191 North Wacker Drive
Chicago, IL 60606
United States
Tel: +1 312 845 1200
brendan.hanifin@ropesgray.com

2099 Pennsylvania Avenue, NW
Washington, DC 20006
United States
Tel: +1 202 508 4600
ama.adams@ropesgray.com
emerson.siegle@ropesgray.com
junsuk.lee@ropesgray.com

www.ropesgray.com

Steptoe & Johnson

Steptoe & Johnson LLP
Avenue Louise 489
1050 Brussels
Belgium
Tel: +32 2 626 0500
rantonini@steptoe.com
emonard@steptoe.com
bmaniatis@steptoe.com
ezachari@steptoe.com

Steptoe & Johnson HK LLP
Unit 8, 31/F Alexandra House
18 Chater Road
Central
Hong Kong
Tel: +852 3729 1800
wwysong@steptoe.com
aburney@steptoe.com

Steptoe & Johnson LLP
1330 Connecticut Avenue, NW
Washington, DC 20036
United States
Tel: +1 202 429 3000
mrathbone@steptoe.com
rpereira@steptoe.com

www.steptoe.com

Sullivan & Cromwell LLP

1700 New York Avenue, NW
Suite 700
Washington, DC 20006-5215
United States
Tel: +1 202 956 7500
kadelej@sullcrom.com
marcoj@sullcrom.com
www.sullcrom.com

Three Raymond Buildings

3 Raymond Buildings
Gray's Inn
London WC1R 5BH
United Kingdom
Tel: +44 20 7400 6400
rachel.barnes@3rblaw.com
ben.summers@3rblaw.com
patrick.hill@3rblaw.com
ciju.puthuppally@3rblaw.com
www.3rblaw.com

Willkie Farr & Gallagher LLP

1875 K Street, NW
Washington, DC 20006-1238
United States
Tel: +1 202 303 1000
dmortlock@willkie.com
bmosman@willkie.com
ncronin@willkie.com
ael-gamal@willkie.com
www.willkie.com

We live in a new era for sanctions. More states are using them, in more creative (and often unilateral) ways.

This, alas, creates complication for the rest of us. Hitherto no book has addressed the complexities that businesses and their advisers must address by dint of this proliferation in a structured way. GIR's *The Guide to Sanctions* fills that gap. Written by contributors from the small but expanding field of sanctions enforcement, it dissects the topic in a practical fashion, from every stakeholder's perspective, and is an invaluable resource.

Visit globalinvestigationsreview.com
Follow @GIRalerts on Twitter
Find us on LinkedIn

ISBN 978-1-80449-256-7