

# The Practitioner's Guide to Global Investigations

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

SEVENTH EDITION

---

**Editors**

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

**2023**

# **The Practitioner's Guide to Global Investigations**

---

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

Reproduced with permission from Law Business Research Ltd  
This article was first published in December 2022  
For further information please contact [insight@globalinvestigationsreview.com](mailto:insight@globalinvestigationsreview.com)

## Contents

Published in the United Kingdom  
by Law Business Research Ltd, London  
Holborn Gate, 330 High Holborn, London, WC1V 7QT  
© 2023 Law Business Research Ltd  
[www.globalinvestigationsreview.com](http://www.globalinvestigationsreview.com)

No photocopying: copyright licences do not apply.

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided was accurate as at November 2022, be advised that this is a developing area.

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

ISBN 978-1-83862-911-3

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

# 30

## Sanctions: The US Perspective

David Mortlock, Britt Mosman, Nikki Cronin and Ahmad El-Gamal<sup>1</sup>

### Overview of the US sanctions regime

30.1

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

---

<sup>1</sup> 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.

### 30.1.1 Statutes and official guidance

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. In addition, the sanctions programmes administered by OFAC also 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 listed in 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.<sup>2</sup> 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.<sup>3</sup> 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 derivative of, or are designed to provide investment exposure to, such securities – of any entity listed on the CMIC List.<sup>4</sup>

---

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

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

4 These sanctions were initially imposed by the Trump Administration pursuant to Executive Order 13959 and were subsequently amended by the Biden Administration pursuant to

OFAC maintains an updated list of US sanctions programmes and country information on its website<sup>5</sup> 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.<sup>6</sup> 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 OFAC's 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.

### Persons to whom sanctions apply

### 30.1.2

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.<sup>7</sup> 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 certain significant activity involving Iran's automotive, shipping, shipbuilding or energy sectors, or involving Iranian SDNs.<sup>8</sup>

---

Executive Order 14032. Exec. Order No. 13959, 85 Fed. Reg. 73185 (12 November 2020); Exec. Order No. 14032, 86 Fed. Reg. 30145 (7 June 2021).

5 US Department of the Treasury's Office of Foreign Assets Control (OFAC), 'Sanctions Programs and Country Information', <https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information>.

6 OFAC FAQs are available at <https://home.treasury.gov/policy-issues/financial-sanctions/faqs>.

7 *ibid.*, No. 11.

8 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);

### 30.1.3 Licensing

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 related to the transmission of telecommunications and the services for personal communications, and the provision of legal services related to the requirements and compliance with US law (among others).

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.<sup>9</sup>

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

---

(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 #545.

<sup>9</sup> 31 CFR §§ 560.530 (3)(ii), 560.530 (4).

## Key jurisdictions

30.1.4

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.

### Cuba

30.1.4.1

The comprehensive sanctions on Cuba, governed by the Cuban Assets Control Regulations (CACR),<sup>10</sup> 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, including 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.<sup>11</sup> 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 placed, limiting the scope of the general licences.

### Iran

30.1.4.2

OFAC's sanctions programme on Iran is primarily governed by the ITSR.<sup>12</sup> The 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 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 States' withdrawal from the JCPOA on 8 May 2018.<sup>13</sup> With the issuance of Executive Order 13902 in January 2020, even more sectors of the Iranian

10 31 CFR Part 515.

11 31 CFR §§ 515.502 to 515.591.

12 31 CFR Part 560.

13 Exec. Orders 13902 and 13871 authorise the imposition of secondary sanctions on specified transactions involving Iran's iron, steel, aluminium copper, construction, mining, manufacturing and textile sectors. See Exec. Order No. 13902, 85 Fed. Reg. 2003 (10 January 2020); Exec. Order No. 13871, 84 Fed. Reg. 20761 (10 May 2019).

economy became the subject of secondary sanctions, meaning that most trade with Iran now potentially carries secondary sanctions exposure.<sup>14</sup>

#### 30.1.4.3 North Korea

The North Korean Sanctions Regulations<sup>15</sup> 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.<sup>16</sup>

#### 30.1.4.4 Syria

The Syrian Sanctions Regulations<sup>17</sup> 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) authorised 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 relating to the government of Syria, its military or any foreign person that is the subject of sanctions with respect to Syria.<sup>18</sup>

#### 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.<sup>19</sup> Executive Order 14065 similarly prohibits the above listed activities with respect to the DNR and the LNR.<sup>20</sup>

---

14 See Exec. Order No. 13902, 85 Fed. Reg. 2003 (10 January 2020).

15 31 CFR Part 510.

16 Exec. Order No. 13810, 82 Fed. Reg. 44705 (20 Sep. 2017).

17 31 CFR Part 542.

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

19 31 CFR Part 589.

20 Exec. Order No. 14065, 87 Fed. Reg. 10293 (23 February 2022).

## 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,<sup>21</sup> OFAC issued Directives 1 to 4, imposing sectoral sanctions against entities identified on OFAC's SSI List<sup>22</sup> operating in certain sectors of the Russian economy, such as financial services, energy and defence.<sup>23</sup> 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.<sup>24</sup>

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 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 a 33 per cent or more ownership interest. 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.<sup>25</sup>

The Directives imposed in early 2022 after Russia's invasion of Ukraine further expanded and added to those 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

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

22 The SSI List is available at <https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/sectoral-sanctions-identifications-ssi-list>.

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

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

25 OFAC FAQ #890; see also, Exec. Order No. 14024, 86 Fed. Reg. 20249 (15 Apr. 2021).

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 greater 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 the 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 owned 50 per cent or more, in the aggregate, 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.

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'<sup>26</sup> 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.<sup>27</sup> OFAC has effectively limited this threat of sanctions to transactions with any Russian person on its SDN list.<sup>28</sup>

CAATSA also mandates that the President impose sanctions on persons determined to have knowingly engaged in a significant transaction with a person 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<sup>29</sup> of persons determined to be part of, or operating for or on behalf of, Russian defence or intelligence sectors.<sup>30</sup>

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

26 See discussion on 'significant transactions', supra note 8B.

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

28 OFAC FAQ, No. 541.

29 CAATSA Section 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](http://www.state.gov/caatsa-section-231d-defense-and-intelligence-sectors-of-the-government-of-the-russian-federation).

30 CAATSA § 231.

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.<sup>31</sup>

## Venezuela

30.1.4.7

Executive Order 13884 blocks all property and interests in property of the government of Venezuela.<sup>32</sup> 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.<sup>33</sup> 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 as to what 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 or controlled’ is understood to encompass holding at least 50 per cent of the equity interest by vote or value, a majority of seats on the board of directors, or otherwise controlling actions, policies and personnel decisions of the foreign entity.<sup>34</sup>

See Chapter 26  
on fines,  
disgorgement, etc.

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

31 CAATSA § 232.

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

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

34 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 SDN List. See ‘OFAC Enforcement Information for October 1, 2019’, The General Electric Company, [https://home.treasury.gov/system/files/126/20191001\\_ge.pdf](https://home.treasury.gov/system/files/126/20191001_ge.pdf).

for ‘causing a violation’ by involving a US person in a transaction that would be prohibited for that US person.<sup>35</sup> 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.<sup>36</sup>

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 days of blocking or rejecting a transaction.<sup>37</sup> Previously, all parties had to report transactions involving blocked property to OFAC, but only US financial institutions were obliged to report rejected transactions.<sup>38</sup>

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

---

35 50 USC § 1705.

36 One example can be found in OFAC’s enforcement action against Standard Chartered Bank (SCB), a financial institution headquartered in the United Kingdom. In 2019, SCB entered into a global settlement with OFAC and other US federal agencies for processing transactions involving persons or countries that are the subject of comprehensive sanctions. The majority of the transactions concerned Iran-related accounts maintained by SCB’s Dubai branches that processed US dollar transactions through SCB’s branch office in New York or other US financial institutions. See ‘OFAC Enforcement Information for April 9, 2019’, Standard Chartered Bank, [https://home.treasury.gov/system/files/126/20190408\\_scb\\_webpost.pdf](https://home.treasury.gov/system/files/126/20190408_scb_webpost.pdf).

37 See 31 CFR § 501.603.

38 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 related to a Cuba-travel-related transaction. See OFAC ‘Enforcement Information for June 13, 2019’, [https://home.treasury.gov/system/files/126/20190612\\_hotelbeds\\_0\\_1.pdf](https://home.treasury.gov/system/files/126/20190612_hotelbeds_0_1.pdf).

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

### Factors to consider

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 various sanctions programmes administered by OFAC.<sup>39</sup> Another example is the ongoing Halkbank matter in which the US Supreme Court has agreed to hear Halkbank's appeal of the DOJ enforcement action against it. The DOJ case built on OFAC's civil enforcement action against Halkbank for apparent violations of the Iranian Transactions and Sanctions Regulations. The case is set for argument before the Supreme Court on 17 January 2023.<sup>40</sup>

30.4

30.4.1

<sup>39</sup> See United States of America Financial Crimes Enforcement Network Department of the Treasury, Consent Order Imposing Money Penalty In The Matter Of: Bittrex, Inc., 11 October 2022, available at: [https://www.fincen.gov/sites/default/files/enforcement\\_action/2022-10-11/Bittrex%20Consent%20Order%2010.11.2022.pdf](https://www.fincen.gov/sites/default/files/enforcement_action/2022-10-11/Bittrex%20Consent%20Order%2010.11.2022.pdf); see OFAC Enforcement Information for 11 October 2022, Bittrex, Inc., available at [https://home.treasury.gov/system/files/126/20221011\\_bittrex.pdf](https://home.treasury.gov/system/files/126/20221011_bittrex.pdf).

<sup>40</sup> See Docket of the Supreme Court for No. 21-1450, *Turkiye Halk Bankasi A.S. v. United States of America*, <https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/21a373.html#>; see Anna Bianca Roach, 'Supreme Court to Hear Halkbank Sanctions Case', *Global Investigations Review*, 3 October 2022, available at: <https://globalinvestigationsreview.com/just-sanctions/article/supreme-court-hear-halkbank-sanctions-case>.

### 30.4.2 Compliance framework

In May 2019, OFAC issued its Framework for Compliance Commitments.<sup>41</sup> 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 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 actions and other businesses in its industry can mitigate risks by implementing compliance policies and procedures proportional to the risks faced by the party and industry as a whole.<sup>42</sup> OFAC has indicated that the strength of a party's compliance programme can also be a significant mitigating or aggravating factor that it will consider when calculating a penalty amount.<sup>43</sup>

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'.<sup>44</sup> The DOJ will evaluate a party's compliance programme when determining whether to impose a monitor on the party once an enforcement action relating to an apparent violation of US sanctions laws is concluded.

---

41 'A Framework for OFAC Compliance Commitments'. [https://home.treasury.gov/system/files/126/framework\\_ofac\\_cc.pdf](https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf).

42 See 'OFAC Enforcement Information for February 26, 2020', Société Internationale de Télécommunications Aéronautiques SCRL, [https://home.treasury.gov/system/files/126/20200226\\_sita.pdf](https://home.treasury.gov/system/files/126/20200226_sita.pdf) ('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.').

43 In OFAC's enforcement action against Haverly Systems 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', [https://home.treasury.gov/system/files/126/20190425\\_haverly.pdf](https://home.treasury.gov/system/files/126/20190425_haverly.pdf).

44 DOJ, 'Evaluation of Corporate Compliance Programs', [www.justice.gov/criminal-fraud/page/file/937501/download](http://www.justice.gov/criminal-fraud/page/file/937501/download).

## Best practices

### 30.4.3

Once an investigation has commenced, parties should proactively collaborate and co-operate with the agency conducting the investigation. OFAC enforcement actions and enforcement guidelines highlight co-operation as a mitigating factor to be taken into account in an enforcement action.<sup>45</sup> Furthermore, if the DOJ is conducting an investigation relating to a wilful violation of US sanctions, the party must fully co-operate with the DOJ to receive the benefits associated with submitting a VSD. Generally, full co-operation 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.<sup>46</sup>

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.

## Self-reporting to OFAC

### 30.4.3.1

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 ensure 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.<sup>47</sup>

OFAC's enforcement guidelines list several instances where notices will not be considered a VSD, including licence applications, notifications from a

45 For example, in OFAC's enforcement action against Stanley Black & Decker, Inc and its subsidiary, OFAC found that Stanley Black & Decker's co-operation 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', [https://home.treasury.gov/system/files/126/20190327\\_decker.pdf](https://home.treasury.gov/system/files/126/20190327_decker.pdf).

46 For guidance on co-operating with OFAC, see 31 CFR 501 Appendix A(III)(G). For guidance on the requirements necessary for credit for full co-operation with a DOJ sanctions-related investigation, see DOJ Export Control and Sanctions Enforcement Policy for Business Organizations, pp. 3 to 5.

47 31 CFR 501 Appendix A(I)(I).

third party of an apparent violation or substantially similar apparent violation because it blocked or rejected a transaction, or if the disclosure:

- includes false or misleading information or is materially incomplete;
- is not self-initiated;
- is made without the authorisation of senior management; or
- is in response to an administrative subpoena or other enquiry form.<sup>48</sup>

### 30.4.3.2 Self-reporting to the DOJ

The DOJ's VSD policy, published on 13 December 2019, states that all business organisations, including financial institutions, are eligible for all the benefits detailed by the policy.<sup>49</sup> 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 co-operate with the investigation; and
- remediate any violations appropriately and in a timely manner.

The threshold for eligibility is self-disclosure of potential violations to CES. Unlike with OFAC, self-disclosing to any other regulatory agency is not considered an eligible VSD to the DOJ under its new policy.<sup>50</sup> Accordingly, to obtain the benefit of self-disclosure in a criminal investigation, parties must disclose to DOJ before OFAC.

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.<sup>51</sup>

To receive credit for full co-operation, parties are required to:

- disclose all relevant facts in a timely manner;
- co-operate 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.<sup>52</sup>

See Chapter 4  
on self-reporting  
to authorities

<sup>48</sup> Id.

<sup>49</sup> DOJ, 'Export Control and Sanctions Enforcement Policy for Business Organizations', [www.justice.gov/nsd/ces\\_vsd\\_policy\\_2019/download](https://www.justice.gov/nsd/ces_vsd_policy_2019/download).

<sup>50</sup> Id. at p. 3.

<sup>51</sup> Id.

<sup>52</sup> Id. at pp. 3 to 5; see also, Deputy Attorney General Lisa Monaco, Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group, 15 September 2022, available at: <https://www.justice.gov/opa/speech/file/1535301/download>. (The document discusses and provides guidance on corporate accountability and what constitutes co-operation during an investigation and VSDs. In the document, Deputy Attorney

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; 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.<sup>53</sup>

### *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. As noted above, if a party files a VSD with any other agency before filing with the DOJ, the party will not get credit from the DOJ for that VSD.

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.<sup>54</sup> 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.<sup>55</sup>

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

---

General Monaco highlights the need for a timely and fulsome disclosure for a corporation to get credit for a VSD, provides additional guidance on how DOJ prosecutors should provide credit for co-operation, 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 fulsome disclosure should be rewarded with credit for co-operation. Conversely, if a corporation uses those foreign laws to shield misconduct, the DOJ may make an adverse inference as to the corporation's co-operation.)

53 *Id.* at pp. 5 to 6.

54 *Id.* at pp. 2 to 3.

55 *Id.*

if the party has implemented an effective compliance programme at the time of resolution.<sup>56</sup> By filing with the DOJ, a party may invite a criminal investigation in addition to heavy, continuing disclosure obligations.

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.<sup>57</sup> 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 State Department.<sup>58</sup>

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.

### 30.4.3.3 Settlement

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

---

<sup>56</sup> *Id.*

<sup>57</sup> The Department of the Treasury maintains a list of memoranda of understanding between OFAC and state and federal banking regulators at <https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information/2019-enforcement-information/memoranda-of-understanding-between-ofac-and-bank-regulators>.

<sup>58</sup> 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 August 30, 2022), available at <https://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 relating to the apparent violation.<sup>59</sup>

## Trends and key issues

30.5

### Recent enforcement activity

30.5.1

Since the release of its 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.<sup>60</sup>*

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.<sup>61</sup> 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 use of servers located in the United States.<sup>62</sup> Late 2020 also saw OFAC

See Chapter 28  
on extraterritoriality

59 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 April 2019), <https://home.treasury.gov/news/press-releases/sm658>.

60 See OFAC 'Enforcement Information for January 27, 2020', Eagle Shipping International, [https://home.treasury.gov/system/files/126/20200127\\_eagle.pdf](https://home.treasury.gov/system/files/126/20200127_eagle.pdf).

61 For example, the 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', British Arab Commercial Bank, available at [https://home.treasury.gov/system/files/126/20190917\\_bacb.pdf](https://home.treasury.gov/system/files/126/20190917_bacb.pdf).

62 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

publish its first enforcement actions targeting apparent violations of US sanctions laws in the cryptocurrency industry.<sup>63</sup>

### 30.5.2 Potential pitfalls

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 to or 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 its Framework for Compliance Commitments, companies should ensure that their compliance programmes are in line with the Framework.

---

contained US-origin software. See OFAC 'Enforcement Information for February 26, 2020', Société Internationale de Télécommunications Aéronautiques SCRL, [https://home.treasury.gov/system/files/126/20200226\\_sita.pdf](https://home.treasury.gov/system/files/126/20200226_sita.pdf).

63 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 related to 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 the users were located in sanctioned jurisdictions based on their IP addresses were seen as aggravating factors. See OFAC 'Enforcement Information for December 30, 2020', BitGo, Inc., [https://home.treasury.gov/system/files/126/20201230\\_bitgo.pdf](https://home.treasury.gov/system/files/126/20201230_bitgo.pdf).

# Appendix 1

## About the Authors of Volume I

### **David Mortlock**

#### **Willkie Farr & Gallagher LLP**

David Mortlock is a partner and chair of the global trade and investment group at Willkie Farr & Gallagher LLP in Washington, DC. David provides clients with guidance on compliance and enforcement on national security-related issues, including sanctions and export controls, anti-money laundering and the Committee on Foreign Investment in the United States. He helps clients to build and implement compliance programmes, conduct internal investigations, respond to government enquiries and address enforcement actions.

From October 2013 to November 2015, David was director for international economic affairs at the White House National Security Council, where he was responsible for coordinating inter-agency work on sanctions, anti-corruption and other illicit finance issues. From August 2009 to October 2013, he held a number of roles at the US Department of State, including attorney-adviser for sanctions and terror finance, and deputy coordinator for sanctions policy.

David was centrally involved in developing or easing the sanctions programmes for Russia, Iran, Cuba, Burma and Venezuela, among others.

### **Britt Mosman**

#### **Willkie Farr & Gallagher LLP**

Britt Mosman is a partner in the global trade and investment group at Willkie Farr & Gallagher LLP in Washington, DC. Britt has advised global financial institutions and leading multinational companies on complex, international compliance and enforcement matters, particularly economic sanctions, anti-money laundering and anti-corruption laws, as well as transaction reviews by the Committee on Foreign Investment in the United States. Britt has deep experience with economic sanctions laws and regulations, having served as an attorney-adviser in the Office of the Chief Counsel (Foreign Assets Control) advising the Treasury Department's Office of Foreign Assets Control, prior to

joining Willkie. In this capacity, she focused on economic sanctions and national security issues, including as a lead attorney on the Iran, Ukraine and Russia, Cuba, Syria election interference and cyber-related sanctions programmes.

### **Nikki Cronin**

#### **Willkie Farr & Gallagher LLP**

Nikki Cronin is an associate in the global trade and investment practice group in Washington, DC. Nikki advises clients on government regulations relating to international trade and investment, with a particular focus on US economic sanctions. Nikki regularly advises both domestic and foreign clients on compliance and enforcement matters relating to US economic sanctions and export controls for a variety of industries, including financial institutions, private equity firms, oil and gas and media companies.

### **Ahmad El-Gamal**

#### **Willkie Farr & Gallagher LLP**

Ahmad El-Gamal is an associate in Willkie's global trade and investment group in Washington, DC. Ahmad provides advice to both domestic and foreign clients on government regulation of international trade and investment, particularly with regard to the Committee on Foreign Investment in the United States, economic sanctions and export controls.

#### **Willkie Farr & Gallagher LLP**

1875 K Street, NW  
Washington, DC 20006-1238  
United States  
Tel: +1 202 303 1000  
Fax: +1 202 303 2000  
dmortlock@willkie.com  
ncronin@willkie.com  
bmosman@willkie.com  
ael-gamal@willkie.com

[www.willkie.com](http://www.willkie.com)

