Global Investigations Review

The Guide to Sanctions

Editors
Rachel Barnes, Paul Feldberg, Nicholas Turner, Anna Bradshaw, David Mortlock, Anahita Thoms and Rachel Alpert

Second Edition

The Guide to Sanctions

Reproduced with permission from Law Business Research Ltd
This article was first published in July 2021
For further information please contact Natalie.Clarke@lbresearch.com

Editors

Rachel Barnes

Paul Feldberg

Nicholas Turner

Anna Bradshaw

David Mortlock

Anahita Thoms

Rachel Alpert

GIR
Global Investigations Review

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK

www.globalinvestigationsreview.com

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as at June 2021, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to:
natalie.hacker@lbresearch.com.
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-596-2

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

Acknowledgements

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

BAKER & HOSTETLER LLP

BAKER MCKENZIE

BARNES & THORNBURG LLP

BDO USA LLP

CARTER-RUCK SOLICITORS

CRAVATH, SWAINE & MOORE LLP

EVERSHEDS SUTHERLAND

FORENSIC RISK ALLIANCE

GLOBAL LAW OFFICE

JENNER & BLOCK LLP

MCGUIREWOODS LLP

MAYER BROWN

MILLER & CHEVALIER CHARTERED

PETERS & PETERS SOLICITORS LLP

SEWARD & KISSEL

SIMMONS & SIMMONS LLP

STEPTOE & JOHNSON

STEWARTS

THREE RAYMOND BUILDINGS

WHITE & CASE LLP

WILLKIE FARR & GALLAGHER LLP

Publisher's Note

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

We live, it seems, in a new era for sanctions: more and more countries are using them, with greater creativity and (sometimes) selfishness.

And little wonder. They are powerful tools. They reach people who are otherwise beyond our jurisdiction; they can be imposed or changed at a stroke, without legislative scrutiny; and they are cheap! Others do all the heavy lifting once they are in place.

That heavy lifting is where this book comes in. The pullulation of sanctions has resulted in more and more day-to-day issues for business 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 in different spheres of activity.

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 will help them do so better. Whoever you are, we are confident you will learn something new.

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*.

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
June 2021

Contents

Foreword

I am pleased to welcome you to the Global Investigations Review guide to economic sanctions. In the following pages, you will read in detail about sanctions programmes, best practices for sanctions compliance, enforcement cases, and the unique challenges created in corporate transactions and litigation by sanctions laws. This volume will be a helpful and important resource for anyone striving to maintain compliance and understand the consequences of economic sanctions.

The compliance work conducted by the private sector is critically important to stopping the flow of funds to weapons proliferators such as North Korea and Iran, terrorist organisations like ISIS and Hezbollah, countering Russia's continued aggressive behaviour, targeting human rights violators and corrupt actors, and disrupting drug traffickers such as the Sinaloa Cartel. I strongly believe that we are much more effective in protecting our financial system when government works collaboratively with the private sector.

Accordingly, as Under Secretary of the US Department of the Treasury's Office of Terrorism and Financial Intelligence from 2017 to 2019, one of my top priorities was to provide the private sector with the tools and information necessary to maintain compliance with sanctions and AML laws and to play its role in the fight against illicit finance. The Treasury has provided increasingly detailed guidance on compliance in the form of advisories, hundreds of FAQs, press releases announcing actions that detail typologies, and the Office of Foreign Assets Control (OFAC) framework to guide companies on the design of their sanctions compliance programmes. Advisories range from detailed guidance from OFAC and our interagency partners for the maritime, energy and insurance sectors, to sanctions press releases that provide greater detail on the means that illicit actors use to try to exploit the financial system, to Financial Crimes Enforcement Network (FinCEN) advisories providing typologies relating to a wide range of illicit activity.

Whether it was for the Iran, North Korea or Venezuela programmes, or in connection with human rights abuses and corrupt actors around the globe, the US Treasury has been dedicated to educating the private sector so that they in turn can further protect themselves.

The objective is not only to disrupt illicit activity but also to provide greater confidence in the integrity of the financial system, so we can open up new opportunities and access to financial services across the globe. That guidance is particularly important today with the increased use of sanctions and other economic measures across a broader spectrum of jurisdictions and programmes.

As you read this publication, I encourage you to notice the array of guidance, authorities and other materials provided by the US Treasury and other authorities cited and discussed by the authors. This material, provided first-hand from those charged with writing and enforcing sanctions laws, gives us a critical understanding of these laws and how the private sector should respond to them. By understanding and using that guidance, private companies can help to protect US and global financial systems against nefarious actors, as well as avoid unwanted enforcement actions.

Thank you for your interest in these subjects, your dedication to understanding this important area of the law, and your efforts to protect the financial system from abuse.

Sigal Mandelker
Former Under Secretary of the Treasury for Terrorism and Financial Intelligence
June 2021

Part III

Sanctions in Practice

18

Issues Arising for Financial Institutions and Regulated Entities

Jason Hungerford, Ori Lev, Tamer Soliman, James Ford and Timothy C Lee[1]

Introduction

Financial institutions and regulated entities face a range of sector-specific challenges when complying with sanctions arising from robust legal requirements and regulatory expectations. In addition, financial institutions and regulated entities are often engaged in an activity that can implicate multiple – and occasionally conflicting – sanctions regimes. This chapter sets out some key considerations for financial institutions and regulated entities to consider in proactively managing sanctions risks, examines some key challenges emerging in the regulated space, and offers some practical recommendations to support financial institutions and regulated entities in navigating the complexities of sanctions.

Customer risk management

Financial institutions face particular compliance risks as a result of their clients' exposure to sanctions targets. Transactions that on their face do not appear to violate sanctions regulations may in fact involve or be for the benefit of sanctions targets or sanctioned jurisdictions. It is essential, therefore, for financial institutions and regulated entities to identify and manage these risks.

Non-US financial institutions should take particular note of the proliferation of US secondary sanctions provisions that target foreign financial institutions (FFIs). A breach of these provisions could result in an FFI being cut off from US correspondent and payable-through accounts or, in certain cases, designated as a specially designated national (SDN). The US Treasury Department's Office of Foreign Assets Control (OFAC) has the authority to impose these types of measures on FFIs under a number of authorities, including

1 Jason Hungerford, Ori Lev and Tamer Soliman are partners, James Ford is a senior associate and Timothy C Lee is a former associate at Mayer Brown. Timothy C Lee currently serves as in-house sanctions and export control counsel at a global social media and technology company.

the provisions of the Countering Americas Adversaries Through Sanctions Act (CAATSA) targeting Russia, Executive Order 13810 Imposing Additional Sanctions with Respect to North Korea (EO 13810) and the Iranian Financial Sanctions Regulations.[2] Under these authorities, OFAC has the power to impose secondary sanctions measures on FFIs that knowingly facilitate a 'significant transaction' or provide 'significant financial services' to, for or on behalf of a person sanctioned under the relevant sanctions programme. These measures can have significant and long-term effects for FFIs. For example, in July 2012, Bank of Kunlun in China was subject to US correspondent banking restrictions for knowingly facilitating significant transactions and providing significant financial services to designated Iranian banks.[3] These measures have effectively barred Bank of Kunlun from accessing the US financial system for more than eight years and, at the time of writing, remain in place.

OFAC has also used its powers to implement some innovative and aggressive new concepts. For example, Section 3 of EO 13810 authorises OFAC to block funds that 'come within the United States' or 'come within the possession' of a 'US Person'[4] that transit accounts located anywhere in the world that OFAC determines to be owned or controlled by a North Korean person or that have been used to transfer funds in which any North Korean person (other than the account holder) has an interest. OFAC has made clear that it may not publicly identify such accounts but may instead identify them by providing 'notice directly to affected parties'.[5] For FFIs accustomed to screening against OFAC's published list of designated parties, OFAC's use of this new authority to privately designate 'accounts' rather than parties raises new compliance challenges.

The practical implications of these developments is that financial institutions have an increasing number of issues to consider in the context of both know-your-customer (KYC) due diligence and transaction monitoring. The sanctions due diligence that a financial institution or regulated entity conducts at the outset of a client relationship or transaction, and periodically thereafter, is critical to managing sanctions risk. Regulators expect financial institutions to have in place due diligence processes sufficient to identify clients' heightened sanctions risk (e.g., based on a client's geographical location, its ownership, supply chains or its prior sanctions history) and to take appropriate steps to mitigate this risk.

Transaction monitoring typically involves the comparison of transaction-related information with the relevant sanctions lists. This can be a complex exercise for a number of

2 31 CFR Part 561.

3 US Dep't of Treasury, Press Center, 'Treasury Sanctions Kunlun Bank in China and Elaf Bank in Iraq for Business with Designated Iranian Banks' (31 July 2012), at www.treasury.gov/press-center/press-releases/Pages/tg1661.aspx.

4 The US Dep't of Treasury's Office of Foreign Assets Control [OFAC] generally defines the term 'US Person' to mean any (1) United States citizen or permanent resident, (2) entity organised under the laws of the United States or any jurisdiction within the United States (including foreign branches), or (3) person in the United States. In the context of certain sanctions programmes, including the Iran, Cuba and North Korea (but only with respect to US financial institutions) sanctions programmes, the term also includes entities that are owned or controlled by persons described in points (1) to (3), regardless of place of incorporation.

5 31 C.F.R. 510.201(e) (providing that funds subject to blocking may be identified 'via actual or constructive notice from OFAC' and that OFAC's determination that an account satisfies the criteria for designation may or may not be 'publicized'). See also, US Dep't of Treasury, OFAC Frequently Asked Questions [hereinafter OFAC FAQ] at No. 526, at /www.treasury.gov/resource-center/faqs/Sanctions/Documents/faq_all.html.

reasons (e.g., the information technology systems involved, the number of sanctions lists to be screened, and screening of foreign names and transliterations). Many financial institutions use complex automated systems to monitor transactions, sometimes with the support of reputable third parties, to assist in reviewing the most current information. Whether automated or manual, an effective compliance programme's monitoring of transactions through screening will inevitably require some level of human involvement, as a screening match does not necessarily mean that there is a sanctions risk or violation. The 'four eyes principle' – which requires two people to agree that a flagged transaction should be cleared or stopped – is one way to ensure thoroughness and accountability in transaction monitoring.

Beyond standard continued screening and KYC due diligence, transaction monitoring by financial institutions ought to be dynamic enough to respond to the complex and evolving customer risk landscape. For example, financial institutions should carefully monitor payment terms when dealing with transactions that involve the debt of US and EU sectoral sanctions targets, giving due consideration to relevant regulatory guidance.[6] Penalties for breaching these sanctions can be significant.[7], [8]

On 31 March 2020, the United Kingdom's Office of Financial Sanctions Implementation announced a £20.4 million penalty against Standard Chartered Bank for engaging in prohibited dealings in the debt of Denizbank AŞ, a majority-owned subsidiary of Sberbank (listed as an EU sectoral sanctions target in Annex III to Council Regulation (EU) No. 833/2014).

On 25 April 2019, OFAC imposed a US$75,375 penalty against Haverly Systems, Inc for prohibited dealings in new debt of JSC Rosneft (identified by OFAC on the Sectoral Sanctions Identification List as subject to Directive 2 (as amended on 29 September 2017) under Executive Order 13662).

In light of CAATSA, financial institutions should also apply heightened scrutiny if there is a risk of facilitation of 'significant transactions' involving Russian sanctioned parties or when processing transactions in which Russian oligarchs have substantial minority interests.

Financial institutions ought to be mindful of regional risks, such as North Korea's extensive illicit procurement network involving Chinese and South-East Asian companies. For example, financial institutions should interrogate information provided by their clients on a risk assessed basis, particularly where transaction parties are based in higher risk regions. In a recent enforcement action, OFAC's enforcement notice states that details of North Korean

6 See, e.g., European Commission, 'Commission Guidance Note on the Implementation of Certain Provisions of Regulation (EU) No. 833/2014' (25 August 2017), at https://ec.europa.eu/fpi/sites/fpi/files/1_act_part1_v3_en.pdf; OFAC FAQ Nos. 370 to 375, 391 to 396, 404 to 411, 419.

7 HM Treasury, Office of Financial Sanctions Implementation [OFSI], Report of Penalty for Breach of Financial Sanctions Regulations (Section 149(2) PACA 2017 report), 'Imposition of Monetary Penalty – Standard Chartered Bank' (31 March 2020), at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/876971/200331_-_SCB_Penalty_Report.pdf.

8 OFAC, Enforcement Notice, Haverly Systems, Inc. (25 April 2019), at www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190425_haverly.pdf.

entities were replaced by details of intermediaries based in third countries on relevant transaction documents.[9]

> On 14 January 2021, OFAC imposed a US$1,016,000 penalty on PT Bukit Muria Jaya (BMJ), a paper products manufacturer located in Indonesia, in connection with the exportation of cigarette paper to North Korea, including to a blocked North Korean person. OFAC's enforcement notice states that BMJ directed payments for these exports to its US dollar bank account at a non-US bank, causing US banks to clear wire transfers related to the shipments in contravention of US sanctions. OFAC's enforcement notice also states that, at the request of its customers, certain BMJ sales employees replaced the names of North Korean entities with the details of intermediaries in third countries on transaction documents such as invoices, packing lists and bills of lading.

Furthermore, OFAC's new use of unpublished account-based blocking notices for non-SDNs under the North Korea sanctions regime presents unique compliance challenges for financial institutions, including whether they should block a customer's other accounts or altogether terminate the relationship, or add the name of the customer to an internal blacklist to prevent any future transactions with them. Finally, OFAC's focus on industry-specific risks presents yet another compliance burden for financial institutions. For example, OFAC has issued an advisory for the maritime industry and related communities (including financial institutions) providing guidance to address illicit shipping and sanctions evasion practices.[10] Among other measures, OFAC suggests that financial institutions that transact with ship owners, charterers and ship managers monitor transactions on a risk-sensitive basis for signs of disabling or manipulating the automatic identification system on vessels, particularly when vessels are known to operate in areas determined to pose a high risk for sanctions evasion. To manage such risks and facilitate sanctions compliance, financial institutions may choose to engage in de-risking, a practice whereby a financial institution terminates or restricts business with companies in certain parts of the world or certain sectors, often because of wider financial crime concerns.

Reporting obligations

As a general rule, financial institutions and regulated entities have an obligation to report to the relevant sanctions authorities if they hold or control blocked funds or assets in which a designated person has an interest. These reporting obligations are common in US, EU and UK sanctions regimes, although the timing and information requirements for reports may vary depending on the regime.

US sanctions laws have long required US financial institutions (and in some cases their non-US subsidiaries) to report all blocked property or rejected funds transfers to OFAC within 10 business days of the property being blocked or the transfer being rejected, and

9 OFAC, Enforcement Notice, PT Bukit Muria Jaya (14 January 2021), at https://home.treasury.gov/system/files/126/20210114_BMJ.pdf.

10 See US Dep't of Treasury, US Dep't of State and US Coast Guard, Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities (14 May 2020), at www.treasury.gov/resource-center/sanctions/Programs/Documents/05142020_global_advisory_v1.pdf.

additionally report on blocked property annually by 30 September for assets blocked as of 30 June.[11]

From 21 June 2019, OFAC expanded these obligations in several ways.[12] First, the obligation to report rejected (i.e., returned to sender) transactions was expanded to apply to all US Persons or persons subject to US jurisdiction, and not just to financial institutions. Other regulated (and non-regulated) entities are now obliged to report rejected transactions. Second, the nature of the information to be reported, especially with respect to rejected transactions, was expanded. These reports must include, *inter alia*, a description of the transaction, the names of intermediary, correspondent, issuing, and advising or confirming banks, and the identities of the associated sanctions targets. Financial institutions must retain reports on rejected transactions for at least five years after the rejection. In the case of blocked property, reports must be retained for the period for which the property is blocked and for five years after the date the property is unblocked.

Under UK sanctions regulations, there are specific reporting requirements for financial institutions and regulated entities.[13] For example, UK sanctions regulations require financial institutions and certain other regulated businesses and professions to report to the United Kingdom's Office of Financial Sanctions Implementation OFSI as soon as practicable if they have reasonable cause to suspect that they have come into contact with a designated person or have dealt in frozen assets in the course of carrying out their business.[14] Such a report must include key information around the relevant dealings, including the information on which the knowledge or suspicion is based and any information about the designated person by which they can be identified.[15]

In the United Kingdom, there is also an obligation for all persons that hold or control funds or economic resources belonging to a designated person to submit a frozen assets report to OFSI annually.[16] There is also a duty to submit a nil return if a report was submitted for the previous year if that report was not itself a nil return. This annual reporting requirement is of particular relevance for financial institutions, which may hold funds or economic resources for, or on behalf of, designated persons.

The practical takeaway for financial institutions and regulated entities is that there are any number of different reporting obligations that may be relevant to the institution, and a sanctions compliance programme ought to ensure compliance with these different obligations.

11 31 CFR §§ 501.603 (blocked property reports), 501.604 (rejected transaction reports).

12 US Dep't of the Treasury, Reporting, Procedures and Penalties Regulations, 84 Fed. Reg. 29055 (21 June 2019).

13 These are described as a 'relevant institution' under The European Union Financial Sanctions (Amendment of Information Provisions) Regulations 2017. These reporting obligations also extend to a 'relevant business or profession', which includes professionals such as auditors, accountants and lawyers. See OFSI, Financial Sanctions Guidance (December 2020) [OFSI Guidance] at Chapter 5.1.2, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/961516/General_Guidance_-_UK_Financial_Sanctions.pdf.

14 OFSI Guidance at Chapter 5.1.1.

15 id.

16 OFSI, Financial Sanctions Notice (3 September 2020), 'Frozen Assets Reporting (2020)', at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/914470/Financial_Sanctions_Notice__2020_.pdf.

Financial institutions and other regulated entities would be well advised to seek local expertise to navigate any applicable reporting regimes.

Correspondent banking

Correspondent banking raises several noteworthy sanctions issues for US and non-US financial institutions alike. US regulators expect US financial institutions that maintain correspondent accounts for FFIs to implement risk-based due diligence procedures that are reasonably designed to manage the risks inherent in cross-border movement of funds. In particular, OFAC expects US financial institutions to conduct sufficient risk-based due diligence on their FFI relationships, including on an FFI's customers.[17]

Non-US financial institutions also need to consider the implications of US sanctions requirements and their jurisdictional reach. As noted above, recently implemented reporting requirements on rejected transactions expressly require financial institutions to report the identities of the correspondent banks involved in the rejected transactions. This requirement will therefore result in the identities of non-US institutions that appear in rejected transactions being made more readily available to OFAC and potentially other US authorities. Accordingly, non-US institutions have an incentive to screen their own transactions that involve a correspondent US financial institution to pre-empt any transactions that could put the bank on the radar of US authorities. This screening should include due diligence that is targeted at determining whether the bank's customers, or potential customers, are front companies for sanctioned countries that are trying to access the US financial system.

In 2020, UK-based British Arab Commercial Bank (BACB) paid US$190.7 million for allegedly violating OFAC's Sudanese Sanctions Regulations between 2010 and 2014 by processing 72 bulk funding payments in US dollars on behalf of several Sudanese banks.

On 4 January 2021, OFAC imposed a US$8,572,500 penalty on France-based Union de Banques Arabes et Francaises (UBAF) in connection with the operation of certain US dollar accounts by UBAF on behalf of sanctioned Syrian financial institutions.

Non-US financial institutions also ought to be wary of how far OFAC is willing to extend its jurisdictional reach.

17 See Press release, 'US Dep't of the Treasury and Federal Banking Agencies, Joint Fact Sheet on Foreign Correspondent Banking: Approach to BSA/AML and OFAC Sanctions Supervision and Enforcement' (30 August 2016), at www.treasury.gov/press-center/press-releases/Documents/Foreign%20Correspondent%20Banking%20Fact%20Sheet.pdf.

The BACB[18] and UBAF[19] cases illustrate OFAC's expansive jurisdictional approach and aggressive enforcement posture towards FFIs that engage in transactions with sanctioned parties, even through complex payment structures that appear to be attenuated from the US financial system. In the former case, even though BACB's transactions for Sudanese banks were not themselves processed through the US financial system, the funding of the correspondent account through the referenced bulk transfers did involve transactions processed through US financial institutions and OFAC determined that the correspondent account was established for the purpose of facilitating payments involving Sudan. In the latter case, among other things, UBAF processed US dollar transfers between a sanctioned Syrian entity and a non-sanctioned client on its own books. It then processed US dollar transfers on behalf of its non-sanctioned client, with transaction dates and amounts closely correlated to the related internal transfers on UBAF's books, through a US Bank. UBAF also processed certain foreign exchange (FX) transactions in a similar way, first processing an internal transfer with a sanctioned Syrian customer and then conducting a US-cleared FX transaction that correlated closely with the original FX transaction involving the sanctioned customer.

Virtual currencies

Fintech is an emerging area in which financial institutions need to understand their legal obligations and the potential risk exposure. Regulatory agencies have been actively engaged in this fast-developing sector and have made it clear that it is of equal concern from a sanctions standpoint.

Regulators have focused their attention on virtual currencies, or cryptocurrencies. Cryptocurrencies have increased in popularity as an alternative to fiat currency and their value has grown exponentially in the recent past.[20] Consequently, some financial institutions have taken steps to embrace virtual currencies by creating offerings for their customers to trade cryptocurrencies, allowing them to purchase cryptocurrencies through their systems, or investing in cryptocurrency exchanges.

However, because cryptocurrencies operate in a decentralised and private network that is largely outside the control of any government authority, they have drawn the attention of nefarious actors, who have used them to evade sanctions. Countries such as Russia and Venezuela have invested in national cryptocurrencies,[21] while North Korea and Iran have embraced the use of virtual currencies as a means to evade sanctions.[22]

---

18 See US Dep't of Treasury, Office of Foreign Assets Control, British Arab Commercial Bank plc Settles Potential Liability for Apparent Violations of the Sudanese Sanctions Regulations (17 September 2019), at www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190917_bacb.pdf. Although the Sudanese Sanctions Regulations are no longer in effect, they were in effect during the period of BACB's alleged conduct.

19 OFAC, Enforcement Release, Union de Banques Arabes et Francaises (4 January 2021), at https://home.treasury.gov/system/files/126/01042021_UBAF.pdf.

20 For example, the value of Bitcoin, perhaps the most well-known virtual currency surged to more than $50,000 per Bitcoin for the first time in February 2021.

21 Russia has developed a national cryptocurrency called the CryptoRuble. Venezuela's cryptocurrency is called the Petromoneda or 'Petro'.

22 The Iranian Presidential Center for Strategic Studies has called for Iran to mine cryptocurrency in order to help the economy amid tough international sanctions. See Tanzeel Akhtar, 'Iran Should Mine Crypto to Skirt Sanctions, Says President-Linked Think Tank', Coindesk (3 March 2021), at www.coindesk.com/iran-shoul

As cryptocurrencies have become more established and sanctioned countries have turned to them as a means of circumventing sanctions, regulators have taken notice. OFAC began taking its position on cryptocurrencies in January 2018, when it cautioned that US Persons may be at risk of violating sanctions if they dealt in the Venezuelan cryptocurrency (the petro) explaining at the time that it 'would appear to be an extension of credit to the Venezuelan government'.[23] Following the issuance of Executive Order 13827, which explicitly prohibited US Persons from engaging in all transactions involving 'any digital currency, digital coin, or digital token' issued by the government of Venezuela,[24] OFAC promulgated additional guidance, clearly stating that US Persons and 'persons otherwise subject to OFAC's jurisdiction, including firms that facilitate or engage in online commerce or process transactions using digital currency' are responsible for ensuring that they comply with OFAC sanctions regardless of whether a transaction is denominated in digital or traditional fiat currency.[25] This guidance makes clear that both US and non-US financial institutions need to consider the particular risks of dealing with cryptocurrencies. In effect, OFAC's guidance signals that both US and non-US Persons operating cryptocurrency platforms or processing digital currency payments are prohibited, or should refrain, from providing financial services to restricted parties. In doing so, OFAC advises 'technology companies, administrators, exchangers, users of digital currencies, and other payment processors' to develop a 'tailored, risk-based compliance program', including sanctions list screening. Although OFAC has begun to add digital currency addresses to the SDN List,[26] screening for these identifiers may prove more difficult in practice because it is currently not possible to search for them against OFAC's Sanctions List Search tool.[27] Accordingly, financial and regulated institutions that screen parties manually will have to download the SDN List regularly to screen for all listed digital currency addresses. Institutions that employ automated screening should ensure that the third-party

---

d-mine-crypto-to-skirt-sanctions-says-president-linked-think-tank. North Korea has turned to stealing cryptocurrencies and laundering them as a source of revenue. See US Dep't of Justice, press release, 'Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe' (17 February 2021), at www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

23 See Jacob Osborn, 'OFAC Issues Statement On Venezuelan Digital Currency', *JD Supra* (18 January 2018), at www.jdsupra.com/post/contentViewerEmbed.aspx?fid=2517d8e4-3f3b-4be6-97ce-fc0b5ba6bc31.

24 See Executive Order No. 13,827, 83 Fed. Reg. 12469, 12469 (19 March 2018).

25 See OFAC FAQ No. 559, at www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#559.

26 OFAC first added digital currency addresses to the SDN List on 28 November 2018, when it took action against two Iran-based individuals for their involvement in exchanging bitcoin ransom payments into Iranian rial on behalf of Iranian hackers. See US Dep't of Treasury, press release, 'Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses' (28 November 2018), at https://home.treasury.gov/news/press-releases/sm556. On 21 August 2019, OFAC added the digital currency addresses belonging to three Chinese nationals designated under the Kingpin Act for their involvement in manufacturing and distributing synthetic opioids. See US Dep't of Treasury, press release, 'Treasury Targets Chinese Drug Kingpins Fueling America's Deadly Opioid Crisis' (21 August 2019), at https://home.treasury.gov/news/press-releases/sm756. On 2 March 2020, OFAC added several Bitcoin and Litecoin addresses to the SDN List in connection with its designation of two Chinese nationals for their involvement in laundering cryptocurrency on behalf of the government of North Korea. See US Dep't of Treasury, press release, 'Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group' (2 March 2020), at https://home.treasury.gov/news/press-releases/sm924.

27 See OFAC FAQ No. 594.

systems they are using are routinely updating their databases to include these addresses. In addition, US Persons are also required to block such property in their possession if an SDN has an interest in it. OFAC does not specify a particular method for blocking digital currencies provided there is an audit trail that will allow the digital currency to be unblocked when authorised by OFAC.[28] However, OFAC does provide some guidance by noting that financial institutions can either block each digital currency wallet associated with the digital currency addresses on the SDN List, or otherwise use their own wallets to consolidate wallets that contain the blocked digital currency.[29]

Recent enforcement actions demonstrate that OFAC is increasingly targeting potential sanctions violations relating to digital currency transactions.

> On 30 December 2020, OFAC imposed a US$98,830 penalty on BitGo, Inc. (BitGo), a US technology company, for failing to prevent persons apparently located in US embargoed countries from using its non-custodial secure digital wallet management service.

In each of these cases, OFAC drew attention to deficiencies in the sanctions compliance programmes of BitGo and BitPay respectively. In the *BitGo* case, OFAC's enforcement release states that BitGo had reason to know that the users in question were located in sanctioned jurisdictions based on IP address data associated with devices used to log into the BitGo platform.[30] In the *BitPay* case, BitPay similarly held location information, including IP addresses, about persons located in sanctioned jurisdictions prior to effecting the relevant transactions.[31] These cases serve as a warning to all companies involved in such activity, including financial institutions, to take steps to mitigate risks relating to cryptocurrency transactions in their sanctions compliance programmes, particularly as regards the screening of IP address data.

In parallel with the rise of cryptocurrencies, ransomware attacks have become increasingly prevalent. This often takes the form of malicious software ('malware') designed to block access to a computer system or data, for example by encrypting data on an IT system, to extort ransom payments from victims in exchange for decrypting the information and restoring access to the blocked IT system. Such attacks have become more focused, sophisticated, costly and numerous in recent years. In October 2020, OFAC published an advisory on potential sanctions risks for facilitating ransomware payments in connection with malicious cyber-enabled activities.[32] This guidance is relevant to all companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions that provide financial services that may involve processing ransom payments (including depository institutions and money services businesses). The advisory states that the sanctions compliance programmes of such companies should account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed

28 See OFAC FAQ No. 646.

29 id.

30 OFAC Enforcement Release, BitGo, Inc. (30 December 2020), at https://home.treasury.gov/system/files/126/20201230_bitgo.pdf.

31 OFAC, Enforcement Release, BitPay, Inc. (18 February 2021), at https://home.treasury.gov/system/files/126/20210218_bp.pdf.

32 See US Dep't of Treasury, OFAC, 'Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments' (1 October 2020), at https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

jurisdiction, in addition to any regulatory obligations under Financial Crimes Enforcement network (FinCEN) regulations.[33]

Beyond the United States, regulators have been grappling with similar challenges of how to approach cryptocurrencies. For example, in the United Kingdom, a House of Commons Briefing Paper considering the commercial and regulatory challenges of bitcoin and other exchange tokens was published in February 2020,[34] the Financial Conduct Authority has issued guidance on cryptoassets,[35] and HM Treasury opened a consultation and call for evidence on the UK regulatory approach to cryptoassets and stablecoins in January 2021.[36] The European Parliament has similarly published papers on the legal context and implications of cryptocurrencies and blockchain for financial crime, money laundering and tax evasion[37] and, in September 2020, the European Commission adopted a Digital Finance Package that included a proposed new legislation on cryptoassets.[38]

Digital currencies present unique sanctions risks for financial institutions. Recent developments illustrate that this is an area of emerging enforcement interest in the United States and that further regulations are under consideration elsewhere. Accordingly, financial institutions need to take appropriate risk-based steps to ensure that cryptocurrencies do not become a compliance pitfall. In particular, cryptocurrency transactions ought to be subject to compliance screening and KYC due diligence processes to ensure that they do not involve direct dealings or the facilitation of transactions on behalf of designated persons. In practice, this can be complicated by the confidentiality that cryptocurrencies afford their users. It will also be important to implement procedures for maintaining an independent record of digital currency transactions that can be used to establish a compliance record in the event of a regulatory inquiry. Financial institutions also need to incorporate digital currencies into their procedures for reporting blocked property or rejected transactions to OFAC.

---

33 See FinCEN Guidance, FIN-2020-A00X, 'Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments' (1 October 2020), for applicable anti-money laundering obligations related to financial institutions in the ransomware context, at www.fincen.gov/resources/advisories/fincen-advisory-fin-2020-a006

34 Steven Browning, 'Cryptocurrencies: Bitcoin and other exchange tokens', House of Commons Briefing Paper, (19 February 2020), at https://commonslibrary.parliament.uk/research-briefings/cbp-8780/. Perhaps illustrating just how volatile and uncertain this area is, the House of Commons Briefing Paper states: 'In June 2019, Facebook announced the proposed launch of a new cryptocurrency, the Libra . . . But the political and regulatory response has been very critical. Many partners have since withdrawn from the project.'

35 UK Financial Conduct Authority, 'Guidance of Cryptoassets', Consultation Paper CP19/3* (January 2019), at https://www.fca.org.uk/publication/consultation/cp19-03.pdf.

36 HM Treasury, 'UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence' (January 2021), at www.gov.uk/government/consultations/uk-regulatory-approach-to-cryptoassets-and-stablecoins-consultation-and-call-for-evidence

37 See, e.g., European Parliament Study, Dr Robby Houben and Alexander Snyers, 'Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion' (July 2018), at www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf.

38 European Commission, 'Digital Finance Package: Commission sets out new, ambitious approach to encourage responsible innovation to benefit consumers and businesses' (24 September 2020), at https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684.

Commingled assets

A challenge financial institutions increasingly face is how to appropriately manage sanctioned interests that exist in pools of commingled assets. This issue may arise in connection with securities custodies or in bulk foreign exchange transactions in which large net settlement payments may be made and some portion of the settlement amount can be arguably attributable to the accounts of sanctioned persons. A closer examination of relevant OFAC enforcement actions on this topic gives some indications as to the risks financial institutions may face in this regard, and the steps that can be taken to mitigate those risks.

In 2014, Clearstream Banking, SA (Clearstream), a Luxembourg entity, paid US$151.9 million to settle potential liability for apparent violations of the Iranian Transactions and Sanctions Regulations. Clearstream maintained an account with a US financial institution in New York through which certain securities, in which the Central Bank of Iran held a beneficial interest, were held in custody at a central securities depository in the United States.

The US financial institution did not have any visibility as to the beneficial ownership interests in the securities at the US depository maintained through the Clearstream account. It transpired that the Central Bank of Iran (CBI) maintained a beneficial ownership interest in these securities. The ultimate place of custody for those securities was the United States and the CBI's interest was held through Clearstream's omnibus account in New York. Although the CBI's interest was buried one layer deep in the custodial chain, the effect was that Clearstream, as intermediary, had exported custody and related services from the United States to the CBI in apparent violation of the Iranian Transactions and Sanctions Regulations.[39]

In 2015, UBS AG (UBS), a Swiss entity, paid US$1.7 million to settle apparent violations of the Global Terrorism Sanctions Regulations. UBS processed more than 200 transactions relating to securities held in custody in the United States for or on behalf of an individual customer who was a designated person.

Although the accounts of the UBS client were blocked in Switzerland following the designation (similar restrictions were imposed by Swiss and other authorities), UBS continued to engage in investment-related activity on the client's behalf, including processing US dollar securities-related transactions to or through the United States. The processing of these securities transactions did not generate any alerts against the client's name because they all amounted to internal transfers that did not involve external parties and were therefore not screened in the same way as outbound and inbound funds transfers.[40]

39 US Dep't of Treasury, OFAC Enforcement Notice, Clearstream Banking, S.A. Settles Potential Liability for Apparent Violations of Iranian Sanctions (23 January 2014), at www.treasury.gov/resource-center/sanctions/CivPen/Documents/20140123_clearstream.pdf.

40 US Dep't of Treasury, OFAC Enforcement Notice, UBS AG Settles Potential Liability for Apparent Violations of the Global Terrorism Sanctions Regulations (27 August 2015), at www.treasury.gov/resource-center/sanctions/

In both of the above cases, transactions undertaken by non-US financial institutions with respect to omnibus accounts held in those institutions' names were considered to violate OFAC sanctions because of a sanctions target's beneficial interest in the underlying securities.

In 2018, JPMorgan Chase NA (JPMC), a US entity, paid US$5.26 million to settle apparent violations of multiple US sanctions programmes. JPMC processed 87 net settlement payments worth in excess of US$1 billion on behalf of two airline associations, of which approximately 0.14 per cent appeared to have been attributable to designated airlines.

The net settlement mechanism employed by JPMC resolved billings by and among its client, a US entity and its members (approximately 100), and a non-US entity and its members (more than 350). The transactions themselves each represented a net settlement payment between JPMC's client and the non-US Person entity, whose members included certain airlines that were at various times designated persons. As with the securities cases, OFAC viewed the transactions in this case as violations despite the designated airlines' minuscule interest in the transactions that were carried out on behalf of the non-designated associations. OFAC also noted that JPMC failed to screen participating member airlines despite being in possession of information necessary to enable screening, and noted that JPMC did not appear to have a process in place to independently evaluate the participating member airlines for sanctions risk, despite having received red flag notifications for OFAC-sanctioned members on numerous occasions.[41]

These cases highlight the importance of financial institutions taking appropriate steps to identify sanctioned interests even if those interests comprise a small part of a larger transaction, such as in a net settlement transaction or in respect of securities held in an omnibus account. The practical challenge is to ensure there are processes in place to effectively identify sanctioned interests when they are commingled in a group of assets, including where the assets are transferred internally, and to implement controls (such as the isolation or sequestration of frozen assets in a separate account) to ensure that the sanctioned interests are not transferred or dealt in.

Recent enforcement trends

Financial institutions and regulated entities continue to be a target for regulatory enforcement actions. In 2019, more than 30 per cent of OFAC's 22 enforcement actions targeted financial institutions or other regulated entities, such as insurance companies. These cases, though representing less than a third of the enforcement actions taken, accounted for approximately US$1.27 billion in penalties, or around 98.8 per cent of OFAC's total penalties for the year. This includes penalties in excess of US$600 million levied against each of Unicredit Bank and Standard Chartered Bank. In 2020, two of OFAC's 16 enforcement actions targeted financial institutions and these were followed by a US$8.5 million penalty that was levied

CivPen/Documents/20150827_ubs.pdf.

41 US Dep't of Treasury, OFAC Enforcement Notice, JPMorgan Chase N.A. Settles Potential Civil Liability for Apparent Violations of Multiple Sanctions Programs (5 October 2018), at www.treasury.gov/resource-center/sanctions/CivPen/Documents/jpmc_10050218.pdf.

against UBAF in January 2021. The message is clear: financial institutions and regulated entities are, and remain, in the words of OFAC Director Andrea Gacki, OFAC's 'principal customers',[42] and so compliance with US sanctions for both US and non-US entities in these sectors remains of paramount importance.

Perhaps a more significant shift in the enforcement environment in recent times is the emergence of OFSI as a serious sanctions enforcement authority. The UK Policing and Crime Act 2017 established a civil enforcement authority for OFSI from 1 April 2017, making its powers similar to OFAC's. Indeed, the announcement of a £20.4 million penalty against Standard Chartered Bank on 31 March 2020 has made financial institutions and regulated entities take note. Three of OFSI's four concluded civil enforcement actions to date have targeted financial institutions and regulated entities, which could indicate OFSI's focus going forward. Furthermore, in October 2020, OFSI noted that a majority of the 140 reports of potential sanctions breaches in 2019–2020 (with a total value of almost £1 billion) were reported by the financial services sector.

Sanctions clauses in financing documents

It is common practice for financial institutions and regulated entities to include sanctions clauses in their financing documents as part of a sanctions toolkit to identify and mitigate sanctions risks. The negotiation of sanctions clauses in financing documents can help to flush out potential sanctions risks at the outset of a transaction or new customer relationship, and often reflects the risk assessment and due diligence conducted by the financial institution or regulated entity. Model clauses in lower risk transactions may include sanctions definitions, representations and undertakings. In higher risk transactions, more extensive sanctions clauses may include other rights, such as termination, mandatory prepayment and information rights as well as more extensive representations and undertakings.

Sanctions clauses present an opportunity for financial institutions and regulated entities to impose standards under their financing documents that reflect their own regulatory obligations and, where different, internal policy. This can be relevant in various situations. For example, a US financial institution may require a non-US incorporated obligor to comply with US sanctions within the sanctions clauses in its financing documents even if there is no US nexus to the underlying activity of the obligor. In another example, if a financial institution has a policy of financing no activity whatsoever with certain territories (such as US embargoed territories) even if the activity were permitted by law (e.g., under a licence), that financial institution may also impose clauses that are more restrictive than the technical legal position so as to reflect its own internal policies and risk appetite. In addition to ensuring that business financed by a financial institution is in compliance with applicable sanctions and internal policy, strict contractual requirements will typically provide a number of contractual options to the financial institution in the event a breach of sanctions occurs in respect of a transaction. This could include triggering mandatory prepayment rights, acceleration or even an event of default.

42 Sam Fry, 'OFAC director: "Our jurisdiction is not limited to banks"', *Global Investigations Review* (18 October 2019), at https://globalinvestigationsreview.com/article/1209748/ofac-director-%E2%80%9Cour-jurisdiction-is-not-limited-to-banks%E2%80%9D.

A recent UK case underscores the importance of contracting parties closely assessing the sanctions risks that will or may arise under a transaction, and taking appropriate steps to allocate those risks under the contract. In *Lamesa Investments Ltd v. Cynergy Bank Ltd*,[43] the High Court of England and Wales (EWHC) considered what is meant by the words 'a mandatory provision of law'. The relevant contract had a provision whereby the defendant (Cynergy Bank Ltd (CBL)) could resist payment under the facility agreement when 'such sums were not paid in order to comply with any mandatory provision of law, regulation or order of any court of competent jurisdiction'. After entry into the contract, the beneficial owner of the claimant (Lamesa Investments Ltd (LIL)) became designated as an SDN.

At first instance, CBL successfully argued that its failure to make payments under the facility agreement with LIL was not a default on the basis that LIL's beneficial owner had become subject to US sanctions by relying on wording in the facility agreement. EWHC agreed that the wording used in the facility agreement included the risk of being subject to restrictive measures under US secondary sanctions. LIL appealed.[44] In upholding the first instance ruling, the Court of Appeal of England and Wales (EWCA) identified a number of relevant contextual factors. Notably, EWCA considered that the drafters of the relevant sanctions clause would have been aware that the clause employed similar language to the EU Blocking Regulation,[45] which itself describes US secondary sanctions as imposing a 'requirement or prohibition' with which EU entities are required to 'comply'. Among other things, EWCA determined that the drafters must have intended the borrower to be capable of obtaining relief from default if its reason for non-payment was to comply with US secondary sanctions. The appeal was, therefore, dismissed.

Another EWHC case brings into focus the importance of carefully drafting sanctions clauses in contracts. In *Mamancochet Mining Ltd v. Aegis Managing Agency Ltd & Others*,[46] the non-US defendant underwriters, some of whom were owned or controlled by US Persons, sought to resist payment under a marine cargo insurance policy following the theft of two cargoes of steel billets when in Iran. The relevant sanctions clause stated that 'no (re)insurer shall be liable to pay any claim . . . to the extent that . . . payment of such claim . . . would expose that (re)insurer to any sanction, prohibition or restriction under . . . the trade or economic sanctions, laws, or regulations of the European Union, United Kingdom or the United States of America'. The insurers sought to rely on this clause to deny cover to the claimant, arguing that payment under the policy would 'expose' them to the risk of secondary sanctions. EWHC found that 'exposure' to sanctions meant that a payment had to actually breach sanctions, as opposed to merely exposing insurers to a real risk of breach. Therefore, the insurers were liable to pay the insurance claim. In its *obiter* comments, EWHC also saw 'considerable force' in the argument that the EU Blocking Regulation[47] is not engaged when an insurer's liability to pay a claim is suspended under a sanctions clause on the basis that the insurer would be relying on the terms of the relevant policy to resist payment as opposed to 'complying' with a third country's prohibition.

43 [2019] EWHC 1877 (Comm).

44 [2020] EWCA Civ 821.

45 Council Regulation (EC) No. 2271/96 (as amended).

46 [2018] EWHC 2643 (Comm).

47 Council Regulation (EC) No. 2271/96 (as amended).

Alternative currency clauses

One recent trend in terms of sanctions clauses is the increased use of alternative currency clauses. The purpose of alternative currency clauses is usually to obviate US primary sanctions risk in the event a party or a transaction becomes subject to US sanctions. Since OFAC jurisdiction is currency neutral and is ordinarily triggered by the involvement of a US Person, alternative currency clauses are only likely to be appropriate in dealings where the only US nexus is the provision for optional US dollar payments, which are likely to involve the US financial system. That is to say alternative currency clauses are likely to appear in practice in dealings involving non-US financial institutions in transactions that otherwise have no US nexus.

Alternative currency clauses are capable of bringing mutual benefit both to borrowers and to non-US financial institutions. From a borrower's perspective, these types of clauses may help to avoid an event of default or mandatory prepayment event if new US sanctions prohibit continued payments to a non-US financial institution in US dollars. From a non-US financial institution's perspective, these types of clauses may ensure that the arrangements with the customer can continue and the business relationship is maintained, albeit with payments being received in a different currency.

A key question for financial institutions and regulated entities is whether the existence and operation of an alternative currency clause could give rise to a risk of 'circumventing' US sanctions warranting the application of sanctions or other consequences. While it is impossible to anticipate how OFAC will interpret the operation of an alternative currency clause on the basis of a specific fact pattern, OFAC jurisdiction would not ordinarily be implicated following the engagement of an alternative currency clause if a non-US borrower makes payments to a non-US financial institution or regulated entity with no apparent US nexus.[48] The mechanism to reach this position, however, can be subject to significant negotiation.

In our experience, there are two main characteristics of alternative currency clauses that may be subject to negotiation. First, the engagement of an alternative currency clause can typically be triggered either by the borrower or automatically by virtue of specific circumstances arising. In the first situation, a borrower may submit a request to pay in an alternative currency (e.g., to the facility agent) either because of legal restrictions preventing payments being made in US dollars or for other specified or non-specified reasons. In the alternative situation, an alternative currency clause may be engaged automatically by virtue of a legal restriction (such as the imposition of US sanctions) effectively preventing payment in the primary currency (i.e., US dollars).

Second, lender approval may be automatic, or lender consent may be required, under the alternative currency clause. In a syndicated facility involving a mixture of US and non-US financial institutions, an automatic mechanism whereby the financial institutions do not need to participate in a decision to change the currency (i.e., an automatic mechanism) may help to minimise any circumvention risk, or the risk of being accused of circumvention, particularly as the negotiation of such clauses would have presumably been concluded before the circumstances leading to the engagement of an alternative currency clause arose.

48 Even assuming no jurisdiction to impose penalties, as discussed above, foreign financial institutions should consider the potential risk of secondary sanctions and blocking authorities when an alternative currency clause may be engaged.

That said, some non-US financial institutions may take the view that express approval for the activation of an alternative currency clause is required so that analysis of the request for a currency switch can be conducted at the relevant time based on the specific facts surrounding the request.

There is no current market standard with regard to alternative currency clauses, although some financial institutions and regulated entities have adopted institutional approaches towards these types of clauses. In practice, the drafting of these clauses should be approached with caution, and give due consideration to the factors described above and in the context of any other transaction or party-specific risks.

Appendix 2

About the Authors

Jason Hungerford
Mayer Brown

Jason Hungerford is a US- and UK-qualified investigations and regulatory partner based in Mayer Brown's London office. Previously based in Washington, DC, Jason advises corporates and financial institutions on economic sanctions and export controls, anti-corruption and anti-money laundering in the context of investigations, complex transactions and compliance programme development and testing.

Jason advises clients across a range of sectors, including financial services, aerospace and defence, oil and gas, mining, shipping, transportation, engineering and heavy machinery, and fast-moving consumer goods. Jason's investigations and compliance work has included mandates in China, South-East Asia, Russia, Brazil, the United States, the Middle East, the Nordic region and throughout Europe.

Jason focuses on US and EU economic sanctions; US, UK and EU dual-use and military end-use trade controls; the US Foreign Corrupt Practices Act and the UK Bribery Act; the UK Proceeds of Crime Act; and the UK Modern Slavery Act. In the course of his practice, Jason represents clients in related enforcement, licensing and interpretive matters before the US Treasury Department's Office of Foreign Assets Control, HM Treasury's Office of Financial Sanctions Implementation, HM Revenue and Customs, the UK Export Control Joint Unit, the US State Department and the US Commerce Department.

Jason serves on the Law Society of England and Wales's Money Laundering Task Force as a financial sanctions adviser.

Ori Lev
Mayer Brown

Ori Lev is a partner in Mayer Brown's Washington, DC, office. He concentrates his practice on representing financial institutions and other companies in government enforcement matters, internal investigations and litigation, and providing regulatory advice and counsel

on economic sanctions and federal consumer financial law. Ori has an extensive regulatory enforcement background, both at the US Treasury Department's Office of Foreign Assets Control (OFAC), where he led the Office of Enforcement and served in other leadership positions, and at the Consumer Financial Protection Bureau, of which he was a founding member and where he served as a deputy enforcement director.

Ori has led internal investigations, helped companies respond to OFAC subpoenas, drafted licence applications and self-disclosures to OFAC, and provided counsel on the applicability of OFAC regulations to a wide range of business conduct. In 2019, Ori was identified as one of the 25 'most respected sanctions lawyers' in Washington, DC, by *Global Investigations Review*.

While serving as senior adviser and then head of enforcement at OFAC, Ori was involved in OFAC's early dollar-clearing and wire-stripping cases, oversaw and reorganised OFAC's enforcement function and participated in major policy decisions. He was the also principal drafter of OFAC's Economic Sanctions Enforcement Guidelines.

Tamer Soliman
Mayer Brown

Tamer Soliman is a partner in Mayer Brown's Washington, DC, and Dubai offices and the global head of the firm's export control and sanctions practice. He advises corporate and government clients on a wide range of international trade issues governing cross-border investments, joint ventures and sales, manufacturing and the development of emerging technologies.

His practice focuses on export control, sanctions and related national security restrictions on trade. For over two decades, he has handled complex export control and sanctions regulatory issues and enforcement proceedings spanning multiple jurisdictions. He advises clients in a wide range of industries, including aerospace and defence, sovereign wealth and investment funds, financial services, private equity, internet technology and logistics.

Prior to joining Mayer Brown in 2017, Tamer spearheaded the international expansion of the export control and sanctions practice at another prominent international law firm based in Washington. He is known for handling cutting-edge issues involving application of the International Traffic in Arms Regulations, Export Administration Regulations and sanctions laws to both US and non-US entities and has successfully advised boards, audit committees and companies in high-stakes investigations and enforcement actions. Tamer has successfully defended both US and non-US companies in multi-agency, data-intensive investigations under applicable export control and sanctions laws.

James Ford
Mayer Brown

James Ford is a senior associate in Mayer Brown's London office. He focuses on regulatory compliance, transactional advice and investigations in the areas of economic sanctions, export controls, anti-corruption and money laundering. He has advised corporates across a range of sectors, including energy, mining and extractives, finance, defence and transport. He has also advised a range of financial institutions, insurers and brokers.

James advises clients on: designing and implementing compliance programmes; compliance programme reviews; designing and delivering training; conducting investigations;

drafting and submitting disclosures; liaising with regulators and supporting licence applications; and transaction due diligence.

His experience includes in-house experience in four different sectors. He has been seconded to the sanctions team of a major European bank, the group legal team of a European-headquartered mining company, the group export controls team of a major defence company during the term of a Consent Agreement with the US State Department, the disputes team of a major international bank, and the bribery and corruption team of a global oil and gas company.

James established and leads the Transparency International Professional Supporters Network, a volunteer initiative of professionals, academics and students aimed at supporting Transparency International's advocacy and outreach efforts.

Timothy C Lee

Tim Lee is formerly an associate in Mayer Brown's Washington, DC, office and currently serves as in-house counsel for sanctions and export controls at a global social media and technology company.

Mayer Brown
201 Bishopsgate
London EC2M 3AF
United Kingdom
Tel: +44 20 3130 3000
jhungerford@mayerbrown.com
jford@mayerbrown.com

1999 K Street, NW
Washington, DC 20006-1101
United States
Tel: +1 202 263 3000
olev@mayerbrown.com
tsoliman@mayerbrown.com

www.mayerbrown.com

We live in a new era for sanctions. More states are using them, in more creative (and often unilateral) ways.

This creates ever more complication for everybody else. Hitherto no book has addressed all the issues raised by the proliferation of sanctions regimes and investigations in a structured way. GIR's *The Guide to Sanctions* addresses that. 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, providing an invaluable resource.

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

an LBR business

ISBN 978-1-83862-596-2