THE GUIDE TO SANCTIONS

THIRD EDITION

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

The Guide to Sanctions

Third Edition

Editors

Rachel Barnes QC

Paul Feldberg

Nicholas Turner

Anna Bradshaw

David Mortlock

Anahita Thoms

Rachel Alpert

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2022
For further information please contact insight@globalinvestigationsreview.com

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

www.globalinvestigationsreview.com

ISBN 978-1-83862-874-1

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 LLP

Carter-Ruck

Cravath, Swaine & Moore LLP

Eversheds Sutherland

Fangda Partners

Forensic Risk Alliance

Global Law Office

Jenner & Block LLP

McGuireWoods LLP

Mayer Brown

Miller & Chevalier Chartered

Navacelle

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.

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

Sanctions have truly become a go-to tool. And little wonder. They are powerful; they reach people who would otherwise be beyond our reach. They are easy – you can impose or change them at a stroke, without legislative scrutiny. And they are cheap (in the simplest sense)! It's up to others once they're in place to do all the heavy lifting.

The heavy lifting part is where this book can help. The pullulation of sanctions regimes, and 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.

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*.

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 2022

Contents

Foreword

I am delighted to welcome you to this third edition of Global Investigations Review's *The Guide to Sanctions*. The international, geographical, political, criminal, legal and regulatory elements that make up sanctions programmes ensure that this will remain one of the most complex compliance areas facing practitioners. The following chapters contain important information, advice and best practice for sanctions and export controls as a compliance discipline, courtesy of some of the world's leading legal, forensic and compliance specialists. The daily change to the international regimes requires practitioners and businesses to be constantly monitoring and horizon-scanning across all relevant jurisdictions, and the Guide is packed full of resources that will enable readers to do just that.

The current sanctions environment makes this Guide a must read for any practitioner who manages or advises on sanctions compliance. This Guide is the work of leading industry specialists who have all given their time and expertise to produce a resource that should be on every bookshelf. At a time of growing complexity, readers may find the Guide worthy of being constantly consulted as a valuable reference resource, not only in its own right, but also for the treasure trove of links and references to information and guidance provided by the regulators who guide industry in implementing sanctions policy.

Sanctions never sleep, and since the previous version of this Guide, we have seen the UK settle into an autonomous programme and increased international coordination with major countries and blocs looking to align as closely as possible. The US is no longer the only major player.

The sanctions regimes in place for countries such as Iran, Syria, North Korea and Yemen, to name just a few, have continued to evolve, but the focus since August 2021 has been squarely on Russia and Belarus. This Guide will bring you

up to date with the significant changes in those regimes, as at the time of writing, covering both the sanctions and export controls, as well as updating you on the developments in other regimes, including China and Hong Kong.

As with earlier editions, this third edition covers the major sanctions programmes from the United Nations, the United States, the European Union, the United Kingdom and the Asia-Pacific region, including the types of prohibitions imposed by the relevant programmes, the licence procedures and the measures that are available to challenge listings. Each of the major jurisdictions has an enforcement section that details the process and elements of enforcement from the relevant jurisdiction. The Guide also covers the re-emergence of thematic sanctions programmes; no longer limited to terrorism and narcotics, these programmes have seen a significant growth over the past few years. The third edition welcomes new authors who share their experiences representing sanctioned clients, among others.

The section on compliance programmes will enable readers to review their own programmes against best practice and improve and enhance their own controls if required. The final section covers sanctions and export controls in practice, giving good advice on how to navigate international, extraterritorial and often conflicting requirements of global sanctions and export control rules.

It is important to remember that financial crime is not a competition and that we make the biggest impact when we work together across industry and governments. The partnerships and collaboration across the globe play an important part in managing international sanctions. Part of my role at UK Finance is to liaise with industry and governments to help promote public–private partnerships and ensure that we are all fighting financial crime, especially in the sanctions space, as a coordinated and collaborative network of specialists, in the UK and elsewhere.

The Guide to Sanctions is intended to enable readers to be a valuable part of the sanctions and export controls community, dedicated to fighting financial crime and helping to protect our wider society from the impacts of those that seek to cause harm on the international stage.

Neil Whiley
Director of Sanctions, UK Finance
June 2022

Part III

Sanctions in Practice

CHAPTER 20

Issues Arising for Financial Institutions and Regulated Entities

Jason Hungerford, Ori Lev, Tamer Soliman and James Ford[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 activities 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 significant sanctions targeting

1 Jason Hungerford, Ori Lev and Tamer Soliman are partners, and James Ford is a senior associate, at Mayer Brown. The authors thank Timothy C Lee for his contribution to previous editions of this chapter.

the FFI, including but not limited to 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 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), the Hong Kong Autonomy Act in relation to Hong Kong, various Hezbollah and global terrorism-related authorities, 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 nine 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

2 31 C.F.R. 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 https://home.treasury.gov/news/press-releases/tg1661.

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.

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 raft of sanctions imposed by a coalition of nations led by the US, EU and UK targeting Russia in particular in light of the conflict in Ukraine has created a number of further challenges for financial institutions and regulated entities. For example, the imposition of sanctions on hundreds of Russian oligarchs by the US, EU and UK (among others) has created new challenges as regards both new and existing business relationships. Two particular areas come to mind. First, despite close coordination of sanctions across G7 nations generally, sanctions authorities have not taken a uniform approach towards which individuals and entities have been designated as subject to asset freeze sanctions; thus, dealings with certain individuals and entities, or entities that they own or control, are prohibited under certain sanctions regimes, but not others. Second, the EU and UK, respectively, have issued guidance to clarify their approach towards assessing ownership and control. The EU issued FAQs in April 2022 that indicate that, where two or more listed persons are each minority shareholders of a non-listed entity, but their aggregate ownership amounts to more than 50 per cent of that entity, the entity should be considered as owned and controlled by listed persons.[6] In contrast, the UK updated its financial sanctions guidance in March 2022 and stated that UK authorities would not simply aggregate different designated persons' holdings in a company, unless, for example, the shares or rights are subject to a joint arrangement between the designated parties or one party controlled the rights of another.[7] These respective tests for 'ownership and control' differ in certain respects to the

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 https://home.treasury.gov/policy-issues/financial-sanctions/faqs/526.

6 European Commission, 'Assets freeze and prohibition to make funds and economic resources available' (4 May 2022), at https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/faqs-sanctions-russia-assets-freezes_en.pdf.

7 Office of Financial Sanctions Implementation HM Treasury (updated 22 March 2022), Section 4.1.4, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1062452/General_Guidance_-_UK_Financial_Sanctions.pdf.

established 50 Percent Rule adopted by OFAC, namely that a party is considered subject to blocking sanctions should it be owned 50 per cent or more in the aggregate by one or more SDNs.[8]

The practical implication 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 and control, 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 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, EU and UK sectoral sanctions targets, giving due

8 OFAC, 'Revised guidance on entities owned by persons whose property and interests in property are blocked' (13 August 2014), at https://home.treasury.gov/system/files/126/licensing_guidance.pdf.

consideration to relevant regulatory guidance.[9] Penalties for breaching these sanctions can be significant.[10]

> 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 1 April 2022, OFAC imposed a US$78,750 penalty on S&P Global, 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 past enforcement action,

---

9 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/info/sites/default/files/business_economy_euro/banking_and_finance/documents/170825-guidance-implementation-regulation-833-2014_en.pdf; OFAC FAQ Nos. 370–375, 391–396, 404–411, 419.

10 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; OFAC, Enforcement Notice, Haverly Systems, Inc. (25 April 2019), at https://home.treasury.gov/system/files/126/20190425_haverly.pdf; OFAC, Enforcement Notice, S&P Global, Inc. (1 April 2022), at https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220401_33.

OFAC's enforcement notice states that details of North Korean entities were replaced by details of intermediaries based in third countries on relevant transaction documents.[11]

> 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 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.[12] 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

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

12 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.

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 additionally report on blocked property annually by 30 September for assets blocked as of 30 June.[13]

From 21 June 2019, OFAC expanded these obligations in several ways.[14] 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, and to all rejected transactions, not just rejected fund transfers. 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. 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.[15] For example, UK sanctions regulations require financial institutions and certain other regulated businesses

13 31 C.F.R. §§ 501.603 (blocked property reports), 501.604 (rejected transaction reports).

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

15 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,

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.[16] 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.[17]

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.[18] 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. 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

---

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.

16 OFSI Guidance at Chapter 5.1.1.

17 id.

18 OFSI, Financial Sanctions Notice (6 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.

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.[19]

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.

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

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 an 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.

19 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.occ.gov/publications-and-resources/publications/banker-education/files/pub-foreign-correspondent-banking-fact-sheet.pdf.

The *BACB*[20] and *UBAF*[21] 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.

The UK and EU have recently adopted correspondent banking and other restrictions in light of the conflict in Ukraine that may impact financial institutions' correspondent banking relationships. For example, the UK has introduced a prohibition on UK credit or financial institutions establishing or continuing a correspondent banking relationship, and from processing sterling payments to, from or via a designated person or a credit or financial institution owned or controlled by them. This has significant implications for UK financial institutions that have any exposure to Russian clients and counterparties. In the EU, there has been an introduction of a new breed of restrictions that are more expansive than sectoral sanctions, but short of an asset freeze. In particular, the EU has introduced a prohibition on engaging in any transactions with certain listed entities, entities outside the EU owned more than 50 per cent by those listed entities, and

20 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 https://home.treasury.gov/system/files/126/20190917_bacb.pdf. Although the Sudanese Sanctions Regulations are no longer in effect, they were in effect during the period of British Arab Commercial Bank's alleged conduct.

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

any entity acting on behalf of or at the direction of any of those entities.[22] The EU has also introduced a prohibition on the provision of specialised financial messaging services (such as the use of the SWIFT system) to a number of listed Russian and Belarusian financial institutions.

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. 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,[23] while North Korea and Iran have embraced the use of virtual currencies as a means to evade sanctions.[24]

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

22 Council Regulation (EU) 2022/428 amending Regulation (EU) No. 833/2014, Annex XIX, at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:087I:FULL&from=EN.

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

24 The Iranian Presidential Center for Strategic Studies has called for Iran to mine cryptocurrency 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-should-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.

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'.[25] 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,[26] 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.[27] 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 List of Specially Designated Nationals and Blocked Persons (the SDN List),[28]

---

25 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.

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

27 See OFAC FAQ No. 559, at https://home.treasury.gov/policy-issues/financial-sanctions/faqs/559.

28 OFAC first added digital currency addresses to the List of Specially Designated Nationals and Blocked Persons (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,

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.[29] 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 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.[30] 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.[31]

Recent enforcement actions demonstrate that OFAC is increasingly targeting potential digital currency transaction sanctions violations.

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

On 18 February 2021, OFAC imposed a US$507,375 penalty on BitPay, Inc, a US payment processing company, for failing to prevent persons apparently located in US embargoed territories from transacting with merchants in the United States through the BitPay platform.

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 internet protocol (IP)

'Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group' (2 March 2020), at https://home.treasury.gov/news/press-releases/sm924.

29 See OFAC FAQ No. 594.

30 See OFAC FAQ No. 646.

31 id.

address data associated with devices used to log into the BitGo platform.[32] In the *BitPay* case, BitPay similarly held location information, including IP addresses, about persons located in sanctioned jurisdictions prior to effecting the relevant transactions.[33] 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 September 2021, OFAC published an updated advisory on potential sanctions risks for facilitating ransomware payments in connection with malicious cyber-enabled activities.[34] 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 jurisdiction, in addition to any regulatory obligations under Financial Crimes Enforcement Network regulations.[35]

Beyond the United States, regulators have been grappling with similar challenges of how to approach cryptocurrencies. For example, in the United Kingdom, the House of Lords published a paper in January 2022 considering the risks and

---

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

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

34 See US Dep't of Treasury, OFAC, 'Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments' (21 September 2021), at https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

35 See Financial Crimes Enforcement Network Guidance, FIN-2021-A004, 'Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments' (8 November 2021), for applicable anti-money laundering obligations related to financial institutions in the ransomware context, at www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf.

benefits of a central bank digital currency;[36] the Financial Conduct Authority has issued guidance on cryptoassets;[37] and the UK government set out plans to make the UK a global cryptoasset technology hub in April 2022 following a public consultation on the UK regulatory approach to cryptoassets and stablecoins.[38] 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[39] and, in March 2022, it agreed draft rules on the supervision, consumer protection and environmental sustainability of cryptoassets, including cryptocurrencies such as Bitcoin.[40]

Digital currencies and other cryptoassets 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

---

36 'Central bank digital currencies: a solution in search of a problem?', House of Lords, Economic Affairs Committee (13 January 2022), at https://committees.parliament.uk/publications/8443/documents/85604/default/.

37 UK Financial Conduct Authority (FCA), 'Guidance of Cryptoassets', Consultation Paper CP19/3* (January 2019), at www.fca.org.uk/publication/consultation/cp19-03.pdf; Joint statement from UK financial regulatory authorities on sanctions and the cryptoasset sector (11 March 2022), at www.fca.org.uk/news/statements/uk-financial-regulatory-authorities-sanctions-cryptoasset-sector; Notice to all FCA regulated firms with exposure to cryptoassets (24 March 2022), at www.fca.org.uk/news/statements/notice-regulated-firms-exposure-cryptoassets.

38 HM Treasury, 'Government sets out plan to make UK a global cryptoasset technology hub', (4 April 2022), at www.gov.uk/government/news/government-sets-out-plan-to-make-uk-a-global-cryptoasset-technology-hub; HM Treasury, 'UK regulatory approach to cryptoassets, stablecoins, and distributed ledger technology in financial markets: Response to the consultation and call for evidence' (April 2022), at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066166/O-S_Stablecoins_consultation_response.pdf.

39 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.

40 European Parliament, 'Cryptocurrencies in the EU: new rules to boost benefits and curb threats' (14 March 2022), at www.europarl.europa.eu/news/en/press-room/20220309IPR25162/cryptocurrencies-in-the-eu-new-rules-to-boost-benefits-and-curb-threats#:~:text=Crypto%2Dassets%2C%20including%20cryptocurrencies%2C,market%20manipulation%20and%20financial%20crime.

not involve direct dealings with 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.

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, 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.[41]

In 2015, UBS AG, 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.[42]

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.

41 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 https://home.treasury.gov/system/files/126/20140123_clearstream.pdf.

42 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 https://home.treasury.gov/system/files/126/20150827_ubs.pdf.

The net settlement mechanism employed by JPMorgan Chase NA (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.[43]

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 2021, 45 per cent of OFAC's 20 enforcement actions targeted financial institutions or other regulated entities, such as payment services companies. These cases accounted for US$13.8 million in penalties, or more than 66 per cent of OFAC's total penalties for the year. The message is clear: financial institutions and regulated entities are, and remain, in the words of OFAC

43 US Dep't of Treasury, OFAC Enforcement Notice, 'JPMorgan Chase Bank, N.A. Settles Potential Civil Liability for Apparent Violations of Multiple Sanctions Programs' (5 October 2018), at https://home.treasury.gov/system/files/126/jpmc_10050218.pdf.

Director Andrea Gacki, OFAC's 'principal customers',[44] 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. The UK's sanctions enforcement focus has also expanded to include fintech companies. In particular, in 2021, OFSI imposed monetary penalties on two fintech companies in connection with multiple payments made on behalf of non-sanctioned parties to accounts held at a sanctioned bank.[45] To date, five of OFSI's six concluded civil enforcement actions have targeted financial institutions and regulated entities, which could indicate OFSI's focus going forward. Furthermore, in October 2021, OFSI noted that 132 potential sanctions breaches were reported in 2020–2021, a majority of which were reported by the financial services sector.[46]

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.

---

44 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.

45 HM Treasury, OFSI, Report of Penalty for Breach of Financial Sanctions Regulations (Section 149(2) PACA 2017 report), 'Imposition of Monetary Penalty – TransferGo Limited' (25 June 2021), at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1008859/050821_-_TransferGo_Penalty_Report.pdf; OFSI, Report of Penalty for Breach of Financial Sanctions Regulations (Section 149(2) PACA 2017 report), 'Imposition of Monetary Penalty – Clear Junction Limited' (25 June 2021), at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1056043/Clear_Junction_Penalty_Report_21.02.22.pdf.

46 OFSI, Annual Review 2021, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025562/OFSI_Annual_Review_2021.pdf.

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. One recent trend in sanctions clauses in light of the conflict in Ukraine is the expansion of the definition of embargoed territories to include the non-government controlled areas of the Donetsk and Luhansk oblasts or, as termed in the US, the 'so-called Donetsk People's Republic and Luhansk People's Republic'.

In addition to ensuring that business financed by a financial institution complies 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.

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*,[47] 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

47 [2019] EWHC 1877 (Comm).

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.[48] 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,[49] 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*,[50] 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

48 [2020] EWCA Civ 821.

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

50 [2018] EWHC 2643 (Comm).

force' in the argument that the EU Blocking Regulation[51] 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.

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

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

a non-US financial institution or regulated entity with no apparent US nexus.[52] 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. 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 due consideration should be given to the factors described above and in the context of any other transaction or party-specific risks.

52 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.

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 also the 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, the 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 sits on the board of trustees of Transparency International UK and also established the Transparency International Professional Supporters Network, a volunteer initiative of professionals, academics and students aimed at supporting Transparency International's advocacy and outreach efforts.

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 than ever, it seems. More states are using them, in more creative (and often unilateral) ways. They've become many states' first line of response.

This, alas, creates a degree of complication for everyone else. Hitherto no book has addressed those issues and the proliferation of sanctions regimes and investigations in a structured way. GIR's *The Guide to Sanctions* solves 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, and is an invaluable resource.

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

ISBN 978-1-83862-874-1