OFAC Update

A framework for compliance and recent settlement

BETTY SANTANGELO, GARY STEIN, JENNIFER M. OPHEIM AND HANNAH M. THIBIDEAU, SCHULTE ROTH & ZABEL

In May 2, 2019, the US Department of the Treasury's Office of Foreign Assets Control ("OFAC") published "A Framework for OFAC Compliance Commitments" ("Framework") outlining five critical components of a risk-based sanctions compliance program.[1] Along with the Framework, OFAC also released a list of compliance program deficiencies most commonly identified as root causes of apparent violations of OFAC regulations. As discussed below, several of these deficiencies have, in fact, been identified by OFAC in its latest settlements and findings, which reflect an aggressive approach to sanctions enforcement, including multimillion-dollar settlements for activity that was primarily conducted abroad by foreign affiliates of US companies.

OFAC's "A Framework for OFAC Compliance Commitments"

OFAC regulations do not require companies to maintain a sanctions compliance program, or "SCP" for short. Nonetheless, OFAC encourages firms subject to US jurisdiction — including foreign entities that conduct business in or with the United States, US persons, or using US-origin goods or services — to adopt a formal SCP. The Framework is intended to assist such firms in developing, implementing and updating their respective SCPs. It also outlines how OFAC may evaluate apparent violations and resolve investigations resulting in settlement. More specifically, if, after determining that a civil monetary penalty is the appropriate administrative action in response to an apparent violation, OFAC will evaluate a firm's SCP — consistent with the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, App. A — and will consider favorably the existence of an effective SCP at the time of an apparent violation.

While each firm's risk-based SCP will depend on a variety of factors, including the company's size and sophistication, products and services, customers and counterparties and geographic locations, each SCP should incorporate five essential components of compliance: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.

First, OFAC has stated that senior management's commitment to, and support of, a firm's SCP is one of the most important factors in determining the success of the SCP. Such support is essential in ensuring that the firm's compliance unit receives adequate resources (including in terms of human capital, expertise and information technology) and that compliance personnel are delegated sufficient authority and autonomy to deploy policies and procedures in a manner that effectively controls risk. To this end, senior management should review and approve a firm's SCP, recognize the seriousness of sanctions rules and promote a culture of compliance throughout the organization — including by discouraging misconduct, highlighting the potential repercussions of non-compliance and addressing the root causes of past violations.

Second, firms should conduct routine, if not ongoing, risk assessments to identify potential OFAC issues, address the particular risks identified, and tailor policies, procedures, internal controls and training to mitigate such risks. The risk assessment should holistically review the firm from top to bottom and assess all touchpoints to the outside world, including, where applicable, customers, supply chains, intermediaries, counterparties, products and services, transactions and geographic locations. The risk assessment should be updated to reflect the root causes of any apparent violations or systemic deficiencies identified either during the routine course of business or through a testing or audit function. The risk assessment should also inform the extent of due diligence conducted at customer on-boarding, as well as in the context of mergers and acquisitions.

Third, effective SCPs should include internal controls. To that end, firms should design and implement written policies and procedures outlining the SCP, including how to identify, interdict, escalate, report and keep records regarding activity that may be prohibited by OFAC.

Fourth, firms should have a comprehensive and objective testing or audit function to identify SCP weaknesses and deficiencies and take immediate and effective action to remediate any gaps.

Lastly, firms should provide OFAC-related training with a scope and frequency tailored to the firm's risk profile.

As noted above, OFAC also issued a non-exhaustive list of root causes associated with apparent violations of OFAC regulations. The aim of this list is to assist firms in designing, updating and amending their SCPs to avoid breakdowns. The root causes identified in the list include (1) lack of a formal OFAC SCP; (2) misinterpreting, or failing to understand the applicability of, OFAC's regulations; (3) facilitating transactions by non-US persons (including through or by overseas subsidiaries or affiliates); (4) exporting or re-exporting US-origin goods, technology, or services to OFAC-sanctioned persons or countries; (5) utilizing the US financial system, or processing payments to or through US financial institutions, for commercial transactions involving OFAC-sanctioned persons or countries; (6) sanctions screening software or filter faults; (7) improper due diligence on customers/clients (e.g., ownership, business dealings, etc.); (8) de-centralized compliance functions and inconsistent application of an SCP; (9) utilizing non-standard payment or commercial practices; and (10) individual liability. With respect to individual liability, OFAC expressed concern about individual employees, particularly in high-level positions, who ignored warning signs that

certain activity was likely prohibited or were aware of the misconduct and actually played an integral role with respect to the violations.

Common to several of these deficiencies is the extension of OFAC's reach to foreign-based operations. For example, OFAC stated that several firms did not understand — or blatantly disregarded — their status as a US person, and thus, the fact that OFAC sanctions applied to them. This is particularly relevant to the applicability of the Cuba and Iran programs to US-owned or controlled subsidiaries, where, for instance, foreign firms may not consider themselves to be US persons, but may nevertheless be subject to OFAC rules and regulations. In addition, many non-US persons were found to have violated OFAC regulations by processing financial transactions through the US financial system.

Many of these deficiencies were identified in the recent settlements and other findings described below. In the Framework, OFAC recommended that all organizations subject to US jurisdiction review OFAC's settlements to reassess and enhance their SCPs.

Stanley Black & Decker Inc. settlement

On March 27, 2019, Stanley Black & Decker Inc. ("Stanley Black & Decker"), based in New Britain, Connecticut, on behalf of itself and its subsidiary Jiangsu Guoqiang Tools Co. Ltd. ("GQ"), located in China, agreed to pay approximately $1.9 million to settle its potential civil liability for apparent violations of the Iranian Transactions and Sections Regulations, 31 C.F.R. part 560 ("ITSR").[2] More specifically, between approximately June 2013 and December 2014, GQ exported and attempted to export 23 shipments of power tools and spare parts, with a total value of approximately $3.2 million, to Iran or to a third country with knowledge that such goods were intended for Iran, in violation of § 560.215 of the ITSR.

Stanley Black & Decker initially identified GQ's exports to Iran during acquisition negotiations in 2011, and required GQ to cease such sales as a precondition to closing. Following the closing, Stanley Black & Decker provided training to GQ's employees, and GQ's senior management executed written agreements in which they attested that GQ would not engage in transactions with Iran. Nevertheless, GQ continued to export goods to Iran through the use of non-routine business practices — GQ used trading companies located in the United Arab Emirates and China as conduits for the sales, created fictitious bills of lading with incorrect ports of discharge and places of delivery, and instructed their customers not to write "Iran" on business documents.

Once Stanley Black & Decker became aware of the potential violations, it initiated an internal investigation, hired a third-party independent investigative company, and voluntarily self-disclosed the apparent violations on behalf of GQ. This action demonstrates that US parent companies face exposure to civil monetary penalties through the actions of their foreign subsidiaries, even where they have taken steps to avoid such violations. US companies should conduct sanctions due diligence, especially on foreign M&A targets, and monitor foreign subsidiaries for compliance through audit and testing functions.

UniCredit Global settlement

On April 15, 2019, several entities within the UniCredit Group — including UniCredit Bank AG,[3] headquartered in Munich, Germany, UniCredit Bank Austria,[4] headquartered in Vienna, Austria, and UniCredit S.p.A.,[5] headquartered in Milan, Italy — agreed to pay over $1.3 billion in penalties as part of a global settlement with multiple US law enforcement agencies[6] in connection with apparent violations of numerous sanctions programs between January 2007 and December 2011.[7] More specifically, all three UniCredit entities were found to have non-transparently routed US dollar payments involving sanctioned countries, entities or individuals by removing, omitting or not revealing references to, or the interest or involvement of, sanctioned parties in the payment messages sent through US financial institutions — a process known as "wire stripping."[8]

For example, in order to conceal from US regulators and banks the involvement of sanctioned entities, UniCredit Bank AG designed and formalized a written policy instructing employees to process transactions with sanctioned entities in an "OFAC-neutral" manner so that "no US bank can see OFAC contents" in any payment message processed through US financial institutions.[9] In addition, for at least two years after the Islamic Republic of Iran Shipping Lines ("IRISL") was added to OFAC's Specially Designated Nationals ("SDN") List, UniCredit Bank AG opened "safe accounts" to send IRISL-related payments through the United States in a manner that concealed information from US financial institutions showing that IRISL and its related companies were the true originators or beneficiaries of the payment.[10]

Similarly, UniCredit Bank Austria made a "business policy decision" to continue non-transparent payment processing and created written guidelines instructing employees to give "attention … that no obvious references in the payment request are included which can suggest an infringement of international regulations (e.g., reason for payment or acting parties)."[11] UniCredit Bank Austria also utilized a double MT202 method to process sanctioned transactions whereby the payment message that was sent to the US correspondent bank did not contain information on the originator or beneficiary of the payment, while a separate message was sent to the overseas beneficiary bank, which contained information regarding the originator and beneficiary of the payment.[12]

Notably, the UniCredit entities subject to this $1.3-billion penalty are foreign financial institutions headquartered and operating abroad. OFAC's only apparent jurisdictional hook was that the transactions in question were US dollar payments that passed through a US financial institution. Thus, this case demonstrates OFAC's expansive view of its jurisdiction and the importance of OFAC compliance even for foreign financial institutions.

Expedia Group Inc. settlement

On June 13, 2019, Expedia Group Inc. ("Expedia"), headquartered in Bellevue, Washington, on behalf of itself and its subsidiaries worldwide, agreed to pay $325,406 to settle its potential civil liability for apparent violations of the Cuban Assets Control Regulations ("CACR"), 31 C.F.R. part 501.[13] More specifically, between April 22, 2011 and October 16, 2014, certain of Expedia's foreign subsidiaries assisted 2,221 persons, including Cuban nationals, with travel or travel-related services for travel within Cuba or between Cuba and non-US locations.

The apparent prohibited travel was electronically booked because of failures or gaps in Expedia's technical implementations and other measures to avoid such apparent violations. In at least one case, Expedia failed to inform the subsidiary that it was subject to US sanctions laws for 15 months.

Once Expedia became aware of these apparent violations it self-disclosed them to OFAC. This settlement demonstrates OFAC's willingness to fine US companies for their oversight over foreign subsidiaries, which is an element identified as part of a root cause of SCP breakdowns or deficiencies. US companies must ensure that foreign subsidiaries are compliant with OFAC's regulations promptly following an acquisition. **THFJ**

FOOTNOTES

1. US Department of the Treasury, "A Framework for OFAC Compliance Commitments" (May 2, 2019).
2. US Department of Treasury, Enforcement Information for March 27, 2019 (Stanley Black & Decker, Inc.), available here; US Department of Treasury, Settlement Agreement (Stanley Black & Decker, Inc.).
3. US Department of the Treasury, Settlement Agreement (UniCredit Bank AG).
4. US Department of the Treasury, Settlement Agreement (UniCredit Bank Austria AG).
5. US Department of the Treasury, Settlement Agreement (OFAC and UniCredit S.p.A.).
6. In addition to OFAC, as part of the global settlement, the UniCredit entities resolved actions with the US Department of Justice, the Board of Governors of the Federal Reserve System, the New York State Department of Financial Services and the New York County District Attorney's Office.
7. The apparent violations relate to the following programs: the Weapons of Mass Destruction Proliferators Sanctions Regulations, 31 C.F.R. Part 544; the Cuban Assets Control Regulations, 31 C.F.R. Part 515; the Burmese Sanctions Regulations, 31 C.F.R. Part 537; the Sudanese Sanctions Regulations, 31 C.F.R. Part 538; the Syrian Sanctions Regulations, 31 C.F.R. Part 542; the Iranian Transactions and Sanctions Regulations, 31 C.F.R. Part 560; the Libyan Sanctions Regulations, 31 C.F.R. Part 570; and the Global Terrorism Sanctions Regulations, 31 C.F.R. Part 594.
8. US Department of Justice, Press Release, "UniCredit Bank AG Agrees to Plead Guilty for Illegally Processing Transactions in Violation of Iranian Sanctions" (Apr. 15, 2019.
9. US v. UniCredit Bank AG, 1:19-cr-00128-BAG, Information at *2 (Apr. 15, 2019.
10. Id.
11. UniCredit Bank Austria Non-Prosecution Agreement at *11 (Apr. 15, 2019).
12. Id.
13. US Department of Treasury, Enforcement Information for June 13, 2019 (Expedia Group, Inc.).