GIR Global Investigations Review

The Practitioner's Guide to Global Investigations

Volume I: Global Investigations in the United Kingdom and the United States

EIGHTH EDITION

Editors
Judith Seddon, Eleanor Davison, Christopher J Morvillo, Luke Tolaini, Celeste Koeleveld, F Joseph Warin, Winston Y Chan

2024

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

www.globalinvestigationsreview.com

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 978-1-80449-273-4

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

Acknowledgements

Addleshaw Goddard LLP

Akrivis Law Group, PLLC

Anagnostopoulos

Baker McKenzie

BCL Solicitors LLP

BDO USA, LLP

Bennett Jones LLP

Campos Mellos Advogados (in association with DLA Piper)

Clifford Chance

Cloth Fair Chambers

Cooley LLP

Cravath, Swaine & Moore LLP

Davis Polk & Wardwell LLP

Debevoise & Plimpton LLP

Dechert LLP

Díaz Reus Abogados

DLA Piper

Eversheds Sutherland

Fornari e Associati

Fountain Court Chambers

Fox Williams LLP

Gibson, Dunn & Crutcher LLP

Goodwin

Herbert Smith Freehills LLP

Homburger

Jones Day

Kingsley Napley LLP

Kirkland & Ellis International LLP

Latham & Watkins

Law Offices of Panag and Babu

Linklaters LLP

McDermott Will & Emery UK LLP

Marval O'Farrell Mairal

Matheson

Meredith Connell

Moroğlu Arseven

Morvillo Abramowitz Grand Iason & Anello PC

Navacelle

Noerr Partnerschaftsgesellschaft mbB

Paul Hastings LLP

Rebaza, Alcázar & De Las Casas

Shearman & Sterling LLP

Skadden, Arps, Slate, Meagher & Flom (UK) LLP

Sullivan & Cromwell LLP

Travers Smith LLP

Uría Menéndez Abogados, SLP

Walden Macht & Haran LLP

Willkie Farr & Gallagher LLP

Withersworldwide

Publisher's Note

The Practitioner's Guide to Global Investigations is published by Global Investigations Review (www.globalinvestigationsreview.com) – a news and analysis service for lawyers and related professionals who specialise in cross-border white-collar crime investigations.

The Guide was suggested by the editors to fill a gap in the literature – namely, how does one conduct (or conduct oneself) in such an investigation, and what should one have in mind at various times?

It is published annually as a two-volume work and is also available online and in PDF format.

The volumes

This Guide is in two volumes. Volume I takes the reader through the issues and risks faced at every stage in the life cycle of a serious corporate investigation, from the discovery of a potential problem through its exploration (either by the company itself, a law firm or government officials) all the way to final resolution – be that in a regulatory proceeding, a criminal hearing, civil litigation, an employment tribunal, a trial in the court of public opinion or, just occasionally, inside the company's own four walls. As such, it uses the position in the two most active jurisdictions for investigations of corporate misfeasance – the United States and the United Kingdom – to illustrate the practices and thought processes of cutting-edge practitioners, on the basis that others can learn much from their approach, and there is a read-across to the position elsewhere.

Volume II takes a granular look at law, regulation, enforcement and best practice in the jurisdictions around the world with the most active corporate investigations spaces, highlighting, among other things, where they vary from the norm.

Online

The Guide is available at www.globalinvestigationsreview.com. Containing the most up-to-date versions of the chapters in Volume I, the website also allows visitors to quickly compare answers to questions in Volume II across all the jurisdictions covered.

The publisher would like to thank the editors for their exceptional energy, vision and intellectual rigour in devising and maintaining this work. Together we welcome any comments or suggestions from readers on how to improve it. Please write to us at:
insight@globalinvestigationsreview.com.

30

Sanctions: The US Perspective

David Mortlock, Britt Mosman, Nikki Cronin and Ahmad El-Gamal[1]

30.1 Overview of the US sanctions regime

The United States imposes economic and trade sanctions on individuals, entities and jurisdictions based on US foreign policy and national security goals. These measures are administered and enforced primarily by the US Department of the Treasury's Office of Foreign Assets Control (OFAC), through a combination of statutes, regulations, executive orders and interpretive guidance.

OFAC's regulations are strict liability, meaning that OFAC need not prove fault or intent to enter an enforcement action and issue a civil penalty. Additionally, if a party wilfully violates US sanctions laws, the Department of Justice (DOJ) and the US Attorney may pursue criminal investigations and enforcement actions. Other regulators, such as the Financial Crimes Enforcement Network and the New York Department of Financial Services, may also play a role in enforcing US sanctions regulations, imposing additional penalties for failures to maintain specific controls to help ensure compliance with OFAC-administered regulations. Both federal and state regulators may pursue enforcement actions for the same conduct simultaneously, potentially leading to multiple related investigations by several entities.

The United States maintains comprehensive sanctions programmes, also called embargoes, generally prohibiting activity involving Cuba, Iran, North Korea, Syria, the Crimea region of Ukraine, the Donetsk People's Republic of Ukraine (DNR) and the Luhansk People's Republic of Ukraine (LNR). In addition to comprehensive sanctions, OFAC implements targeted sanctions on specific individuals and entities (persons) under one or more of its sanctions

1 David Mortlock and Britt Mosman are partners and Nikki Cronin and Ahmad El-Gamal are associates at Willkie Farr & Gallagher LLP.

programmes targeting various activities, such as narcotics trafficking, terrorism, proliferation activities involving nuclear or other weapons of mass destruction, or human rights violations. Both direct and indirect activities involving governments or persons that are the subject of targeted sanctions can give rise to violations of US sanctions laws.

Statutes and official guidance 30.1.1

The United States maintains several sanctions regimes, each with its own restrictions and regulations. In addition to the country-specific sanctions programmes, such as the Iranian Transactions and Sanctions Regulations (ITSR), which primarily govern US sanctions on Iran, OFAC can also sanction persons under several targeted sanctions programmes, such as the Foreign Narcotics Kingpin Act or the Global Magnitsky Act.

Pursuant to these sanctions programmes, persons designated by the State or Treasury departments will be added to OFAC's List of Specially Designated Nationals and Blocked Persons (the SDN List). US persons are generally prohibited from engaging in any transactions, directly or indirectly, involving persons on OFAC's SDN List, as well as any entity of which 50 per cent or more is owned by one or more persons on the SDN List, unless authorised by OFAC or exempt.[2] In addition, the sanctions programmes administered by OFAC generally prohibit US persons from 'facilitating' actions of non-US persons, which, although completely legal for a non-US person, could not be directly performed by US persons owing to sanctions restrictions.

OFAC also imposes certain more narrowly targeted sanctions on particular regions or persons; for example, certain sectors of Russia's economy are on OFAC's Sectoral Sanctions Identifications List (the SSI List). Listed persons operating in identified sectors of the Russian economy, such as financial services, energy and defence, will be added to the SSI List under one of the Directives implemented pursuant to Executive Order 13662.[3] Each Directive places specific prohibitions, requirements and restrictions on transactions by US persons with those listed persons.

Additionally, OFAC has imposed a 'new investment prohibition' that bars US persons from the commitment of capital or other assets for the purpose of generating returns or appreciation in Russia.[4] As another example, OFAC has placed investment restrictions on certain Chinese companies identified as Chinese Military-Industrial Complex Companies (CMICs), prohibiting US persons from purchasing publicly traded securities – or any securities that are

2 For example, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) 50 Percent Rule does not apply to the prohibitions in Directive 4 under Executive Order 14024 targeting the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation and the Ministry of Finance of the Russian Federation. OFAC FAQ No. 1001 (https://ofac.treasury.gov/faqs/search/1001).

3 Exec. Order No. 13662, 79 Fed. Reg. 16169-71 (24 Mar. 2014).

4 Exec. Order No. 14024, 86 Fed. Reg. 20249-52 (15 Apr. 2021).

derivative of, or are designed to provide investment exposure to, such securities – of any entity on the non-SDN CMIC List.[5]

OFAC maintains an updated list of US sanctions programmes and country information on its website[6] and a list of compiled frequently asked questions that provide a wide range of details and guidance on topics, including OFAC's interpretation of newly issued sanctions regulations, enforcement practices specific to certain sanctions programmes and the implementation of authorisations provided in general licences.[7] OFAC also regularly releases separate guidance documents that advise companies of specific risk factors for certain industries and suggest best practices for designing appropriate sanctions compliance programmes.

OFAC's enforcement authority and procedures are set forth in its Economic Sanctions and Enforcement Guidelines at 31 CFR Part 501 Appendix A. The Guidelines establish, among other things, the potential outcomes of an investigation or enforcement action and the method and relevant factors for calculating the base penalty amount of an apparent sanctions violation.

30.1.2 Persons to whom sanctions apply

US sanctions generally restrict activities within the jurisdiction of the United States and by US persons, generally defined as any US citizen, permanent resident alien, entity organised under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States.[8] For Iran and Cuba, the prohibitions also extend to any entity owned or controlled by a US person.

The US government may also impose sanctions against non-US persons for certain activity, even with no nexus to the United States. 'Secondary sanctions' authorise OFAC or the State Department to impose sanctions against non-US persons for certain specified activity with Iran, Russia, North Korea and Syria. These are intended to discourage non-US persons from engaging in the specified activity and can result in sanctions against the foreign company itself; for example, when the United States reimposed secondary sanctions for certain activity involving specified sectors of the Iranian economy following the US withdrawal from the Joint Comprehensive Plan of Action (JCPOA), non-US persons became exposed to secondary sanctions for engaging in

5 These sanctions were initially imposed by the Trump administration pursuant to Executive Order 13959 (85 Fed. Reg. 73185, 12 Nov. 2020) and were subsequently amended by the Biden administration pursuant to Executive Order 14032 (86 Fed. Reg. 30145, 7 June 2021).

6 OFAC, 'Sanctions Programs and Country Information' (https://ofac.treasury.gov/sanctions-programs-and-country-information).

7 See OFAC FAQs (https://ofac.treasury.gov/faqs).

8 Id., No. 11 (https://ofac.treasury.gov/faqs/11).

certain significant activity involving Iran's automotive, shipping, shipbuilding or energy sectors, or involving Iranian SDNs.[9]

Licensing 30.1.3

OFAC may issue a general licence or a specific licence to authorise certain activity that would otherwise be prohibited by sanctions.

A general licence is available to any person engaging in activity that fits the criteria set forth in the licence. Each general licence relates to a particular sanctions programme and generally offers broad authorisations covering certain categories of transactions; for example, a general licence is typically available to authorise the export of food, medicine and medical devices to countries that are the subject of a comprehensive embargo.

In addition to the general licence for the export of food, medicine and medical devices, most sanctions programmes also include general licences permitting certain transactions with respect to official business of the US federal government or international organisations such as the United Nations, certain transactions regarding the transmission of telecommunications and the services for personal communications, and the provision of legal services in respect of requirements and compliance with US law (among other things).

It is important to analyse carefully the general licence specific to each country programme as the requirements and restrictions may vary from programme to programme; for example, the general licence for the export of agricultural commodities, medicine and medical devices to Iran, set forth in the ITSR, includes authorisations only for certain 'covered persons' and excludes the export of some specified goods.[10]

Furthermore, some sanctions programmes contain general licences authorising the export of certain goods or services that are highly tailored to a specific country and its respective sanctions programme and that do not appear in any form in other country sanctions programmes; for example, Cuba, Venezuela and Russia have highly individualised sets of general licences that change frequently and are specific to the unique sanctions programme for each country.

Specific licences are granted case by case under certain limited situations and conditions. Requests for specific licences may be submitted directly to

9 OFAC will consider the totality of the circumstances when determining whether a transaction is significant, using seven factors: (1) the size, number and frequency of the transaction(s); (2) the nature of the transaction(s); (3) the level of awareness of management and whether the transaction(s) are part of a pattern of conduct; (4) the nexus between the transaction(s) and a blocked person; (5) the impact of the transaction(s) on statutory objectives; (6) whether the transaction(s) involve deceptive practices; and (7) such other factors that the Secretary of the Treasury deems relevant case by case. OFAC FAQ No. 545 (https://ofac.treasury.gov/faqs/search/545).

10 31 CFR §§ 560.530 (3)(ii), 560.530 (4).

OFAC. These licences will typically be granted only if the activity is in the interests of US foreign policy.

30.1.4 Key jurisdictions

The United States maintains comprehensive sanctions on Cuba, Iran, North Korea, Syria, the Crimea Region of Ukraine, the DNR and the LNR. Additionally, OFAC imposes significant sanctions on Russian persons and the government of Venezuela.

30.1.4.1 Cuba

The comprehensive sanctions on Cuba, governed by the Cuban Assets Control Regulations (CACR),[11] generally prohibit any transaction by a person subject to US jurisdiction, including foreign entities owned or controlled by a US person, in which Cuba or a Cuban national has an interest. This includes the export of goods and services, such as financial services, to Cuba and the import of Cuban goods into the United States. US persons are also prohibited from approving, financing, facilitating or guaranteeing any transaction by a foreign person in which they would be prohibited from engaging themselves.

The CACR contains several general licences authorising activities supporting the Cuban people and private enterprise in Cuba.[12] Additionally, the CACR currently contains general licences regarding travel-related transactions for a variety of specified activities. All general licences should be checked frequently to confirm that relevant authorisations are still in effect and that additional restrictions or requirements have not been put in place, limiting the scope of the general licences.

30.1.4.2 Iran

OFAC's sanctions programme on Iran is primarily governed by the ITSR,[13] which generally prohibit the export, re-export, sale or supply, directly or indirectly, from the United States or by a US person, wherever located, of any goods, technology or services to Iran and US person facilitation of those prohibited transactions. The prohibitions in the ITSR also apply to foreign entities owned or controlled by a US person.

OFAC reimposed significant secondary sanctions that threaten sanctions on non-US persons for certain transactions involving Iranian SDNs and for specified activities in key sectors of the Iranian economy following the United

11 31 CFR Part 515.

12 31 CFR §§ 515.502 to 515.591.

13 31 CFR Part 560.

States' withdrawal from the JCPOA on 8 May 2018.[14] With the issuance of Executive Order 13902 in January 2020, even more sectors of the Iranian economy became the subject of secondary sanctions, meaning that most trade with Iran now potentially carries secondary sanctions exposure.[15]

North Korea 30.1.4.3

The North Korean Sanctions Regulations[16] generally prohibit the export, re-export, sale or supply, directly or indirectly, from the United States or by a US person, wherever located, of any goods, technology or services to North Korea and facilitation of those prohibited transactions by US persons.

In addition to the primary sanctions detailed above, a number of North Korea-related executive orders authorise the imposition of secondary sanctions on persons determined to be engaging in certain specified commercial activities involving North Korea.[17]

Syria 30.1.4.4

The Syrian Sanctions Regulations[18] generally prohibit the export, re-export, sale or supply, directly or indirectly, from the United States or by a US person, wherever located, of any services to Syria and US person facilitation of those prohibited transactions.

Additionally, Section 7412 of the National Defense Authorization Act for Fiscal Year 2020 (also titled the Caesar Syria Civilian Protection Act of 2019[19]) authorises sanctions against any foreign person determined to knowingly provide significant financial, material or technological support to, or knowingly engage in a significant transaction with, certain persons in Syria, primarily

14 Exec. Orders 13902 (85 Fed. Reg. 2003, 10 January 2020) and 13871 (84 Fed. Reg. 20761, 10 May 2019) authorise the imposition of secondary sanctions on specified transactions involving Iran's iron, steel, aluminium copper, construction, mining, manufacturing and textile sectors.

15 See Exec. Order No. 13902, 85 Fed. Reg. 2003 (10 Jan. 2020).

16 31 CFR Part 510.

17 Exec. Order No. 13810, 82 Fed. Reg. 44705 (20 Sept. 2017).

18 31 CFR Part 542.

19 The Assad Regime Anti-Normalization Act of 2023 (www.foreign.senate.gov/imo/media/doc/09-26-23_assad_regime_anti-normalization_act_of_2023.pdf), introduced in the Senate at the end of September 2023, would extend the Caesar Act until 2032. The foreign relations committee's press release describes the Act in respect of sanctions as follows:

- *Expands sanctions to entities that divert humanitarian assistance or expropriate property from the Syrian people for luxury or personal gain;*
- *Expands sanctions to the Syrian People's Assembly and senior officials of the Arab Socialist Ba'ath Party in Syria;*
- *Clarifies that sanctions apply to energy transactions; and*
- *Directs the President to determine whether Asma al-Assad's 'charity', the Syria Trust for Development, meets the criteria for sanctions under the Caesar Act.*

relating to the government of Syria, its military or any foreign person that is the subject of sanctions with respect to Syria.[20]

30.1.4.5 Crimea, DNR and LNR

The Ukraine-/Russia-related Sanctions Regulations generally prohibit the export, re-export, sale or supply, directly or indirectly, from the United States or by a US person, wherever located, of any goods, technology or services to Crimea and the facilitation of those prohibited transactions by US persons.[21] Executive Order 14065 similarly prohibits the above-listed activities with respect to the DNR and the LNR.[22]

30.1.4.6 Russia

Russia is the subject of various US sanctions, which have increased in severity and complexity in response to Russia's invasion of Ukraine. A significant number of prominent Russian persons appear on OFAC's SDN List, including key political and military officials, oligarchs, Russian state-owned enterprises and financial institutions.

In addition, pursuant to Executive Order 13662,[23] OFAC issued Directives 1 to 4, imposing sectoral sanctions against entities identified on OFAC's SSI List[24] operating in certain sectors of the Russian economy, such as financial services, energy and defence.[25] After Russia's invasion of Ukraine, OFAC issued four additional Directives pursuant to Executive Order 14024, two of which target entities identified on OFAC's SSI List operating in the financial services sector of the Russian economy, with the remainder targeting the Russian Central Bank, National Wealth Fund and Ministry of Finance.[26]

The sharp increase in sanctions targeting Russia necessitates additional diligence and vigilance from persons operating in Russia, or entering into transactions with or involving Russian persons, to ensure that they are not entering into transactions that would constitute violations of the US sanctions on Russia.

Prior to the publication and implementation of the Russian Harmful Foreign Activities Sanctions in February 2022, the original four Directives imposed pursuant to Executive Order 13662 prohibited US persons from dealing in new debt and equity on behalf of designated Russian entities

---

20 Caesar Civilian Protection Act, § 7412(2) of the National Defense Authorization Act for Fiscal Year 2020.

21 31 CFR Part 589.

22 Exec. Order No. 14065, 87 Fed. Reg. 10293 (23 Feb. 2022).

23 Exec. Order No. 13662, 79 Fed. Reg. 16169-71 (24 Mar. 2014).

24 The Sectoral Sanctions Identifications List is available at https://ofac.treasury.gov/consolidated-sanctions-list-non-sdn-lists/sectoral-sanctions-identifications-ssi-list.

25 Exec. Order No. 13662, 79 Fed. Reg. 16167 (20 March 2014); Exec. Order No. 14024, 86 Fed. Reg. 20249-52 (15 Apr. 2021).

26 Exec. Order No. 14024, 86 Fed. Reg. 20249-52 (15 Apr. 2021).

operating in Russia's financial, energy and defence sectors and from providing support for deep-water and Arctic offshore or shale projects involving listed Russian entities or where a listed Russian entity has an ownership interest of 33 per cent or more. Directive 1 was expanded by Executive Order 14024, published on 15 April 2021, to prohibit US financial institutions from participating in the primary market for rouble or non-rouble denominated funds by, or the lending of rouble or non-rouble denominated funds to, Russia's Central Bank, National Wealth Fund or Ministry of Finance.[27]

The Directives imposed in early 2022 after Russia's invasion of Ukraine further expanded and added to the Directives already in place. Directive 1A, which superseded Directive 1, expanded the prohibition on rouble and non-rouble bonds issued by Russia's Central Bank, National Wealth Fund or Ministry of Finance to secondary market transactions. Directive 2 prohibits US financial institutions from opening or maintaining correspondent accounts or payable through accounts for or on behalf of or processing transactions involving foreign financial institutions subject to Directive 2. Directive 3 is similar to the prior Directives implemented under Executive Order 13662, prohibiting transactions involving new debt with more than 14 days maturity or new equity of entities subject to Directive 3. Finally, Directive 4 prohibits any transactions involving Russia's Central Bank, National Wealth Fund or Ministry of Finance. Several entities that were initially listed on the SSI List and subject to one of the Directives listed above – such as Sberbank, which was initially listed as subject to Directive 2 – were later designated as SDNs by OFAC in response to Russia's continuing aggression.

Companies engaging in transactions with SSI entities should scrutinise payment terms to ensure that they do not violate the requirements of the applicable Directive or enter into a transaction involving a Russian financial institution, entity or individual that has been added to OFAC's SDN List. Companies should also be aware of OFAC's 50 per cent rule, which states that any entities of which 50 per cent or more, in the aggregate, is owned by any sanctioned entity or entities will also be subject to those same sanctions. This is particularly important when conducting due diligence on Russian entities, as several have complex business structures where multiple sanctioned entities hold interests at varying levels of the ownership chain.

In addition to the blocking and sectoral sanctions imposed by OFAC on Russian entities, the United States has imposed prohibitions on the provision and export of certain services to Russia. On 6 April 2022, President Biden signed Executive Order 14071 prohibiting new investment in the Russian Federation by a US person, wherever located.[28] In a novel use of sanctions based on the International Emergency Economic Powers Act, the Executive Order also prohibits the exportation, re-exportation, sale or supply, directly or

27 OFAC FAQ No. 890 (https://ofac.treasury.gov/faqs/search/890); see also Exec. Order No. 14024, 86 Fed. Reg. 20249 (15 Apr. 2021).

28 Exec. Order No. 14071, 86 Fed. Reg. 20999 (6 Apr. 2021).

indirectly, from the United States, or by a US person, of any category of services as may be determined by the Secretary of the Treasury to any person located in the Russian Federation. OFAC has since issued seven determinations pursuant to Executive Order 14071 prohibiting the exportation, re-exportation, sale or supply, directly or indirectly, from the United States, or by a US person, wherever located, of accounting, trust and corporate formation, management consulting services, architecture services, engineering services, and various other services to any person located in the Russian Federation.[29]

The United States, in partnership with other G7 countries, has also implemented a price cap for the provision of certain services (covered services)[30] regarding the maritime transport of Russian oil and petroleum products. US persons are prohibited from providing covered services as they relate to the maritime transport of Russian oil and petroleum products unless the oil or petroleum products were purchased at or below the price cap.[31]

The United States also maintains secondary sanctions on Russia. The Countering America's Adversaries Through Sanctions Act (CAATSA) mandates the imposition of sanctions against persons that the President determines have knowingly facilitated a 'significant transaction'[32] for or on behalf of any person subject to sanctions imposed by the United States with respect to the Russian Federation, including for or on behalf of a Russian person or entity on OFAC's SDN List.[33] OFAC has effectively limited this threat of sanctions to transactions with any Russian person on its SDN list.[34]

CAATSA also mandates that the President impose sanctions on persons determined to have knowingly engaged in a significant transaction with a person

---

29 See 'Examples, Determination Pursuant to Section 1(a)(ii) of Executive Order 14071: Prohibitions Related to Certain Accounting, Trust and Corporate Formation, and Management Consulting', 5 May 2023 (https://ofac.treasury.gov/media/922956/download?inline); 'Determination Pursuant to Section 1(a)(ii) of Executive Order 14071: Prohibitions Related to Architecture Services and Engineering Services', 19 May 2023 (https://ofac.treasury.gov/media/931776/download?inline).

30 The covered services are trading or commodities brokering, financing, shipping, insurance, flagging and customs brokering. Medical evacuation, health, travel and liability insurance for crew members, classification, inspection, bunkering and pilotage are specifically excluded.

31 'Determination Pursuant to Sections 1(a)(ii), 1(b), and 5 of Executive Order 14071: Price Cap on Petroleum Products of Russian Federation Origin', effective 5 February 2023 (https://ofac.treasury.gov/media/931026/download?inline) ('the price cap on Discount to Crude petroleum products of Russian Federation origin shall be $45 per barrel, and the price cap on Premium to Crude petroleum products of Russian Federation origin shall be $100 per barrel'). See generally 'Price Cap Coalition – Advisory for the Maritime Oil Industry and Related Sectors: Best Practices in Response to Recent Developments in the Maritime Oil Trade', 12 October 2023 (https://ofac.treasury.gov/media/932201/download?inline).

32 See discussion on 'significant transactions', supra note 9.

33 Countering America's Adversaries Through Sanctions Act (CAATSA) § 228.

34 OFAC FAQ No. 541 (https://ofac.treasury.gov/faqs/search/541).

involved in the intelligence or defence sectors of the Russian government. The Department of State published the List Regarding the Defense Sector of the Government of the Russian Federation[35] of persons determined to be part of, or operating for or on behalf of, Russian defence or intelligence sectors.[36]

Finally, CAATSA also mandates that the President impose sanctions on persons determined to have made significant investments above a specified threshold that directly and significantly contribute to Russia's ability to construct energy export pipeline projects initiated on or before 2 August 2017, or that provide significant goods, services, technology, information or support to directly and significantly facilitate the maintenance or expansion of the construction, modernisation or repair of energy export pipelines.[37]

Venezuela 30.1.4.7

Executive Order 13884 blocks all property and interests in property of the government of Venezuela.[38] This means that US persons are generally prohibited from engaging in any transaction in which the government of Venezuela has an interest, including with entities of which 50 per cent or more is owned by the government of Venezuela.

Additionally, Executive Order 13850 blocks the property of additional persons who may be contributing to the situation in Venezuela, including those operating in specified sectors of the Venezuelan economy as determined by the Secretary of the Treasury.[39] Notably, OFAC designated the Venezuelan state oil company, Petróleos de Venezuela SA, pursuant to this authority on 28 January 2019.

OFAC has published several general licences authorising certain activities by US persons that would otherwise be prohibited by the Venezuela-related sanctions programme. A majority of these general licences change frequently and are very specific in respect of the actions they authorise and to whom they apply. As such, companies should ensure they scrutinise and carefully monitor any general licence relied on to conduct business otherwise prohibited by the Venezuela-related Executive Orders.

Offences and penalties 30.2

Generally, US primary sanctions prohibit transactions only by US persons or transactions subject to US jurisdiction. For Cuba and Iran, the restrictions also apply to foreign entities that are owned or controlled by a US person. 'Owned

See Chapter 26 on fines, disgorgement, etc.

35 CAATSA § 231(e), Defense and Intelligence Sectors of the Government of the Russian Federation (www.state.gov/caatsa-section-231d-defense-and-intelligence-sectors-of-the-government-of-the-russian-federation).

36 CAATSA § 231.

37 CAATSA § 232.

38 Exec. Order No. 13884, 84 Fed. Reg. 38843 (6 Aug. 2019).

39 Exec. Order No. 13850, 83 Fed. Reg. 55243 (2 Nov. 2018).

or controlled' is understood to encompass holding at least 50 per cent of the equity interest by vote or value, holding a majority of seats on the board of directors or otherwise controlling actions, policies and personnel decisions of the foreign entity.[40]

Although non-US companies are generally not themselves required to comply with OFAC regulations, they can still face potential liability for exporting goods or services from the United States to a target of US sanctions or for 'causing a violation' by involving a US person in a transaction that would be prohibited for that US person.[41] The most typical way that such a violation by a non-US person might occur is if a transaction involving a target of US sanctions is denominated in US dollars because most US dollar transactions clear through US banks and, therefore, involve the services of a US financial institution.[42]

Under secondary sanctions, access by a non-US company to US markets or the US financial system may be restricted, including by being added to the SDN List, if it engages in certain conduct relating to Iran, Russia or North Korea.

30.3 Commencement of sanctions investigations

The US government can learn of a potential sanctions violation in several ways, including through voluntary self-disclosure (VSD), a report of a blocked or rejected transaction, referral from another government agency and even publicly available information, such as a media report.

If a company learns of a potential violation, it may submit a VSD to OFAC. This has many benefits, including a significant reduction in the base penalty for a potential enforcement action; however, parties should carefully consider whether to file based on the circumstances of, and facts surrounding, the potential violation and their history of engagement with OFAC.

In addition to VSDs, the US government often learns of potential violations through blocked or rejected transaction reports filed by US persons, typically financial institutions, based on suspected sanctions violations. Since June 2019, all US persons must submit reports to OFAC within 10 business

40 31 CFR §§ 515.329, 560.215. For example, in 2019, OFAC entered enforcement proceedings against General Electric regarding apparent violations by three of its non-US subsidiaries for accepting payments from a party owned by the Cuban government and on OFAC's List of Specially Designated Nationals and Blocked Persons. See OFAC, 'Enforcement Information for October 1, 2019' re: The General Electric Company (https://ofac.treasury.gov/media/26481/download?inline).

41 50 USC § 1705.

42 One example can be found in OFAC's enforcement action against Bank of China (UK) Limited (BOC UK), a financial institution located in the United Kingdom. In 2021, BOC UK agreed to remit US$2,329,991 to settle its potential civil liability for apparent violations of the non-repealed Sudan sanctions programme. According to OFAC, the transactions were conducted in US dollars, meaning that BOC UK processed 111 payments via US correspondent banks in apparent violation of the Sudanese Sanctions Regulations.

days of blocking or rejecting a transaction.[43] Previously, all parties had to report transactions involving blocked property to OFAC, but only US financial institutions were obliged to report rejected transactions.[44]

OFAC may also learn of sanctions violations through anti-money laundering reports, primarily suspicious activity reports or criminal investigations conducted by the DOJ or other federal and state law enforcement agencies.

On learning of a potential violation, OFAC may send an initial request for information to the parties with an administrative subpoena or, depending on the nature of the violation, send an informal set of questions to the involved parties, including non-US persons.

Enforcement 30.4

Factors to consider 30.4.1

The test in the United States for civil enforcement of sanctions is one of strict liability. This means that companies can be liable for sanctions violations without proof of knowledge, fault or intent, highlighting the importance of sanctions compliance programmes. Parties should also determine whether there was a wilful violation of US sanctions laws that could lead to a criminal investigation or enforcement action. Parties should balance the need to move quickly after identifying a potential violation with taking the time to understand the nature of the violation to determine whether a VSD is appropriate and to whom the parties should report.

Additionally, OFAC has increasingly worked with other government agencies to bring joint enforcement actions for sanctions violations and attempted evasion of sanctions, and an enforcement action by OFAC can attract the attention of other regulators and law enforcement authorities. This includes the parallel enforcement actions by OFAC and the Financial Crimes Enforcement Network against Bittrex, Inc, a virtual currency exchange based in the United States, settling violations of both the Bank Secrecy Act and various sanctions programmes administered by OFAC.[45] Another example is the ongoing Halkbank matter in which the US Supreme Court heard

43 See 31 CFR § 501.603.

44 An example of OFAC learning of a potential violation through a blocked transaction report can be found in the enforcement action against Hotelbeds USA. OFAC was notified of the apparent violations through a blocked payment report filed by a US financial institution regarding a Cuba travel-related transaction. See OFAC, 'Enforcement Information for June 13, 2019' (https://ofac.treasury.gov/media/16326/download?inline).

45 See United States of America Financial Crimes Enforcement Network Department of the Treasury, Consent Order Imposing Money Penalty, In The Matter Of: Bittrex, Inc., Number 2022-03 (https://www.fincen.gov/sites/default/files/enforcement_action/2023-04-04/Bittrex_Consent_Order_10.11.2022.pdf); see OFAC, Enforcement Release: October 11, 2022: 'OFAC Settles with Bittrex, Inc. for $24,280,829.20 Related to Apparent Violations of Multiple Sanctions Programs' (https://ofac.treasury.gov/media/928746/download?inline).

Halkbank's appeal of the DOJ enforcement action against it. The DOJ case was built on OFAC's civil enforcement action against Halkbank for apparent violations of the Iranian Transactions and Sanctions Regulations. The case was argued before the Supreme Court on 17 January 2023 and the Supreme Court's opinion was published on 19 April 2023.[46]

30.4.2 Compliance framework

In May 2019, OFAC issued 'A Framework for OFAC Compliance Commitments'.[47] This guidance document encourages a risk-based approach, noting that no single compliance programme is suitable for every institution; however, the document provides five components that OFAC highlights as essential to any effective compliance programme:

- management commitment;
- risk assessment;
- internal controls;
- testing and auditing; and
- training.

Since publishing the Framework, OFAC has highlighted the importance of an effective risk-based compliance programme and has reserved the final paragraph of published enforcement actions to discuss how the facts relate to the Framework and how both the party subject to the enforcement action and other businesses in its industry can mitigate risks by implementing compliance policies and procedures proportional to the risks faced by the party and the industry as a whole.[48] OFAC has indicated that the strength of a party's

46 The Supreme Court's opinion affirmed the Second Circuit Court of Appeal's ruling that the Foreign Sovereign Immunities Act did not cover criminal cases, but remanded the case back to the Second Circuit as it was determined that the Second Circuit did not fully consider various common law immunity arguments that were raised by the parties. See *Turkiye Halk Bankasi A.S. v. United States of America*, 598 U.S. ____ (2023), Docket of the Supreme Court for No. 21-1450 (www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/21a373.html); see also Anna Bianca Roach, 'Supreme Court to hear Halkbank sanctions case', Global Investigations Review (3 Oct. 2022) (https://globalinvestigationsreview.com/just-sanctions/article/supreme-court-hear-halkbank-sanctions-case).

47 'A Framework for OFAC Compliance Commitments' (https://ofac.treasury.gov/media/16331/download?inline).

48 See OFAC, 'Enforcement Information for February 26, 2020' re: Société Internationale de Télécommunications Aéronautiques SCRL (https://ofac.treasury.gov/media/33096/download?inline). ('As noted in OFAC's Framework for Compliance Commitments issued in May 2019, companies can mitigate sanctions risks by conducting risk assessments and exercising caution when engaging in business transactions with entities that are affiliated with, or known to transact with, OFAC-sanctioned persons or jurisdictions, or otherwise pose high risks due to their joint ventures, affiliates, subsidiaries, customers, suppliers, geographic location, or the products and services they offer.').

compliance programme can also be a significant mitigating or aggravating factor that it will consider when calculating a penalty amount.[49]

To further mitigate sanctions risks, parties should also ensure that their compliance programme meets the criteria presented in the DOJ's 'Evaluation of Corporate Compliance Programs'.[50] The DOJ will evaluate a party's compliance programme when determining whether to impose a monitor on the party once an enforcement action regarding an apparent violation of US sanctions laws is concluded.

Best practices 30.4.3

Once an investigation has commenced, parties should proactively collaborate and cooperate with the agency conducting the investigation. OFAC enforcement actions and enforcement guidelines highlight cooperation as a mitigating factor to be taken into account in an enforcement action.[51] Furthermore, if the DOJ is conducting an investigation into a wilful violation of US sanctions, the party must fully cooperate with the DOJ to receive the benefits associated with submitting a VSD. Generally, full cooperation includes internal investigations to discover the root cause of an apparent violation, responding to regulators' requests for additional information in a timely and complete manner, preserving all sensitive or relevant documents, and collaborating with regulators to develop and implement effective remedial measures.[52]

Once an investigation has commenced, under no circumstances should parties attempt to hide or destroy material information or evidence. Any indication that the parties have attempted to oppose an investigation is likely to lead federal and state investigators into taking a more hostile approach.

---

49 In OFAC's enforcement action against Haverly Systems, Inc for violations of the Ukraine-/Russia-Related Sanctions Regulations, OFAC considered the fact that Haverly did not have 'a formal OFAC sanctions compliance programme at the time the apparent violations occurred' was an aggravating factor. See OFAC, 'Enforcement Information for April 25, 2019' re: Haverly Systems, Inc (https://ofac.treasury.gov/media/16626/download?inline).

50 DOJ, Criminal Division, 'Evaluation of Corporate Compliance Programs' (updated Mar. 2023), available at www.justice.gov/criminal-fraud/page/file/937501/download.

51 For example, in OFAC's enforcement action against Stanley Black & Decker, Inc and its subsidiary, OFAC found that Stanley Black & Decker's cooperation with OFAC, including an extensive internal investigation and meaningful responses to OFAC's requests for additional information, was a mitigating factor when determining the penalty amount. See OFAC, 'Enforcement Information for March 27, 2019' re: Stanley Black & Decker, Inc (https://ofac.treasury.gov/media/9321/download?inline).

52 For guidance on cooperating with OFAC, see 31 CFR 501 Appendix A(III)(G). For guidance on the requirements necessary for credit for full cooperation with a DOJ sanctions-related investigation, see DOJ, National Security Division, 'Enforcement Policy for Business Organizations', pp. 4–6.

30.4.3.1 Self-reporting to OFAC

OFAC generally views VSDs favourably, and a VSD will reduce the base penalty of an apparent violation by up to 50 per cent. To be considered voluntary, a disclosure must be self-initiated and submitted to OFAC before it or any other government agency or official discovers the apparent violation. One exception is that a VSD to another government agency may be considered a VSD to OFAC, case by case.

A VSD to OFAC must include, or be followed by, a report containing sufficient details to provide a complete understanding of the circumstances of the apparent violation. In some instances, it may be beneficial to the party to make a preliminary disclosure to OFAC before knowing all the facts, to be timely and to ensure that disclosure is considered voluntary. Parties should ensure that their VSD and follow-up report contain all the details known at the time they are made and be prepared to respond to any follow-up enquiries.[53]

OFAC's enforcement guidelines list several instances where notices will not be considered a VSD, including licence applications, notifications from a third party of an apparent violation or a substantially similar apparent violation because it blocked or rejected a transaction, or if the disclosure:

- includes false or misleading information or is materially incomplete;
- is not self-initiated;
- is made without the authorisation of senior management; or
- is in response to an administrative subpoena or other enquiry form.[54]

OFAC's policies and requirements with respect to VSDs were further summarised in the Department of Commerce, Department of the Treasury and Department of Justice Tri-Seal Compliance Note: 'Voluntary Self-Disclosure of Potential Violations' (the Tri-Seal Compliance Note).[55] Published on 26 July 2023, the Tri-Seal Compliance Note provides guidance to businesses on recent updates to compliance and VSD requirements while also underscoring the enhanced level of cooperation and coordination among the bodies responsible for enforcing US sanctions and export control laws.

30.4.3.2 Self-reporting to the DOJ

The DOJ's VSD policy, published on 13 December 2019 and most recently updated on 1 March 2023, states that all business organisations, including financial institutions, are eligible for all the benefits detailed by the policy.[56]

---

53 31 CFR 501 Appendix A(I)(I).

54 Id.

55 'Voluntary Self-Disclosure of Potential Violations', Dept. Commerce, Treasury, Justice (26 July 2023) (The Tri-Seal Compliance Note) (https://ofac.treasury.gov/media/932036/download?inline).

56 See DOJ, National Security Division, 'NSD Enforcement Policy for Business Organizations' (1 Mar. 2023) (www.justice.gov/file/1570996/download).

Similar to other DOJ self-disclosure policies, companies are eligible for the benefits of the updated VSD policy when they:

- voluntarily self-disclose export control or sanctions violations to the National Security Division's Counterintelligence and Export Control Section (CES);
- fully cooperate with the investigation; and
- remediate any violations appropriately and in a timely manner.

The threshold for eligibility is self-disclosure of potential violations to the CES. Unlike with OFAC, self-disclosing to any other regulatory agency is not considered an eligible VSD to the DOJ under its new policy.[57]

For a party's disclosure to be considered voluntary, it must be made before there is an imminent threat of disclosure or government investigation, and reasonably promptly after discovery of the offence. Further, the party must disclose all relevant facts known to it at the time of the disclosure.[58]

See Chapter 4 on self-reporting to authorities

To receive credit for full cooperation, parties are required to:

- disclose all relevant facts in a timely manner;
- cooperate proactively with the DOJ;
- preserve, collect and disclose all relevant documents and information;
- deconflict witness interviews when required; and
- make officers and employees of the party available for interviews by the DOJ when so requested.[59]

Finally, parties are required to demonstrate a thorough analysis of the causes of underlying conduct and, where appropriate:

- engage in remediation;
- implement an effective compliance programme;
- discipline employees identified by the party as responsible for the oversight;

57 Id. at p. 4.

58 Id.

59 Id. at pp. 4–5; see also DOJ, memorandum from Deputy Attorney General Lisa Monaco, 'Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group' (15 Sept. 2022) (www.justice.gov/opa/speech/file/1535301/download). (The document discusses and provides guidance on corporate accountability and what constitutes cooperation during an investigation and VSDs. In the document, Deputy Attorney General Monaco highlights the need for timely and full disclosure for a corporation to get credit for a VSD, provides additional guidance on how DOJ prosecutors should provide credit for cooperation and describes how an effective compliance policy can have a significant impact on the terms of the resolution of a DOJ investigation. Deputy Attorney General Monaco noted that corporations that find ways to navigate issues of foreign law, such as privacy laws, blocking statutes or other restrictions, to provide a full disclosure should be rewarded with credit for cooperation. Conversely, if a corporation uses those foreign laws to shield misconduct, the DOJ may make an adverse inference as to the corporation's cooperation.)

- retain business records and prohibit the improper destruction of those records; and
- take any additional steps that demonstrate recognition of the seriousness of a party's misconduct.[60]

Of note, and highlighted by the Tri-Seal Compliance Notice, the DOJ has announced that it will generally not seek guilty pleas regarding prompt and complete disclosures that meet the DOJ's VSD criteria, described above.[61] Furthermore, the Tri-Seal Compliance Notice also highlighted the fact that the DOJ now examines whether a company has enacted disciplinary measures against employees who participated in, or had oversight over, the conduct that is the subject of the VSD, including compensation clawbacks.[62]

Considerations

Submitting a VSD to OFAC can have several benefits, the most significant of which is that it is considered a mitigating factor in the calculation of a potential penalty amount. In some cases, a VSD can allow a party to avoid an enforcement action altogether if OFAC determines the conduct does not constitute a violation or that it does not warrant a civil monetary penalty; however, there are general costs associated with making a VSD to either OFAC or the DOJ, including legal expenses, government investigation, additional scrutiny, reputational harm and, in some cases, large monetary penalties. There is also the potential for a government investigation to reveal unknown or undisclosed violations.

When submitting a VSD to OFAC, in particular, parties should carefully consider the possibility that the conduct was wilful and that, as a result, OFAC may refer the case to the DOJ for criminal enforcement.

If a party submits a VSD to the DOJ that satisfies the requirements of its updated VSD policy, there is a presumption that the party will receive a non-prosecution agreement and pay no fine, in the absence of aggravating factors;[63] however, even if a party receives a non-prosecution agreement, at a minimum it will not be permitted to retain any of the unlawfully obtained gain and will be required to pay all disgorgement, forfeiture or restitution resulting from the misconduct.[64]

Even if there are aggravating circumstances, the DOJ will still recommend a fine of at least 50 per cent less for a qualifying party than would have been levied in the absence of a VSD and will not require the imposition of a monitor if the party has implemented an effective compliance programme at the time of

60 Id. at pp. 6–7.

61 The Tri-Seal Compliance Note, op. cit. note 55, at p. 2.

62 Id. at p. 3.

63 Id. at pp. 2–3.

64 Id.

resolution.[65] By filing with the DOJ, a party may invite a criminal investigation in addition to heavy, continuing disclosure obligations.

See Chapter 4 on self-reporting to authorities

Overall, effective use of OFAC and the DOJ's VSD programmes rests in the strength of a party's compliance programme, policy and procedures. Even if the policy and procedures fail to prevent an apparent violation, they can help parties quickly and more accurately determine the nature of the violation and whether a VSD to OFAC or the DOJ is necessary and beneficial.

Other government authorities

In addition to OFAC and the DOJ, parties should also consider notifying potential violations to relevant US and non-US regulators, shareholders, counterparties, insurers and other interested parties. Parties should also be aware that OFAC maintains memoranda of understanding with several state and federal banking regulatory agencies, which may impose penalties on financial institutions in connection with apparent violations of US sanctions laws.[66] As such, financial institutions should consider notifying their regulators of potential violations.

Parties should also determine whether the potential violation of US sanctions laws also violates sanctions laws in foreign jurisdictions and whether it would be appropriate to make disclosures to the relevant regulatory bodies. Finally, parties should also be aware that sanctions programmes are often accompanied by export control restrictions implemented and enforced by the Department of Commerce and the State Department.[67]

All these considerations should be made while conscious of the requirements for VSD submissions to OFAC and the DOJ, namely when a VSD is no longer considered eligible for the benefits.

Settlement 30.4.3.3

OFAC enforcement actions often end in settlement. Settlement discussions may be initiated by either OFAC or the party committing the apparent violation at several points during the enforcement process. These settlements can also include multiple violations or be a part of a comprehensive settlement

65 Id.

66 The Department of the Treasury maintains a list of memoranda of understanding between OFAC and state and federal banking regulators (https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information/2019-enforcement-information/memoranda-of-understanding-between-ofac-and-bank-regulators).

67 For example, the Department of Commerce imposed additional export control restrictions on both Russia and Belarus in coordination with the sanctions imposed by OFAC. See US Department of Commerce, Bureau of Industry and Security, 'Resources on Export Controls Implemented in Response to Russia's Invasion of Ukraine' (updated 6 Oct. 2023) (www.bis.doc.gov/index.php/policy-guidance/country-guidance/russia-belarus).

with other federal, state or local agencies that are also pursuing investigations or enforcement actions in respect of the apparent violation.[68]

30.5 Trends and key issues

30.5.1 Recent enforcement activity

Since the release of 'A Framework for Compliance Commitments' in May 2019, OFAC has been able to map compliance programmes against the Framework to determine whether a party's compliance programme should be considered an aggravating or mitigating factor; for example, in an enforcement action against Eagle Shipping International, OFAC stated that:

> *[a]s noted in OFAC's Framework for Compliance Commitments, this case demonstrates the importance for companies operating in high-risk industries (e.g., international shipping and trading) to implement risk-based compliance measures, especially when engaging in transactions involving exposure to jurisdictions or persons implicated by U.S. sanctions.*[69]

Recent enforcement activity has also shown that OFAC is willing to use a minimal or indirect nexus to the United States to proceed with an enforcement action against a non-US party.[70] OFAC has also showed its willingness to expand its extraterritorial jurisdiction to penalise non-US companies for transactions that would not have been covered by OFAC's jurisdiction if not for the

See Chapter 28 on extraterritoriality

68 One example of this is UniCredit Bank AG agreeing to pay approximately US$611 million to OFAC as part of a US$1.3 billion settlement with federal and state government partners. See, e.g., US Department of the Treasury, press release, 'U.S. Treasury Department Announces Settlement with UniCredit Group Banks' (15 Apr. 2019) (https://home.treasury.gov/news/press-releases/sm658).

69 See OFAC, 'Enforcement Information for January 27, 2020' re: Eagle Shipping International (USA) LLC (https://ofac.treasury.gov/media/33086/download?inline).

70 For example, in its enforcement action against British Arab Commercial Bank (BACB), OFAC considered even tenuous and indirect contact with US financial institutions as grounds for an enforcement action. OFAC found that BACB had violated Sudanese sanctions despite the fact that the transactions at issue were not processed to or through the US financial system. BACB operated a nostro account in a country that imports Sudanese-origin oil for the stated purpose of facilitating payments involving Sudan. The bank funded the nostro account with large, periodic US dollar wire transfers from banks in Europe, which in turn transacted with US financial institutions in a manner that violated OFAC sanctions. See OFAC, 'Enforcement Information for September 17, 2019' re: British Arab Commercial Bank plc (www.moneylaundering.com/wp-content/uploads/2019/09/OFAC.SettlementAgreement.091719.pdf).

use of servers located in the United States.[71] In late 2020, OFAC published its first enforcement actions targeting apparent violations of US sanctions laws in the cryptocurrency industry.[72]

Potential pitfalls 30.5.2

Companies should be wary of OFAC's continued use of increasingly indirect and tenuous links to the US financial system to bring enforcement actions against foreign parties for 'causing a violation' by US banks. As such, non-US companies should scrutinise the structure of transactions with persons or countries subject to US sanctions to ensure that there are no potential direct or indirect links to the US financial system, including transactions that use US dollars. Additionally, given the emphasis OFAC places on it, companies should ensure that their compliance programmes are in line with 'A Framework for Compliance Commitments'.

71 For example, regarding the enforcement action against Société Internationale de Télécommunications Aéronautiques SCRL (SITA), OFAC's basis for jurisdiction over SITA, a global information technology services provider headquartered in Switzerland and serving commercial air transportation, was that the technology provided to sanctioned parties was hosted on, and incorporated functions that routed messages through, US servers and contained US-origin software. See OFAC, 'Enforcement Information for February 26, 2020', op. cit. note 48.

72 For example, regarding the enforcement action against BitGo, Inc, OFAC signalled its intent to enforce sanctions compliance in the cryptocurrency industry. The apparent violations involved users located in sanctioned jurisdictions signing up for and accessing BitGo's secure digital wallet management services to engage in digital currency transactions. Despite having access to the IP addresses of its customers, tracked at the time for security purposes in respect of logins, BitGo did not use that information for sanctions compliance purposes. OFAC highlighted the importance of entities involved in providing digital currency services to implement sanctions compliance controls commensurate with their risk profile. The fact that BitGo did not implement 'appropriate, risk-based sanctions compliance controls' and 'had reason to know that . . . users were located in sanctioned jurisdictions based on [their] IP address data' were seen as aggravating factors. See OFAC, Enforcement Release: December 30, 2020, 'OFAC Enters Into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions' (https://ofac.treasury.gov/media/50266/download?inline).