International
Comparative
Legal Guides

Practical cross-border insights into sanctions

Sanctions 2022

Third Edition

Contributing Editors:
Roberto J. Gonzalez & Rachel M. Fiorill
Paul, Weiss, Rifkind, Wharton & Garrison LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Recent Developments in U.S. Sanctions: OFAC Enforcement Trends and Compliance Lessons Learned


Roberto J. Gonzalez


Rachel M. Fiorill

Paul, Weiss, Rifkind, Wharton & Garrison LLP

Introduction

The U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") is in the midst of a record-setting streak of enforcement. Since January 2020, OFAC has taken 27 public enforcement actions and assessed over $39.2 million in civil monetary penalties. Increasingly, OFAC has drawn explicit links in its public enforcement actions to the compliance expectations laid out in its landmark 2019 guidance on the "hallmarks of an effective compliance program" (the "Framework"). U.S. and non-U.S. companies alike would be well-served to learn from the mistakes of similarly situated entities and incorporate the compliance guidance found in recent OFAC enforcement actions into their own sanctions risk assessments and compliance programmes.

This chapter discusses several of the main themes from recent OFAC enforcement actions and highlights the related compliance lessons learned.

OFAC's Compliance Framework

The 2019 Framework, and the related "compliance commitments" that are now a standard part of OFAC settlements, represent a new effort by OFAC to more clearly and comprehensively communicate its expectations about appropriate sanctions compliance practices. OFAC made clear that the guidance is intended not only for U.S. companies, but also for non-U.S. companies that conduct business in or with the United States, with U.S. persons, or using U.S.-origin goods or services. U.S. and non-U.S. companies would be well-advised to study the Framework carefully because, among other things, OFAC will consider a compliance programme that follows the Framework, a mitigating factor in the event of an enforcement action.[1]

The Framework describes five "essential components" of an effective sanctions compliance programme ("SCP"):[2]

- ***Management Commitment***. The Framework notes that Senior Management's[3] commitment to, and support of, a company's risk-based SCP is "one of the most important factors in determining its success". This commitment can be evidenced by management's: (1) review and approval of the SCP; (2) ensuring that the compliance function has sufficient authority and autonomy to deploy policies and procedures to effectively control OFAC risk (this includes the designation of a sanctions compliance officer); (3) ensuring the compliance function receives adequate resources; (4) promoting a "culture of compliance"; and (5) recognition of the seriousness of, and the implementation of necessary measures to reduce the occurrence of, sanctions violations.[4]
- ***Risk Assessment***. As is consistent with OFAC's past practice, the Framework recommends that SCPs be designed and updated pursuant to a "risk-based approach". OFAC officials have emphasised that not every company is expected to satisfy every element of the Framework, but rather companies should tailor their programmes to their unique risk profiles. One of the "central tenets" of a risk-based approach is for companies to "conduct a routine, and if appropriate, ongoing 'risk assessment' for the purposes of identifying potential OFAC issues they are likely to encounter."[5] OFAC identifies two core elements of a commitment to meet this compliance component: periodic risk assessments (including the conducting of due diligence during client and third-party onboarding and merger-and-acquisition activities); and the development of a methodology to analyse and address the particular risks identified by these risk assessments (which could include the root causes of any apparent violations or systemic deficiencies identified by the organisation during the routine course of business as well as through its testing and audit function).[6]
- ***Internal Controls***. Effective OFAC compliance programmes generally include internal controls to identify, interdict, escalate, report, and keep records pertaining to prohibited activity. Key elements include: (1) written policies and procedures tailored to the organisation's operations and risk profile and enforced through internal and/or external audits; (2) adequately addressing the results of a company's OFAC risk assessment; (3) implementation of immediate and effective remedial actions; (4) clear communication of policies and procedures to all relevant staff; and (5) identification of designated personnel responsible for integrating policies and procedures into daily operations.[7]
- ***Testing and Auditing***. A comprehensive and objective SCP audit function ensures the identification of programme weaknesses and deficiencies. OFAC notes that it is the company's responsibility to enhance its programme, including all programme-related software, systems, and other technology, to remediate any identified compliance gaps.
- ***Training***. The Framework describes training as "integral" and outlines OFAC's expectation that training programmes be "provided to all appropriate employees and personnel on a periodic basis (and at a minimum, annually) and generally should accomplish the following: (i) provide job-specific knowledge based on need; (ii) communicate the sanctions compliance responsibilities for each employee; and (iii) hold employees accountable for sanctions compliance training through assessments".[8]

© Published and reproduced with kind permission by Global Legal Group Ltd, London

As an appendix to the Framework, OFAC also describes some of the common "root causes" of the violations that were the subject of its prior enforcement actions. These themes and others are addressed in the enforcement trends section below.

Enforcement trends

Consistent with its new focus on compliance, OFAC has routinely incorporated compliance commitments into its public settlement agreements since December 2018; these settlements have involved both financial institutions and non-financial institutions.[9] In these settlements, OFAC has also imposed a requirement that the settling party annually certify its compliance with the commitments over a five-year period, a process which will likely require settling parties to invest additional resources in their SCPs and therefore increases the costs associated with OFAC settlements.

OFAC's enforcement actions in 2020 and the first half of 2021, together with the Framework's discussion of "root causes", highlight compliance deficiencies or breakdowns that are commonly responsible for sanctions violations. We describe the major areas of concern below.

Use of the U.S. financial system, including the use of U.S. dollar payments

OFAC has long viewed the use of the U.S. financial system for the benefit of sanctioned persons or jurisdictions as constituting a violation of U.S. sanctions.

OFAC's "big bank" enforcement actions have historically focused on global banks utilising "wire stripping" or other non-transparent payment methods to process transactions prohibited by U.S. sanctions through the U.S. financial system.[10] The 2019 multiagency resolutions with UniCredit Group ("UniCredit") ($1.3 billion in combined fines) and Standard Chartered Bank ("SCB") ($1.1 billion in combined fines assessed by the United States and United Kingdom), shows that the march of large, multi-agency enforcement actions against banks for such conduct continues to the present day.[11] The SCB action demonstrates that U.S. regulators have also taken enforcement action against financial institutions outside the context of "wire stripping" or other non-transparent payment methods. For example, DOJ cited the bank's transactions with an Iranian national who allegedly used supposed general trading companies in the UAE as fronts for a money exchange business located in Iran, and OFAC highlighted the bank's alleged delays in restricting sanctioned country access to its online banking platform and fax transmissions as a compliance failure that led to apparent sanctions violations.

Historically, OFAC and DOJ enforcement focused on banks – and not the banks' customers – that were conducting transactions with sanctioned jurisdictions or parties. However, in 2017, OFAC made clear through its enforcement action against Singaporean entity CSE Global Limited and its subsidiary CSE TransTel Pte. Ltd. that non-U.S. companies can violate U.S. sanctions by *causing* – through initiating U.S. dollar payments – U.S.-based banks or branches to violate sanctions by engaging in the prohibited exportation of financial services from the United States for the benefit of sanctioned parties or jurisdictions.

On July 16, 2020, DOJ and OFAC announced parallel resolutions with Essentra FZE Company Limited ("Essentra"), a UAE-based supplier, for selling cigarette products it knew to be ultimately destined for North Korea.[12] The transactions involved documentation falsely naming China as the destination. OFAC concluded that Essentra's conduct of this business and its *receipt* of three payments into its bank accounts at the non-U.S. branch of a U.S. bank "caused" the branch (a U.S. person) to export, directly or indirectly, financial services to North Korea. Similarly, in DOJ and OFAC's January 14, 2021, resolutions with PT Bukit Muria Jaya ("BMJ"), a paper products manufacturer located in Indonesia, BMJ "directed" payments for its North Korean exports to its USD bank account at a non-U.S. bank, which caused U.S. banks to clear wire transfers related to these exports.[13] Non-U.S. companies are now on notice of the risk of *criminal* enforcement in addition to OFAC enforcement for the use of U.S. dollar transactions (or transactions denominated in other currencies utilising non-U.S. branches of U.S. banks) in connection with sanctioned-country business. To reduce their risks, non-U.S companies should consider strengthening their sanctions compliance programmes, including training, controls, and employee oversight.

OFAC also recently issued its first and second public enforcement actions against cryptocurrency companies. First, on December 30, 2020, OFAC entered into a settlement with BitGo, Inc. ("BitGo"), a U.S. company that implements security and scalability platforms for digital assets and offers non-custodial secure digital wallet management services.[14] OFAC determined that deficiencies in BitGo's sanctions compliance procedures caused the company to fail to prevent persons it knew (based on IP address data) were located in sanctioned jurisdictions from using its non-custodial secure digital wallet management service. Similarly, on February 18, 2021, OFAC entered into a settlement with BitPay, Inc. ("BitPay"), a U.S. company that offers a payment processing solution for merchants to accept digital currency as payment, for processing payments on behalf of individuals who, based on IP addresses and information available in invoices, were located in sanctioned jurisdictions. Additionally, OFAC has recently focused on money service businesses ("MSBs"), as evidenced by its 2021 actions against Payoneer Inc. ("Payoneer") and MoneyGram Payment Systems, Inc. ("MoneyGram"). OFAC stated that such digital currency businesses and MSBs, like other financial services providers, are responsible for ensuring compliance with OFAC sanctions, including understanding their sanctions-related risks and taking steps to mitigate against such risks.[15]

Utilising non-standard payment or commercial practices

The Framework notes that companies are best positioned to determine whether a particular dealing, transaction, or activity is performed in a manner consistent with industry practice. Sometimes deviations from standard practice are driven by an effort to evade or circumvent sanctions. For example, on January 4, 2021, OFAC entered into a $8,572,500 settlement with Union de Banques Arabes et Françaises ("UBAF"), a French bank specialising in trade finance, for processing 127 payments on behalf of sanctioned Syrian financial institutions.[16] The majority of the apparent violations involved UBAF's processing of internal book-to-book transfers on behalf of Syrian entities that were followed by corresponding funds transfers through the U.S. financial system. The remaining violations were either "back-to-back" letter of credit transactions – where a sanctioned Syrian entity was the beneficiary of export letters of credit or the applicant for import letters of credit that did not involve USD clearing, but the intermediary entered into or received one or more corresponding USD letters of credit to purchase or sell the same goods – or other trade finance transactions involving sanctioned parties, all of which were processed through a U.S. bank. OFAC stated that UBAF's actions during this time

© Published and reproduced with kind permission by Global Legal Group Ltd, London

period demonstrated knowledge of OFAC sanctions, but the bank incorrectly believed that avoiding direct USD clearing on behalf of sanctioned parties was sufficient for compliance. In other instances, a customer may ask for accommodation that results in a sanctions violation. In OFAC's May 2019 Haverly Systems Inc. ("Haverly") settlement, it was determined that the company collected a debt from an entity on the Sectoral Sanctions Identification ("SSI") List outside of the permitted maturity window.[17] In this case, Haverty's Russian customer requested that Haverly reissue an invoice with a different date, in an attempt to re-characterise the debt as without the permitted maturity window.

Export or reexport of U.S.-origin goods

OFAC has regularly pursued enforcement actions against non-U.S. companies that purchased U.S.-origin goods with the intent of reexporting, transferring, or selling the items to a sanctioned person or jurisdiction. As noted in the Framework, some of OFAC's public enforcement actions in this area have focused on large or sophisticated entities that "engaged in a pattern or practice that lasted multiple years, ignored or failed to respond to numerous warning signs, utilised non-routine business practices, and – in several instances – concealed their activity in a wilful or reckless manner".[18]

For example, in April 2021, SAP SE ("SAP") entered into parallel resolutions with DOJ, OFAC, and BIS totalling around $8 million regarding U.S. sanctions and export violations involving the export of software and related services to Iran.[19] These resolutions involved, in part, SAP's release of U.S.-origin software to non-U.S. third parties who made the software available in Iran. OFAC determined that in some cases, SAP managers had direct knowledge and facilitated the purchase of this software. OFAC further determined that SAP had reason to know from IP address data that services were being downloaded in Iran. SAP was faulted for not adopting IP blocking technology to prevent such downloads. Additionally, several U.S.-based SAP subsidiaries allowed Iranian users to access U.S.-based cloud services. OFAC faulted SAP for allowing these subsidiaries to operate as standalone entities for years with respect to compliance, despite pre- and post-acquisition reports of significant compliance deficiencies.

Other OFAC actions in this area involve less egregious conduct. For example, in February 2020 OFAC reached a $2.4 million settlement with the Swiss entity Société Internationale de Télécommunications Aéronautiques SCRL ("SITA") involving, in part, SITA's provision of U.S.-origin software for the benefit of sanctioned airlines and its provision of messaging services that routed through servers in the United States, where messaging went to or from sanctioned airlines or other parties that were providing services to those airlines.[20] The SITA action represents OFAC's first public enforcement action involving sets of violations where the only U.S. nexuses were the provision of U.S.-origin software by a non-U.S. person and the use of a U.S.-based server, respectively.

U.S. parent liability for non-U.S. subsidiary business; facilitating activities of non-U.S. affiliates

Multiple recent OFAC enforcement actions highlight OFAC's increased willingness to hold U.S. parent companies liable for the Iranian or Cuban business conducted by their non-U.S. subsidiaries. For example, in Berkshire Hathaway, Inc.'s ("Berkshire"), October 20, 2020 settlement, OFAC held Berkshire accountable for its Turkish subsidiaries' sales to two Turkish intermediary companies with knowledge that these goods would be resold to Iran. OFAC found that these violations occurred despite the fact that Berkshire and other Berkshire subsidiaries repeatedly communicated with and sent policies to the Turkish subsidiary regarding Iran sanctions. The Turkish subsidiary nonetheless took steps to conceal its dealings with Iran, such as using private email addresses that bypassed the controls of the corporate email system, utilising false names and false invoices, and providing false responses to compliance inquiries. OFAC found that certain other Berkshire subsidiaries received information that could have revealed that orders might have been destined for Iranian end users – but only one Berkshire subsidiary flagged that transactions with Iranian customers were prohibited. These actions highlight the importance of performing appropriate due diligence in connection with the acquisition of non-U.S. entities and ensuring that subsidiaries of U.S. companies, and other entities controlled by U.S. companies, understand their obligations to comply with U.S. sanctions on Iran and Cuba, including when they supply goods to other companies within their corporate organisation.

Relatedly, multiple OFAC enforcement actions have involved U.S. firms referring business to, approving, or otherwise facilitating dealings with sanctioned persons or jurisdictions by their non-U.S. affiliates. On October 1, 2020, OFAC announced a $5.8 million settlement with New York travel services company Generali Global Assistance, Inc. ("GGA") for apparent violations of Cuba sanctions. GGA intentionally referred Cuba-related payments to its Canadian affiliate to avoid processing reimbursement payments directly to Cuban parties and to travelers while they were located in Cuba. GGA subsequently reimbursed its Canadian affiliate for those payments.

Additionally, non-U.S. companies with U.S. operations should take steps to ensure that U.S. offices and employees are walled off or recused from any sanctioned business engaged in by non-U.S. parts of the company. In July 2021, OFAC penalised a U.S. subsidiary of Alfa Laval AB for its referral of an Iranian business opportunity to its non-U.S. affiliate.[21] This case demonstrates the importance of adopting training to ensure U.S. persons know they are prohibited from referring or participating in business opportunities involving sanctioned jurisdictions.

Deficient due diligence

A fundamental element of sanctions compliance is conducting appropriate due diligence on customers, supply chains, intermediaries, and counterparties. OFAC has recently brought several enforcement actions resulting from deficient due diligence.

As demonstrated by OFAC's September 20, 2020 settlement with Deutsche Bank Trust Company Americas ("DBTCA"), financial institutions are expected to conduct appropriate diligence on transactions that raise sanctions red-flags prior to processing transactions.[22] Specifically, OFAC faulted DBTCA for not independently corroborating verbal representations it received from the U.S. counsel of a non-accountholder party to the transaction at issue in order to confirm that there was no SDN interest in the transaction. OFAC stated that although the payment transactions associated with the transaction did not contain an explicit reference to the SDN, the payment was "related to a series of purchases of fuel oil that involved" the SDN and that, at the time of the transaction, "DBTCA had reason to know of [the SDN's] potential interest in the transaction underlying the payment, which closely coincided [with the SDN's designation]". OFAC and other regulators expect companies to fully review all the documentation they receive for potential indicia of a nexus to a sanctioned jurisdiction or person prior to sending, approving, or facilitating a payment.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Similarly, OFAC expects that companies implement measures, beyond contractual provisions, to monitor and minimise sanctions risk over the life of a contractual relationship, such as a leasing agreement. In its settlement with U.S.-based Apollo Aviation Group LLC ("Apollo"), OFAC determined that Apollo leased three aircraft engines to a UAE company that subleased them to an airline in Ukraine that, in turn, installed the engines on an aircraft wet leased to an SDN.[23] When the engines were returned, Apollo discovered that the engines had been installed on aircraft owned by or leased to an SDN and used in Sudan (which, at the time, was subject to comprehensive U.S. sanctions). Although Apollo's lease agreements with the UAE company included sanctions commitments, OFAC faulted Apollo Aviation for failing to take steps to monitor whether the engines were being used in a sanctions compliant manner.

Misinterpreting, or failing to understand the applicability of, OFAC's regulations

Often companies will misunderstand the applicability or scope of OFAC's sanctions prohibitions either because they are not aware of sanctions regulations or because they are unaware that such regulations apply to them by virtue of their status as U.S. persons, U.S.-owned subsidiaries (with respect to Cuba and Iran sanctions), or non-U.S. persons engaged in activities with a U.S.-nexus (involving U.S. persons, U.S.-origin goods, or U.S. territory, including payments transiting the U.S. financial system).

For example, on July 28, 2020, Whitford Worldwide Company, LLC's ("Whitford"), settled with OFAC for conduct with Iran conducted by Whitford and its subsidiaries in Italy and Turkey.[24] Whitford's Regulatory Affairs Manager had incorrectly advised that Whitford's non-U.S. subsidiaries could continue selling to Iran legally as long as there were no direct connections between a subsidiary and Iran. As a result of this advice, Whitford developed a plan to continue selling to Iran, which required that all sales be directed through third-party distributors and that documents related to those sales avoid referencing Iran.

Another area of recent enforcement focus is the failure of companies to identify an applicable general licence or adhere to a general licence's conditions, rendering the otherwise available authorisation inapplicable. For example, in OFAC's May 2020 settlement with BIOMIN America, Inc., BIOMIN incorrectly believed that it could structure transactions involving a Cuban counterparty that would be consistent with OFAC's Cuba sanctions.[25] BIOMIN coordinated and received commissions on sales to a Cuban counterparty as executed by BIOMIN's non-U.S. affiliates. In determining that BIOMIN's conduct resulted in violations, OFAC noted that the company could have availed itself of an existing general licence – if the exports had been licensed by the Commerce Department – or applied for a specific licence, and likely avoided the violations, but because the company appears not to have understood the scope of OFAC's Cuba sanctions, it was not in a position to take advantage of these potential licensing avenues. Likewise, in OFAC's July 2020 settlement with Amazon.com, Inc. ("Amazon"), OFAC determined that Amazon's failure to abide by the reporting requirements associated with a general licence under its Ukraine-related sanctions effectively nullified that authorisation with respect to the affected transactions.

These actions demonstrate how companies can benefit from seeking appropriate advice and guidance when contemplating business involving U.S. sanctioned parties or jurisdictions. Management and sales teams would be wise to consult with internal and/or external legal or compliance experts to ensure that cross-border transaction structures do not run afoul of U.S. sanctions requirements. Such experts are also well positioned to identify potential eligibility for authorisations from OFAC, including general and specific licences.

Screening software limitations; deficiencies in automated processes

Many companies screen their customers and other third parties, but such screening may be deficient due to a failure to adequately calibrate, update, or audit their screening software, lists, and procedures. A significant number of recent enforcement actions involved sanctions screening deficiencies, making it clear that the utilisation of defective screening software or insufficient screening lists will not provide a shield against regulatory enforcement.

For example, in its November 2018 settlement with Cobham Holdings, Inc. ("Cobham"), OFAC found that Cobham made three shipments of goods through distributors in Canada and Russia to an entity that did not appear on the SDN List, but which was blocked under OFAC's "50 percent rule" because it was 51 per cent owned by a Russian SDN.[26] The apparent violations appear to have been caused by reliance on deficient third-party screening software. Although Cobham had selected "fuzzy" searching to detect partial matches, the software instead used an "all word" match criteria. The names of the blocked party and its subsidiary both contained several of the same uncommon words such that fuzzy searching apparently would have detected the match; however, under the "all word" criteria, the transactions were not flagged and were processed.

Additionally, in its settlement with Amazon, OFAC faulted, in part, the company's failure to screen for a city within a sanctioned jurisdiction and common alternative spellings of a sanctioned jurisdiction. OFAC also determined that Amazon's automated screening processes also failed to identify the correctly spelled names and addresses of persons on OFAC's SDN List. And in a second September 2020 settlement with DBTCA, OFAC determined that DBTCA failed to stop payments destined for accounts at a designated financial institution because – contrary to its existing policies and procedures – DBTCA did not include in its sanctions screening tool the designated financial institution's SWIFT Business Identifier Code.[27]

OFAC's April 30, 2020 finding of violation issued to American Express Travel Related Services Company ("Amex"), criticised Amex for approving an SDN's customer application submitted by a non-U.S. bank due to system deficiencies.[28] When the non-U.S. bank entered the SDN's information into the screening system, Amex's "risk engine" identified the applicant as a potential SDN and generated multiple "declined" messages to the non-U.S. bank indicating that the application could not be processed. However, the non-U.S. bank made several additional approval attempts that caused the screening engine to time out, triggering the application to be automatically approved.

OFAC has stated that companies should carefully review and understand the functionality and limitations of their sanctions screening software, ensure sufficient staff training regarding the software, update the software accordingly, and periodically evaluate the software with test data to ensure that it sufficiently flags transactions even absent an exact match. Additionally, companies should ensure that automated sanctions compliance controls measures cannot be overridden without appropriate review. Companies should also ensure that the lists they screen against not only capture indicators for sanctioned jurisdictions – such as cities, regions, and ports within sanctioned jurisdictions – but also appropriate name variations for those locations. The Cobham settlement further suggests that, depending on their risk profile, companies should consider investing in systems for identifying entities that are treated as SDNs under OFAC's 50 percent rule. In that settlement, OFAC recognised Cobham's adoption of such a system as a risk-reducing measure.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Mergers and acquisitions

Multiple recent OFAC enforcement actions highlight the importance of performing adequate sanctions due diligence with regard to potential acquisition targets and to implementing strong sanctions compliance procedures following acquisition. Often, although these non-U.S. subsidiaries were required by their U.S. parents to cease their transactions with sanctioned jurisdictions, the non-U.S. subsidiaries failed to do so.

For example, in its September 24, 2020 settlement with OFAC Keysight Technologies, Inc. ("Keysight"), agreed to pay $473,157 to settle violations of Iran sanctions on behalf of its former Finnish subsidiary, Anite Finland Oy ("Anite").[29] Prior to Keysight's acquisition of Anite in 2015, Anite had committed to cease all existing and future business with certain sanctioned countries, including Iran. After the acquisition, Keysight reiterated to Anite that sales to these countries must cease. Nevertheless, Anite's Vice President for Europe, Middle East, and Africa and its Regional Director for the Middle East both expressed reluctance to comply. The Regional Director and two employees then took measures to obfuscate from Keysight their dealings with Iran, including omitting references to Iran in correspondence. Although Keysight conducted an internal investigation upon discovering the misconduct and voluntarily self-disclosed the violations, OFAC deemed Anite's violations an egregious case due to the willful violations, active participation by senior managers, and attempts at concealment.

Individual liability

Historically, OFAC has generally not pursued enforcement actions against individuals outside of the Cuba-travel context. However, the Framework notes that "individual employees – particularly in supervisory, managerial, or executive-level positions – have played integral roles in causing or facilitating" sanctions violations, even in instances where "the U.S. entity had a fulsome sanctions compliance program in place" and in some cases these employees "made efforts to obfuscate and conceal their activities from others within the corporate organisation, including compliance personnel, as well as from regulators or law enforcement".[30] The Framework states that, in such instances, OFAC will consider enforcement actions not only against the entities, but against the individuals as well.[31]

In 2019, OFAC took the unprecedented step of designating a former company manager as a foreign sanctions evader while concurrently announcing a settlement with the company's U.S. parent.[32] Specifically, OFAC designated the former managing director of the U.S. company's Turkish subsidiary whom OFAC determined to be primarily responsible for directing the apparent violations at issue and seeking to conceal them. This designation highlights increased personal risk for personnel who play a central role in causing violations of U.S. sanctions law.

Conclusion

Although OFAC's regulations do not themselves require the implementation of a compliance programme, OFAC's Framework and the compliance guidance embedded in recent enforcement actions represent a new effort by OFAC to more clearly and comprehensively communicate its expectations about appropriate sanctions compliance practices. U.S. and non-U.S. companies alike would be well-advised to study this guidance and consider making appropriate enhancements to their compliance practices.

Endnotes

1. Paul, Weiss, *OFAC Issues Guidance on Sanctions Compliance Programs and Flags "Root Causes" Underlying Prior Enforcement Actions*, (May 14, 2019), available at https://www.paulweiss.com/practices/litigation/economic-sanctions-aml/publications/ofac-issues-guidance-on-sanctions-compliance-programs-and-flags-root-causes-underlying-prior-enforcement-actions?id=28725.
2. U.S. Dep't of the Treasury, Office of Foreign Assets Control, *A Framework for OFAC Compliance Commitments*, (May 2, 2019), available at https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information.
3. OFAC considers "senior management" to "typically include senior leadership, executives, and/or the board of directors". *See* Framework at 2.
4. *Id.* at 2–3.
5. *Id.* at 3.
6. *Id.* at 3–5.
7. *Id.* at 5–6.
8. *Id.* at 7.
9. *See e.g.*, U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Nov. 19, 2018*, available at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information; *Enforcement Information for Apr. 15, 2019*, available at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information; *see* also Paul, Weiss, *UniCredit Group Banks Agree to Pay a Combined $1.3 Billion Penalty for Iranian and Other Sanctions Violations; One Bank Pleads Guilty* (May 1, 2019), available at https://www.paulweiss.com/practices/litigation/economic-sanctions-aml/publications/unicredit-group-banks-agree-to-pay-a-combined-13-billion-penalty-for-iranian-and-other-sanctions-violations-one-bank-pleads-guilty?id=28671.
10. U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Nov. 19, 2018,* available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190415_uni_webpost.pdf; *Enforcement Information for Apr. 15, 2019*, available at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information; *see* also *Paul, Weiss, UniCredit Group Banks Agree to Pay a Combined $1.3 Billion Penalty for Iranian and Other Sanctions Violations; One Bank Pleads Guilty (May 1, 2019)*, available at https://www.paulweiss.com/practices/litigation/economic-sanctions-aml/publications/unicredit-group-banks-agree-to-pay-a-combined-13-billion-penalty-for-iranian-and-other-sanctions-violations-one-bank-pleads-guilty?id=28671.
11. U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Nov. 19, 2018,* available at https://home.treasury.gov/policy-issues/financial-sanctions/civ il-penalties-and-enforcement-information; *Enforcement Information for Apr. 15, 2019*, available at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information; *see* also *Paul, Weiss, UniCredit Group Banks Agree to Pay a Combined $1.3 Billion Penalty for Iranian and Other Sanctions Violations; One Bank Pleads Guilty (May 1, 2019)*, available at https://www.paulweiss.com/practices/litigation/economic-sanctions-aml/publications/unicredit-group-banks-agree-to-pay-a-combined-13-billion-penalty-for-iranian-and-other-sanctions-violations-one-bank-pleads-guilty?id=28671.
12. *See* U.S. Dep't of Justice, Essentra Fze Admits to North Korean Sanctions and Fraud Violations, Agrees to Pay Fine (July 16, 2020), available at https://www.justice.gov/

© Published and reproduced with kind permission by Global Legal Group Ltd, London

opa/pr/essentra-fze-admits-north-korean-sanctions-and-fraud-violations-agrees-pay-fine ("DOJ Press Release"); Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Essentra FZE Company Limited (July 16, 2020) available at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information ("OFAC Settlement Agreement"); *see* also Paul, Weiss, DOJ and OFAC Enforcement Actions Against Essentra FZE Signal New Sanctions Risks for Non-U.S. Companies Utilizing the U.S. Financial System (July 23, 2020), available at https://www.paulweiss.com/media/3980400/23july20-doj-ofac.pdf.

13. U.S. Dep't of Justice, *Indonesian Company Admits To Deceiving U.S. Banks In Order To Trade With North Korea, Agrees To Pay A Fine Of More Than $1.5 Million* (Jan. 17, 2021), available at https://www.justice.gov/opa/pr/indonesian-company-admits-deceiving-us-banks-order-trade-north-korea-agrees-pay-fine-more-15; U.S. Dep't of Treasury, *OFAC Settles with PT Bukit Muria Jaya for Its Potential Civil Liability for Apparent Violations of the North Korea Sanctions Regulations* (Jan. 14, 2021), available at https://home.treasury.gov/system/files/126/20210114_BMJ.pdf.
14. U.S. Dept. of Treasury, Office of Foreign Assets Control, *Enforcement Information for Dec. 30, 2020*, available at https://home.treasury.gov/system/files/126/20201230_bitgo.pdf.
15. *See* U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for July 23, 2021,* available at https://home.treasury.gov/system/files/126/20210723_payoneer_inc.pdf; U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for April 29, 2021*, available at https://home.treasury.gov/system/files/126/20210429_moneygram.pdf.
16. U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Enters Into $8,572,500 Settlement with Union de Banques Arabes et Françaises for Apparent Violations of Syria-Related Sanctions Program* (Jan. 4, 2021), available at https://home.treasury.gov/system/files/126/01042021_UBAF.pdf.
17. U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Apr. 25, 2019*, available at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information.
18. Framework at 10.
19. U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Apr. 29, 2021*, available at https://home.treasury.gov/system/files/126/20210429_sap.pdf.
20. U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Feb. 26, 2020*, available at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information. Paul, Weiss, *OFAC Cites the Use of U.S.-Origin Software and U.S. Network Infrastructure in Reaching a Nearly $8 Million Settlement with a Swiss Commercial Aviation Services Company* (Mar. 16, 2020), available at https://www.paulweiss.com/media/3979437/16mar20-ofac.pdf.
21. U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for July 19, 2021*, available at https://home.treasury.gov/system/files/126/20210719_al.pdf.
22. U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Sept. 20, 2020*, available at https://home.treasury.gov/system/files/126/20200909_DBTCA.pdf.
23. U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Nov. 7, 2019*, available at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information; *see* also Paul, Weiss, *OFAC Enforcement Action against U.S. Aviation Company Shows the Importance of Ongoing Monitoring over the Course of a Contractual Relationship* (Dec. 9, 2019), available at https://www.paulweiss.com/practices/litigation/economic-sanctions-aml/publications/ofac-enforcement-action-against-us-aviation-company-shows-the-importance-of-ongoing-monitoring-over-the-course-of-a-contractual-relationship?id=30324.
24. U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for July 28, 2020*, available at https://home.treasury.gov/system/files/126/20200728_whitford.pdf.
25. U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for May 2, 2019*, available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20200506_biomin.pdf.
26. U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Nov. 27, 2019*, available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20181127_metelics.pdf; *see* also Paul, Weiss, *OFAC Reaches Settlement with Cobham Holdings, Inc. for Violations Resulting from Deficient Screening Software* (Nov. 29, 2018), available at https://www.paulweiss.com/practices/litigation/economic-sanctions-aml/publications/ofac-reaches-settlement-with-cobham-holdings-inc-for-violations-resulting-from-deficient-screening-software?id=27872.
27. U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Sept. 20, 2020*, available at https://home.treasury.gov/system/files/126/20200909_DBTCA.pdf.
28. U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Issues a Finding of Violation to American Express Travel Related Services Company for Violations of the Weapons of Mass Destruction Proliferators Sanctions Regulations* (Apr. 30, 2020), available at https://home.treasury.gov/system/files/126/20200430_amex.pdf.
29. U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Sept. 24, 2020*, available at https://home.treasury.gov/system/files/126/20200924_keysight.pdf.
30. Framework at 12.
31. *Id.*
32. U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Feb. 7, 2019*, available at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information; Paul, Weiss, *In Unprecedented Move, OFAC Takes Enforcement Action Against U.S. Parent Company for Turkish Subsidiary's Iran Sanctions Violations and Simultaneously Sanctions the Subsidiary's Ex-Managing Director* (Feb. 11, 2019), available at https://www.paulweiss.com/media/3978456/11feb19-ofac-kollmorgen.pdf.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Roberto J. Gonzalez is a litigation partner and the co-chair of the firm's Economic Sanctions and Anti-Money Laundering Practice Group. He represents global financial institutions, technology companies and other clients in civil and criminal investigations and enforcement matters relating to U.S. economic sanctions, export controls, and anti-money laundering. He also provides regulatory advice, compliance counselling, and transactional due diligence to U.S. and non-U.S. companies across a range of sectors. He writes and speaks frequently on these topics. Roberto joined Paul, Weiss after serving several years in senior legal positions at the U.S. Treasury Department, the Consumer Financial Protection Bureau, and the White House Counsel's Office. As Deputy General Counsel of the Treasury Department, Roberto supervised over a hundred lawyers – including the legal offices of OFAC and FinCEN – in the areas of sanctions, anti-money laundering, and financial regulation. He uses his multi-faceted experience in the federal government to help clients navigate the constantly evolving U.S. regulatory and enforcement landscape.

Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K Street, NW
Washington, D.C., 20006-1047
USA

Tel: +1 202 223 7316
Email: rgonzalez@paulweiss.com
URL: www.paulweiss.com

Rachel M. Fiorill, Counsel in the Litigation Department, formerly served as an Enforcement Section Chief at the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC").
At OFAC, Rachel led the investigation and resolution of hundreds of enforcement actions, including several groundbreaking civil monetary penalties. She served the Enforcement Division's lead for Ukraine/Russia and Syria-related investigations and developed particular expertise with OFAC's Iran sanctions while representing the Enforcement Division in agency-wide Joint Comprehensive Plan of Action ("JCPOA") implementation matters. She liaised with other law enforcement and intelligence agencies regarding joint investigations, enforcement priorities and strategies and provided guidance on OFAC's Economic Sanctions Enforcement Guidelines and sanctions programmes to counterparts at other agencies and the public.
She advises clients on government inquiries and investigations, sanctions compliance and risk management, and transactional due diligence. She counsels on a variety of financial crime and international trade issues, including economic sanctions, anti-money laundering, anti-corruption, and export controls.

Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K Street, NW
Washington, D.C., 20006-1047
USA

Tel: +1 202 223 7346
Email: rfiorill@paulweiss.com
URL: www.paulweiss.com

Paul, Weiss is a firm of more than 1,000 lawyers with diverse backgrounds, personalities, ideas and interests who provide innovative and effective solutions. We take great pride in representing our clients in their most critical legal matters and most significant transactions, as well as individuals and organisations in need of *pro bono* assistance.
Our team advises U.S. and non-U.S. clients across industries on their most sensitive U.S. economic sanctions, export control, and Bank Secrecy Act/anti-money laundering (BSA/AML) issues. We provide regulatory advice and compliance counselling, apply for licences and interpretive guidance on behalf of clients, and perform transactional due diligence. With our preeminent regulatory defence and white collar experience, we are also uniquely positioned to: assist clients in responding to regulator inquiries, examinations, and subpoenas; conducting internal investigations; and handling matters that develop into multi-agency civil and criminal investigations.

www.paulweiss.com

Paul | Weiss

© Published and reproduced with kind permission by Global Legal Group Ltd, London

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: glg global legal group