Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Navigating the rough waters of Global Sanctions

An e-Book publication sponsored by REFINITIV™ DATA IS JUST THE BEGINNING

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily e-mail newsletter, a bi-monthly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. www.complianceweek.com

REFINITIV™

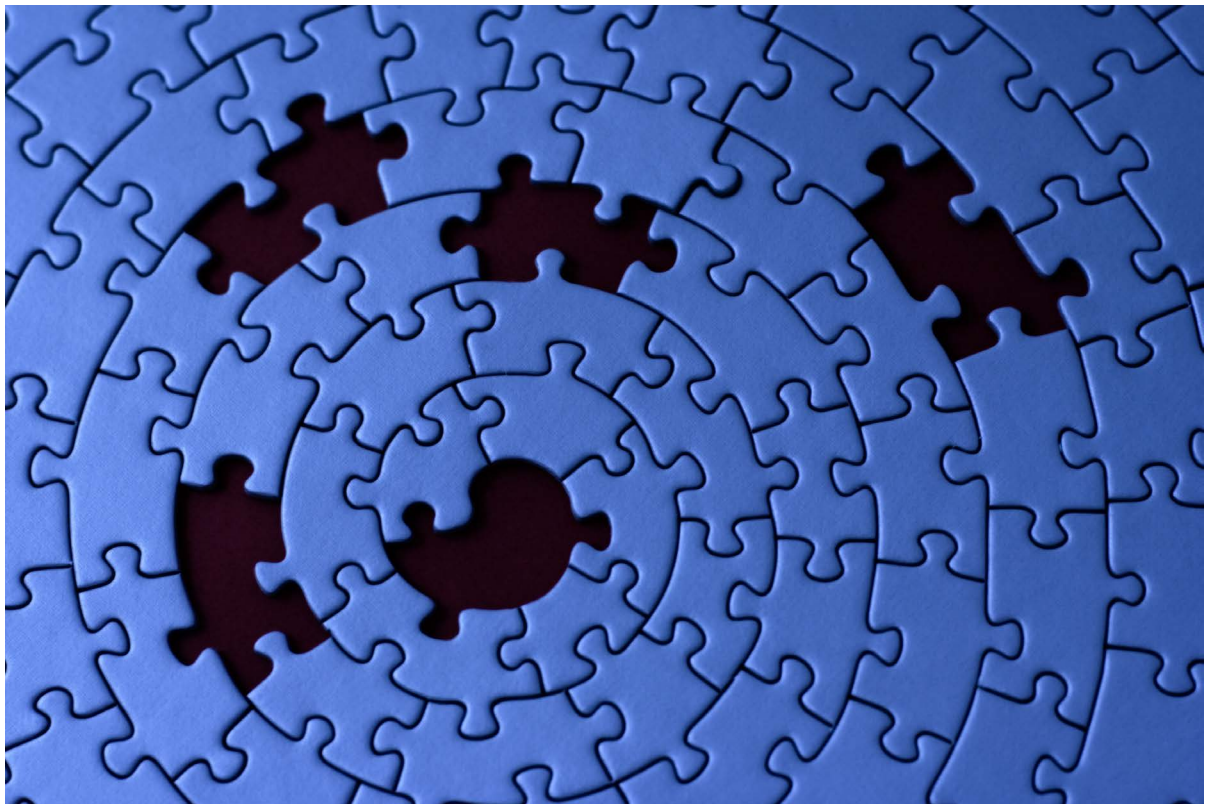
DATA IS JUST
THE BEGINNING

One of the world's largest providers of financial markets data and infrastructure, and serving more than 40,000 institutions in over 190 countries, Refinitiv delivers trusted risk management solutions that encompass regulatory change, anti-bribery and corruption, third party and supply chain risk, anti-money laundering, financial crime, KYC, and enterprise GRC management.

To help mitigate risk, Refinitiv provides an end-to-end third party risk management solution to take your internal processes from initial screening and due diligence through on-boarding and monitoring. At our core is a unique open ecosystem of expert partners and curated products that uncovers opportunity and drives change.

The possibilities? Endless. A dynamic combination of data, insights, technology, and news means you can access solutions for every challenge, including a breadth of applications, tools, and content – all supported by human expertise. To learn more, visit www.refinitiv.com

Inside this e-Book



Five 'essential components' of sanctions compliance

Chief Compliance Officers got some much-needed guidance from OFAC on how to build a well-crafted sanctions compliance program. **Jaclyn Jaeger** reports.

Chief compliance officers seeking some much-needed guidance on how to build a well-crafted sanctions compliance program would be remiss to ignore the first-ever "Framework for OFAC Compliance Commitments" published by the Department of the Treasury's Office of Foreign Assets Control. The guidance includes a non-exhaustive list of common "root causes" of sanctions violations identified during the investigative process and in the context of recent enforcement actions.

"OFAC developed this framework in our continuing effort to strengthen sanctions compliance practices across the board," said OFAC Director Andrea Gacki. "This underlines our commitment to engage with the private sector to further promote understanding of, and compliance with, sanctions requirements."

The 12-page sanctions compliance framework, published May 2, 2019, applies not just to U.S. companies, but also to companies that may find themselves subject to U.S. sanctions laws—such as foreign entities that conduct business in or with the United States, those that employ U.S. citizens, or that use U.S.-origin goods or services.

The framework comes at a time when the stakes for non-compliance have never been higher. From November through May 2019, OFAC issued 18 enforcement actions and a record $1.3 billion in total penalties, according to enforcement data from OFAC's Website

Chief compliance officers and chief risk officers will not find anything earth-shattering in the guidance, only that "it takes a lot of mystery out of what is expected," John Melican, global head of Exiger's financial crime compliance practice, said during a June 25, 2019 Webcast on the OFAC framework. "This is not regulation. This is guidance, so there are no standards, no new expectations."

In fact, much of what is in the framework resembles the revised Evaluation of Corporate Compliance Programs, published by the Justice Department's Criminal Division on April 30, 2019. Specifically, OFAC reiterated that each risk-based, sanctions compliance program (SCP) should take a tailored approach based on a variety of factors—including the company's size and sophistication, products and services, customers and counterparties, and geographic locations.

At the same time, however, OFAC stressed that each risk-based SCP should be predicated on and incorporate five "essential components." Below, we dive into not only what those five essential components are, as outlined in the OFAC guidance, but how to implement them in practice.

1. Senior management commitment

In its guidance, OFAC said senior management commitment is "one of the most important factors" in determining an SCP's success. Such commitment is essential in ensuring that the SCP receives adequate resources and is fully integrated into daily operations. It also helps to "legitimize the program, empower its personnel, and foster a culture of compliance throughout the organization," according to OFAC.

Chief compliance officers, particularly, should welcome the guidance in this aspect, as it puts the onus on senior management to ensure compliance units have "sufficient authority and autonomy" to effectively implement policies and procedures designed to minimize risk and ensure compliance has adequate resources. It also calls on senior management to review and approve the SCP.

One way to evidence senior management commitment to OFAC is to have in place a "dedicated" OFAC sanctions compliance officer. Where some companies, depending on size and complexity, designate a single person to oversee all areas of financial crimes or export control compliance, "this may be the same person serving in other senior compliance positions," like a Bank Secrecy Act officer or an export control officer, OFAC said.

Another way to evidence senior management commitment is through the quality and experience of the personnel dedicated to the SCP, including those with technical knowledge and expertise around OFAC's regulations, processes, and actions; the ability to understand complex financial and commercial activities and apply their knowledge of OFAC to these items; and someone with appropriate experience and authority within the organization. Compliance personnel should also have an appropriate level of control functions that support the risk-based SCP.

2. Risk assessments

Risk assessments should "generally consist of a holistic review of the organization from top-to-bottom and assess its touchpoints to the outside world," OFAC said. Areas to assess for potential risks include customers, supply chains, intermediaries, and counter-parties; the products and services that the organization offers, including how and where

"OFAC developed this framework in our continuing effort to strengthen sanctions compliance practices across the board. This underlines our commitment to engage with the private sector to further promote understanding of, and compliance with, sanctions requirements."

Andrea Gacki, Director, OFAC

such items fit into other financial or commercial products, services, networks, or systems; and the geographic locations of the organization.

In the financial services industry, banks have been risk-rating their clients and customers for years now. "Corporates are going to have to engage in that same process," Melican said, by asking, "'What are our risky products and services? Which are the ones that cross borders? Which are the ones that are likely to enter sanctioned jurisdictions?'" The Federal Financial Institutions Examination Council (FFIEC) also provides guidance on risk management processes that non-financial institutions could leverage, he said.

When assessing sanctions risks, look to leverage what you have and develop the SCP from there. "There is no expectation of reinventing the wheel," said David Sewell, a counsel in Debevoise & Plimpton, who also spoke on the Webcast.

An anti-bribery/anti-corruption risk assessment, for example, may be a good foundation for the SCP risk assessment, since regions that pose a high risk for bribery likely pose a high sanctions risk, as well. In its guidance, OFAC also recommends companies leverage existing information derived during onboarding, such as through the Customer Due Diligence (CDD) or Know Your Customer (KYC) process.

"Risk assessments and sanctions-related due diligence is also important during mergers and acquisitions, particularly in scenarios involving non-U.S. companies," OFAC stressed. In practice, the compliance function should engage in appropriate due diligence to ensure sanctions-related issues are identified, escalated to senior management, addressed prior to the conclusion of any transaction, and incorporated into the risk assessment process.

Following the completion of an M&A transaction, audits "will be critical to identifying any additional sanctions-related issues," OFAC said. Finally, risk assessments must be updated to account for the root causes of any violations or systemic deficiencies identified by the organization during the routine course of business—for example, through a testing or audit function.

3. Internal controls

The purpose of internal controls relative to an SCP is to clarify expectations, define procedures and processes pertaining to OFAC compliance (including reporting and escalation chains), and minimize the risks identified by the SCP risk assessment. The policies and procedures outlining the SCP should be "relevant to the organization, capture the organization's day-to-day operations and procedures, are easy to follow, and designed to prevent employees from engaging in misconduct," OFAC said.

There should also be someone with primary responsibility for "integrating the SCP's policies and procedures into the daily operations of the company," the guidance states. "This process includes consultations with relevant business units and confirms the organization's employees understand the policies and procedures."

In practice, this means if you simply have policies and procedures in place and no one with primary responsibility to integrate them, "I don't think you're going to get the credit from OFAC that [you are] looking for if something goes wrong," Melican said.

Policies and procedures should be enforced, and weaknesses should be identified (including through root cause analysis of any compliance breaches) and remediated. Furthermore, internal or external audits and assessments of the program should be conducted periodically.

4. Testing and auditing

A comprehensive and objective testing or audit function within an SCP ensures the company identifies program weaknesses and deficiencies. Moreover, it is the company's responsibility to enhance the program to remediate any identified compliance gaps.

Testing and auditing can be conducted on a specific element of an SCP or at the enterprise-wide level. "Make sure that your foreign subsidiaries are subject to the same audit policy," Melican said.

5. Training

The training program should be provided to all appropriate employees and personnel on a periodic basis, and at a minimum, annually. Generally, OFAC advised, the training program should provide job-specific knowledge based on need; communicate the sanctions compliance responsibilities for each employee; and hold employees accountable for sanctions compliance training through assessments.

Furthermore, such training should extend to not just employees, but all stakeholders—clients, suppliers, business partners, and counterparties—to support the organization's OFAC compliance efforts. In the event of a negative testing result or audit finding, further training or other corrective action should be provided concerning relevant personnel. Lastly, training materials should be easily accessible and available to employees on an ongoing basis.

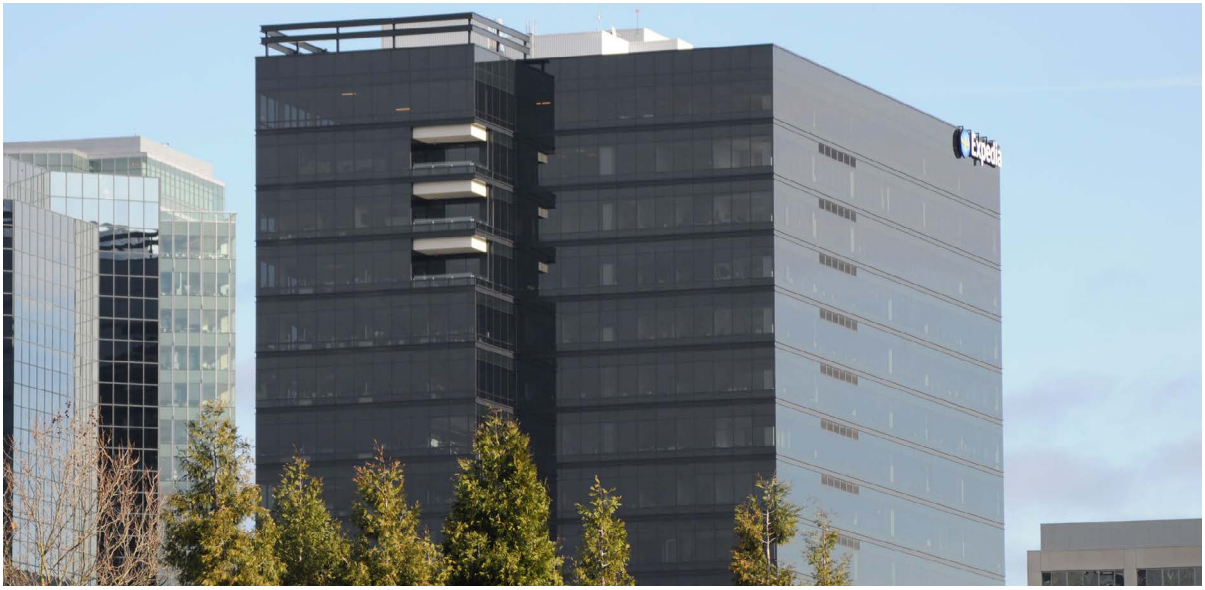
Ten common 'root causes' of violations

In addition to outlining the five essential components of an SCP, OFAC also helpfully includes a non-exhaustive list of 10 common "root causes" of sanctions violations that it identified during the investigative process. "These are reoccurring areas where companies have had problems," Sewell said.

The root causes OFAC has outlined include:

- Lack of a formal OFAC sanctions compliance program;
- Misinterpreting, or failing to understand the applicability of, OFAC's regulations;
- Facilitating transactions by non-U.S. persons, including through or by overseas subsidiaries or affiliates;
- Exporting or re-exporting U.S.-origin goods, technology, or services to OFAC-sanctioned persons or countries;
- Using the U.S. financial system for transactions involving OFAC-sanctioned parties;
- Incomplete due diligence on customers/clients;
- Failure to update sanctions screening software;
- Using non-standard payments or commercial practices;
- Decentralized compliance functions and inconsistent application of an SCP; and
- Individual liability playing integral roles in causing or facilitating violations of the regulations administered by OFAC.

Now that OFAC has spelled out what it's looking for in a robust sanctions compliance program and has described what it has identified as the "root causes" of sanctions violations, compliance officers for U.S. companies and global companies with a U.S. nexus should review the framework to ensure their SCP meets OFAC's expectations, particularly since OFAC said it will "consider favorably" effective SCPs when resolving an enforcement action. ■



Expedia settles with Treasury for violations of U.S. sanctions on Cuba

Jaclyn Jaeger explores details of Expedia's $325K settlement with Treasury's Office of Foreign Assets Control.

Expedia Group has agreed to pay $325,406 to resolve allegations that it violated U.S. sanctions on Cuba, the Treasury's Office of Foreign Assets Control announced.

According to the settlement agreement, between April 2011 and October 2014, Expedia allegedly violated U.S. sanctions by assisting 2,221 people, some of whom were Cuban nationals, with travel or travel-related services for travel within Cuba or between Cuba and locations outside the United States.

OFAC said the violations occurred "because certain Expedia foreign subsidiaries lacked an understanding of and familiarity with U.S. economic sanctions laws, and Expedia employees overlooked particular aspects of Expedia's business that presented risks of non-compliance with sanctions. Specifically, electronically booked travel resulted from failures or gaps in Expedia's technical implementations and other measures to avoid such apparent violations."

"With respect to at least one foreign subsidiary, Expedia failed to inform the subsidiary until approximately 15 months after Expedia acquired the subsidiary that it was subject to U.S. jurisdiction and law," OFAC said. "Expedia was slow to integrate the subsidiary into the Expedia corporate family, including with respect to compliance with U.S. sanctions, and the subsidiary continued operating independently during the integration period."

In determining the settlement amount, OFAC considered the following to be aggravating factors: Expedia "failed to exercise a minimal degree of cau-

tion or care" in avoiding the conduct that led to the violations. Moreover, based on the number of violations, the length of time over which the violations occurred, and the number of Expedia entities involved, the violations "appear to have resulted from a pattern or practice of conduct," OFAC said.

Expedia, however, voluntarily self-disclosed the violations to OFAC. After discovering the violations, Expedia also implemented "significant remedial measures to strengthen its U.S. economic sanctions compliance program throughout the Expedia corporate family, including domestic and foreign direct and indirect subsidiaries," OFAC noted.

OFAC also said that Expedia cooperated with OFAC's investigation "by submitting data analytics associated with the apparent violations, responding to OFAC's requests for additional information, and entering to multiple tolling agreements."

As part of the settlement agreement with OFAC, moreover, Expedia has committed to enhancing its compliance procedures by ensuring that Expedia:

» Has a management team in place that is committed to compliance;
» Conducts regular risk assessments to ensure that Expedia's internal controls appropriately mitigate its sanctions-related risks;
» Conducts regular testing and audits; and
» Provides ongoing sanctions compliance training throughout the Expedia corporate family.

Additionally, Expedia has steadily increased its resources dedicated to compliance with U.S. sanctions, resulting in substantially more robust staffing and resources corporate-wide and has taken measures to increase compliance with U.S. sanctions, including enhanced screening methods and implementation of automated software restrictions, OFAC noted.

OFAC said the case illustrates the sort of benefits that companies can realize—including, with respect to OFAC's Cuba sanctions, entities owned or controlled by U.S. persons—when they implement corporate-wide compliance measures. "U.S. companies can mitigate risk by conducting sanctions-related due diligence both prior and subsequent to mergers and acquisitions," OFAC said, "and taking appropriate steps to audit, monitor, train, and verify newly acquired subsidiaries for OFAC compliance."

Prudent compliance officers will want to heed OFAC's advice, particularly since OFAC unveiled amendments to the Cuban Assets Control Regulations (CACR) on June 4, 2019. These amendments complement changes to the Department of Commerce's Bureau of Industry and Security (BIS) Export Administration Regulations (EAR). BIS, in coordination with OFAC, is amending the EAR to make passenger and recreational vessels and private and corporate aircraft ineligible for a license exception and to establish a general policy of denial for license applications involving those vessels and aircraft.

"Cuba continues to play a destabilizing role in the Western Hemisphere, providing a communist foothold in the region and propping up U.S. adversaries in places like Venezuela and Nicaragua by fomenting instability, undermining the rule of law, and suppressing democratic processes," said Treasury Secretary Steven Mnuchin. "This Administration has made a strategic decision to reverse the loosening of sanctions and other restrictions on the Cuban regime. These actions will help to keep U.S. dollars out of the hands of Cuban military, intelligence, and security services. ■

"U.S. companies can mitigate risk by conducting sanctions-related due diligence both prior and subsequent to mergers and acquisitions."

OFAC

FinCEN to financial firms: Beware of Venezuelan money laundering

FinCEN recently alerted financial institutions of continued widespread public corruption in Venezuela. **Jaclyn Jaeger** has more.

The Financial Crimes Enforcement Network (FinCEN) issued an updated advisory alerting financial institutions of continued widespread public corruption in Venezuela and the methods Venezuelan senior political figures and their associates may use to move and hide proceeds of their corruption.

The advisory also provides and updates several financial red flags to watch for to assist in identifying and reporting suspicious activity that might be indicative of corruption.

"The international financial community must be vigilant to prevent exploitation by corrupt regime insiders and their enablers, including front companies and foreign financial institutions that continue to prop up this illegitimate regime," Sigal Mandelker, under secretary of the Treasury for Terrorism and Financial Intelligence, said in a statement.

On Jan. 23, the United States recognized the President of the Venezuelan National Assembly, Juan Guaidó, as the interim president of Venezuela and the legitimate leader of the Venezuelan people. The illegitimate regime of former Venezuelan president Nicolas Maduro has engaged in corruption through state-owned enterprises and offshore third parties, FinCEN said. In recent years, financial firms have reported increased activity with suspected links to Venezuelan public corruption, including government contracts.

FinCEN warns of the misuse of Venezuela's government-sponsored food distribution program, Los Comités Locales de Abastecimiento y Producción ("Local Supply and Production Committees"), which is commonly referred to as the "CLAP program." CLAP was created in 2016 for the publicly stated purpose of providing subsidized food rations to Venezuelan citizens.

"The illegitimate former Maduro regime is using the CLAP program to provide subsidized food to its supporters, withhold food from ordinary Venezuelan citizens and those critical of the regime, and enrich corrupt regime insiders and their allies through embezzlement, price manipulation, and trade-based money laundering schemes using front and shell companies," FinCEN said.

The Maduro regime also has experimented with the use of digital currency to circumvent sanctions and generate revenue, according to FinCEN. It has developed a digital currency called the "petro" and reportedly continues to develop new tokens.

In 2018, Russian bank Evrofinance Mosnarbank emerged as the primary international financial institution willing to finance the petro, FinCEN notes. In March 2019, Treasury's Office of Foreign Assets Control (OFAC) sanctioned Evrofinance Mosnarbank for materially assisting, sponsoring, or providing financial, material, or technological support for, or goods or services to or in support of, Petroleos de Venezuela, S.A. (PdVSA). Financial institutions are reminded that Executive Order 13827 prohibits U.S. persons from any involvement in the petro digital currency.

"Financial institutions should take risk-based steps to identify and limit any exposure they may have to funds and other assets associated with Venezuelan public corruption fueled by the Maduro regime," FinCEN said. "However, financial institutions should be aware that normal business and other transactions involving Venezuelan nationals and businesses do not necessarily represent the same risk as transactions and relationships identified as being connected to the former Venezuelan regime." ■

UniCredit Group Banks pay $1.3B for sanctions abuses

Jaclyn Jaeger provides an in-depth look at court documents expounding on UniCredit's sanctions violations.

UniCredit Bank, a Munich-based financial institution operating under the name HypoVereinsbank, has pleaded guilty and will pay approximately $1.3 billion for processing hundreds of millions of dollars of transactions through the U.S. financial system on behalf of an entity designated as a weapons of mass destruction proliferator and other Iranian entities subject to U.S. economic sanctions.

UniCredit Bank (UCB AG) and UniCredit Bank Austria (BA)—both part of the UniCredit Group—agreed to forfeit $20 million and enter into a non-prosecution agreement (NPA) to resolve an investigation into its violations of the International Emergency Economic Powers Act (IEEPA). UniCredit SpA, the parent of both UCB AG and BA, has agreed to ensure that UCB AG and BA's obligations are fulfilled.

According to court documents, UCB AG over 10 years "knowingly and willfully moved at least $393 million through the U.S. financial system on behalf of sanctioned entities, most of which was for an entity the U.S. government specifically prohibited from accessing the U.S. financial system. UCB AG engaged in this criminal conduct through a scheme formalized in its own bank polices and designed to conceal from U.S. regulators and banks the involvement of sanctioned entities in certain transactions."

Court documents describe how UCB AG routed illegal payments through U.S. financial institutions for the benefit of the sanctioned entities in ways that concealed the involvement of the sanctioned entities. "When the United States sanctioned Iranian entities for proliferating weapons of mass destruction, UCB AG went to great lengths to help one such entity—Islamic Republic of Iran Shipping Lines—evade sanctions to gain access to the U.S. financial system," said Assistant Attorney General Brian Benczkowski.

UCB AG will waive indictment and be charged in a one-count felony criminal information, according to documents to be filed in federal court in the District of Columbia, charging UCB AG with knowingly and willfully conspiring to commit violations of IEEPA and to defraud the United States from 2002 through 2011. UCB AG has agreed to plead guilty, entered into a written plea agreement, and accepted responsibility for its criminal conduct. The plea agreement, subject to approval by the court, provides that UCB AG will forfeit $316.5 million and pay a fine of $468.3 million.

According to admissions in the NPA and accompanying statement of facts, between 2002 and 2012, BA used non-transparent methods to send payments related to sanctioned jurisdictions such as Iran through the United States. BA conspired to violate IEEPA and defraud the United States by processing transactions worth at least $20 million through the United States on behalf of customers located or doing business in Iran and other countries subject to U.S. economic sanctions or customers otherwise subject to U.S. economic sanctions. Due to its crimes, BA will forfeit $20 million and has agreed to additional compliance and sanctions enhancements.

Also, UCB AG has entered into a plea agreement with the New York County District Attorney's Office (DANY) for violating New York State law and will pay $316.5 million. BA has also entered an NPA with DANY for violating New York State law. DANY conducted its own investigation alongside the Justice Department.

UniCredit SpA, UCB AG, and BA have also entered into settlement agreements, including with the U.S. Treasury's Office of Foreign Assets Control (OFAC); the Board of Governors of the Federal Reserve System; and the New York State Department of Financial Services under which they will pay additional penalties of $611 million to OFAC, which will be satisfied in part by payments to the Justice Department and the Federal Reserve; $157.7 million to the Federal Reserve, and $405 million to NYDFS.

Compliance obligations

According to OFAC, between 2007 and 2011, UCB AG processed over 2,000 payments totaling over $500 million through financial institutions in the United States in violation of multiple U.S. sanctions programs. During this time, UniCredit operated U.S. dollar accounts on behalf of the Islamic Republic of Iran Shipping Lines (IRISL) and several companies owned by or otherwise affiliated with IRISL, and managed the accounts of those companies in a manner that obscured the interest or involvement of IRISL in transactions sent to or through U.S. intermediaries.

For several years (UCB AG) and 2012 (BA and UniCredit Bank S.p.A.), all three banks processed payments to or through the United States in a manner that did not disclose underlying sanctioned persons or countries to U.S. financial institutions that were acting as financial intermediaries. These transactions constitute violations of contemporaneous sanctions programs targeting proliferators of weapons of mass destruction, global terrorism, and the following countries: Burma, Cuba, Iran, Libya, Sudan, and Syria.

Sigal Mandelker, Under Secretary for Terrorism and Financial Intelligence, said: "These banks have agreed to implement and maintain commitments to enhance their sanctions compliance. As the United States continues to enhance our sanctions programs, incorporating compliance commitments in OFAC settlement agreements is a key part of our broader strategy to ensure that the private sector implements strong and effective compliance programs that protect the U.S. financial system from abuse."

Under the agreements, each bank must implement and maintain compliance commitments designed to minimize the risk of violations reoccurring. The full set of commitments are identified in each of the banks' public settlement agreements and include a commitment from senior management to promote a "culture of compliance" throughout each organization; a commitment that each bank implements internal controls that adequately address the results of its OFAC risk assessment and profile; and a commitment to providing adequate training to support each bank's OFAC compliance efforts. ■

REFINITIV EXPERT TALK

U.S. Sanctions on Venezuela: Are all your risk-bases covered?

By Ernst Pienaar
Head of Content Specialists, World-Check®, Refinitiv

As global financial institutions (FIs) continue to scramble to deal with the ramifications of a further round of sanctions on Venezuela imposed by the United States, how can you ensure that your organization does not inadvertently fall foul of the law?

Background

In 2017 the U.S. imposed Sectoral Sanctions against the Government of Venezuela, the Central Bank of Venezuela and state-owned oil company, Petroleos de Venezuela SA (PdVSA). In January 2019 the U.S. Government broadened its existing Executive Order 13850[1] and took 'additional steps to address the national emergency with respect to Venezuela' with Executive Order 13857.[2]

This was the latest in a lengthy history of U.S. sanctions against Venezuela. According to a February 2019 publication by the Congressional Research Service, 'For more than a decade, the United States has employed sanctions as a policy tool in response to activities of the Venezuelan government or respective Venezuelan individuals. These have included sanctions, including targeted sanctions against almost 100 individuals, related to terrorism, drug trafficking, trafficking in persons, antidemocratic actions, human rights violations and corruption.'[3]

The January 2019 round of sanctions, which were also implicit in nature, have effectively blocked U.S. companies from transacting with PdVSA while it remains under the control of Nicolás Maduro's government.

In January, the European Parliament voted to recognize opposition leader Juan Guaido as interim president while Maduro's government stands accused of 'stifling democracy'.[4]

In August 2019 US Executive Order 13884 was issued now effectively blocking all property and interests in property of the Government of Venezuela that are in the United States, that come within the United States, or that are or come within possession or control of any United States person. While this is not a country embargo, this Executive Order directly targets the Maduro regime and those who support it, while exempting transactions related to humanitarian activity, including the provision of articles such as food, clothing, and medicine intended to be used to relieve human suffering.

OFAC has concurrently issued a general license authorizing transactions with Interim President Juan Guaido, the National Assembly, and individuals appointed or designated by Guaido.

According to the E.O. the term "Government of Venezuela" includes the state and Government of Venezuela, any political subdivision, agency, or instrumentality thereof, including the Central Bank of Venezuela and Petroleos de Venezuela, S.A. (PdVSA), any person owned or controlled, directly or indirectly, by the foregoing, and any person who has acted or purported to act directly or indirectly for or on behalf of, any of the foregoing, including as a member of the Maduro regime.

1 treasury.gov/resource-center/sanctions/Programs/Documents/venezuela_gl11.pdf
2 m.treasury.gov/resource-center/sanctions/Programs/Documents/13857.pdf
3 fas.org/sgp/crs/row/IF10715.pdf
4 reuters.com/article/us-venezuela-politics-eu-idUSKCN1PP1HQ

Narrative sanctions and the 50% rule

Narrative sanctions (also referred to as implicit sanctions) are those that don't specifically name an entity but where the sanctions still applies to such non-listed entity (other than the main sanctioned entity). This creates a challenge for organizations, as there is no finite sanction list to follow, but rather they must ensure that they do not transact with any blocked entity in terms of the 50% rule, described more fully below.

In 2014, the U.S. Department of Treasury issued the 'REVISED GUIDANCE ON ENTITIES OWNED BY PERSONS WHOSE PROPERTY AND INTERESTS IN PROPERTY ARE BLOCKED' stating that 'Persons whose property and interests in property are blocked pursuant to an Executive Order or regulations administered by Office of Foreign Asset Control (OFAC) (blocked persons) are considered to have an interest in all property and interests in property of an entity in which such blocked persons own, whether individually or in the aggregate, directly or indirectly, a 50% or greater interest'.

Consequently, any entity owned in the aggregate, directly or indirectly, 50% or more by one or more blocked persons, is itself considered to be a blocked person. The property and interests in property of such an entity are blocked regardless of whether the entity itself is listed in the annex to an Executive Order or otherwise placed on the U.S. OFAC list of Specially Designated Nationals (SDNs). Accordingly, a U.S. person generally may not engage in any transactions with such an entity, unless authorized by OFAC. U.S. persons are advised to act with caution when considering a transaction with a non-blocked entity, in which one or more blocked persons have a significant ownership interest that is less than 50% or which one or more blocked persons may control by means other than a majority ownership interest. Such entities may be the subject of future designation or enforcement action by OFAC.[5]

This effectively means that any entity that is 50% or more owned by blocked individuals or entities is also considered to be blocked. Ownership can be direct or indirect or in the aggregate.

Developing a targeted response

These developments have left many FIs and businesses scrambling to comply and needing watertight assurance that they have not missed potential risk related to transacting with any entity implicated in terms of the 50% rule.

A holistic and targeted response involves screening for such entities and then conducting enhanced due diligence (EDD) on any entity flagged as high risk. These steps are discussed in more detail below.

Screening for sanctions

Efficient screening depends on access to reliable and complete information as well as the right tools to pinpoint relevant nuggets of information.

Data – finding what's relevant

World-Check Risk Intelligence is the trusted solution when dealing with the onerous task of complying with the 50% rule. Our data for example also covers entity records where credible and reputable sources indicate that OFAC sanctioned SDNs individuals or entities and Sectoral Sanctions Identifications (SSIs) entities own, exercise control, sit on the Board of Directors of, or are closely associated with the entity itself.

Such entities are tagged with the World-Check keyword INSAE-WC (International Sanctions Associated Entity – World-Check data) to indicate that they have been included on the database because they are more than 25% owned (beneficial ownership, in order to flag cases where caution is advised even where ownership is less than 50%) or controlled by or associated with a sanctioned (OFAC, EU, UN, UKHMT) individual or entity, either directly or in aggregate ownership of 50% or more. In the latter instance, these records are also tagged with the INSAE-50-WC keyword to indicate said direct, indirect or aggregate majority ownership.

Tagging removes much of the noise factor and ensures that these relevant entities are not missed.

How has Refinitiv responded to the Venezuela Executive Orders?

When the Venezuelan Sectoral Sanctions were issued at the end of 2017 under E.O. 13808, Refinitiv responded with the addition of a new keyword and completed thorough and rigorous research to uncover all entities owned or controlled by the Government of Venezuela, the Central Bank of Venezuela and PdVSA.

This keyword, USA – VEPTRE-WC (Venezuela Prohibited Transactions Relevant Entity World-Check Data), covered all entities connected to, related to, associated with, affiliated or linked to, owned, or controlled by PdVSA, the Central Bank of Venezuela, or any entity owned or controlled (directly or indirectly) or acting on behalf of the Government of Venezuela within World-Check per U.S. Executive Order 13808.

On 28 January 2019, PdVSA was also added to OFACs SDN list.[6] This meant that the company and its non-OFAC listed subsidiaries are now subject to full financial restrictions and not only the Sectoral Sanctions. Refinitiv responded by allocating two existing keywords to relevant entries for PdVSA on the VEPTRE-WC keyword. These two World-Check specific keywords* have also been assigned to both directly and indirectly owned PdVSA entries as follows:

5 m.treasury.gov/resource-center/sanctions/Documents/licensing_guidance.pdf

6 lexology.com/library/detail.aspx?g=1a5f286c-698b-48f6-9a07-1a8ff5c2ce62

*Please note that these keywords are not Sanction, Law or Regulatory Enforcement keywords but merely general keywords requested by clients to simplify targeted data extraction from the World-Check database.

- The INSAE-WC keyword covers all entities (not individuals) owned or controlled by or associated with a sanctioned (UN, EU, OFAC, UKHMT) individual or entity within World-Check.
- The INSAE-50-WC keyword covers any entity owned 50% or more by a sanctioned individual/entity either direct, indirect or in the aggregate, within World-Check.

As a result of the August 2019 U.S. Executive Order 13884 now effectively blocking all property and interests in property of the Government of Venezuela the VEPTRE-WC keyword no longer is a pure Sectoral Sanctions keyword but can also be used for screening for E.O. 13884 related entities. These updates offer peace of mind that entities potentially implicated by recent developments are also covered.

Carrying out Enhanced Due Diligence

Once initial screening has identified any entities or areas of concern, the next step is to undertake a detailed review of such entities, and make informed decisions to help you safeguard your reputation and comply with all relevant legislation. An Enhanced Due Diligence (EDD) report is the magnifying glass that delivers detailed and targeted information on any entity or individual anywhere in the world and being able to access this critical intelligence empowers organizations to make informed decisions to avoid risk.

EDD reports provide a greater level of scrutiny of potential business associates and highlight risk that cannot be detected at geopolitical analysis or batch screening level. They offer auditable proof of due diligence and help meet legal obligations.

Partnering for a holistic solution

Many organizations may choose to partner with a trusted provider to manage the complex and ever-changing regulatory landscape, particularly in light of these recent U.S. sanctions.

Screening Resolution Service (SRS) is Refinitiv's managed service that helps companies with an international footprint implement effective internal control procedures to ensure compliance with the full range of legal requirements and reduce exposure to risk during the customer onboarding, screening, and monitoring phases.

Our service highlights positive and possible matches for any customer identification program, detecting heightened risk individuals and entities, screened against World-Check Risk Intelligence.

Staying on the right side of the (changing) law

Given the complex and far-reaching nature of these sanctions, many organizations feel that they need to up their game.

"We're going to have to require not enhanced due diligence, but (in some instances) a kind of super due diligence."

Daniel Gutierrez, a Miami-based compliance officer and chair for the anti-money laundering compliance committee for the Florida International Bankers Association (FIBA).[7]

There are some key tools that will ensure a nimble and immediate response to a changing sanctions landscape and empower organizations to avoid any breach in compliance. These include access to complete and trusted data, tools to pinpoint any relevant entities affected by the most recent sanctions and access to the level of 'super due diligence' that may be needed in cases of heightened risk.

Ernst Pienaar
Head of Content Specialists at World-Check

Ernst Pienaar is the Head of Content Specialists at World-Check and is responsible for all risk data inclusion policies, legal matters and knowledge management within World-Check. Ernst also acts as the lead Content Professional for the World-Check product for client and regulator engagements as it relates to international sanctions, law and regulatory enforcement matters, politically exposed persons compliance and financial and related crime screening.

He is the former Global Head of Research for Financial Crime and Reputational Risk activities at World-Check. In this capacity he was responsible for the management of the then five global World-Check Research centers (Santiago, Washington DC, Cape Town, Singapore and Penang) tasked with the creation and update of the World-Check and related risk databases for over 245 countries and territories in over 65 local languages. He assumed responsibility for managing the World-Check global research team in 2009. Pienaar joined World-Check in 2009 from the Sanlam Life Group in South Africa where, over a ten year period, he was the Head of Forensic Investigations and Group Money Laundering Reporting Officer. Previously he was a Senior State Advocate with South Africa's Office for Serious Economic Offences, and began his career as a State Prosecutor in Johannesburg. He holds a Master's Degree in Constitutional Law and LLB and B.lur law degrees.

7 TRRI article: U.S. banks preparing 'super due diligence' in wake of new Venezuela sanctions. Published 31-Jan-2019 by Brett Wolf, Regulatory Intelligence, Reuters and Accelus News

Visit **refinitiv.com**

RE1033840/9-19

FinCEN expounds on virtual currency risk, obligations

SARs and due diligence are cited as effective tools for avoiding virtual currency malfeasance, says FinCEN. **Jaclyn Jaeger** reports.

In April 2019, the Financial Crimes Enforcement Network (FinCEN) assessed a civil money penalty for willful violations of the Bank Secrecy Act's registration, program, and reporting requirements.

The money services business, which operated as a peer-to-peer exchanger of convertible virtual currency, had no written policies or procedures for ensuring compliance with the BSA and failed to report suspicious transactions and currency transactions.

FinCEN then added guidance and clarification to its regulatory framework for virtual currencies and "provide regulatory certainty for businesses and individuals engaged in expanding fields of financial activity."

The guidance, it says, is in response to questions raised by financial institutions, law enforcement, and regulators concerning the regulatory treatment of multiple variations of businesses dealing in convertible virtual currencies (CVCs).

It also issued an "Advisory on Illicit Activity Involving Convertible Virtual Currency" to assist financial institutions in identifying and reporting suspicious activity related to criminal exploitation of CVCs for

money laundering, sanctions evasion, and other illicit financing purposes. It highlights prominent typologies, associated "red flags," and identifies information that would be most valuable to law enforcement if contained in suspicious activity reports (SARs).

"FinCEN was the first financial regulator to address virtual currency and the first to assign obligations to related businesses to guard against financial crime," said FinCEN Director Kenneth Blanco. "Our regulatory approach has been consistent and despite dynamic waves of new financial technologies, products, and services, our original concepts continue to hold true. Simply stated, those who accept and transfer value, by any means, must comply with our regulations and the criminal misuse of any methodology remains our fundamental concern."

The guidance does not establish any new regulatory expectations. Rather, it consolidates current FinCEN regulations, guidance, and administrative rulings that relate to money transmission involving virtual currency and applies the same interpretive criteria to other common business models.

FinCEN's rules define certain businesses or individuals involved with CVCs as money transmitters subject to the same registration requirements and a range of anti-money laundering, program, recordkeeping, and reporting responsibilities as other money services businesses.

Highlights on the compliance advisory include:

» "Virtual currencies, particularly CVCs, are increasingly used as alternatives to traditional payment and money transmission systems. As with other payment and money transmission methods, financial institutions should carefully assess and mitigate any potential money laundering, terrorist financing, and other illicit financing risks associated with CVCs.
» "The risks posed by CVCs may create illicit finance vulnerabilities due to the global nature, distributed structure, limited transparency, and speed of the most widely utilized virtual currency systems.
» "New types of anonymity-enhanced CVCs have emerged that further reduce the transparency of transactions and identities as well as obscure the source of the CVC through the incorporation of anonymizing features, such as mixing and cryptographic enhancements.

"Some CVCs appear to be designed with the express purpose of circumventing anti-money laundering/countering the financing of terrorism (AML/CFT) controls. All of these factors increase the difficulty for law enforcement and other national security agencies' efforts to combat money laundering, terrorist financing, and other financial crimes facilitated through CVCs.

» A financial institution that fails to comply with its AML/CFT program, recordkeeping and reporting obligations, as well as other regulatory obligations, such as those administered by the Office of Foreign Assets Control (OFAC), risks exposing the financial system to greater illicit finance risks. This is particularly true among unregistered MSBs that may be attempting to evade supervision and fail to implement appropriate controls to prevent their services from being leveraged in money laundering, terrorist financing, and other related illicit activities.
» According to FinCEN's analysis of BSA and other data, illicit actors have used CVCs to facilitate criminal activity such as human trafficking, child exploitation, fraud, extortion, cyber-crime, drug trafficking, money laundering, terrorist financing, and to support rogue regimes and facilitate sanctions evasion."

"Of particular concern is that CVC has come to be one of the principal payment and money transmission methods used in online darknet marketplaces that facilitate the cyber-crime economy.

» Mixing or tumbling involves the use of mechanisms to break the connection between an address sending CVC and the addresses receiving

CVC. The use of CVC in conjunction with darknet market activity may indicate drug purchases or sales, child exploitation, cyber-crime, or other criminal activity. Accordingly, detectable darknet marketplace linkages, such as through a customer's online behavior, may indicate CVC use in support of illicit activity.

» Entities facilitating the transmission of CVCs are required to register with FinCEN as an MSB. If such an entity has not registered with FinCEN, it may be operating illegally as an unregistered MSB.

» Foreign-located MSBs seeking to avoid regulatory coverage generally choose to operate in jurisdictions that lack or have limited AML/CFT laws governing the use of CVC. These foreign-located MSBs often do not comply with the AML/CFT regime of the United States, despite doing business wholly or in substantial part within the U.S."

"CVC kiosks are ATM-like devices or electronic terminals that allow users to exchange cash and virtual currency. CVC kiosks generally facilitate money transmission between a CVC exchange and a customer's wallet or operate as a CVC exchange themselves. While some operators have registered and implemented AML/CFT controls, other kiosks have operated in ways that suggest a willful effort to evade BSA mandates.

» Some kiosk operators have assisted in structuring transactions, failed to collect and retain required customer identification information, or falsely represented the nature of their business—for instance by claiming involvement in cash-intensive activities—to their CVC exchange and depository institutions.

» When evaluating potential suspicious activity, institutions should be mindful that some red flags might be more readily observable during general transactional screening, while others may be more readily observable during transaction- specific reviews.

» Because some red flags associated with abuse of CVC may reflect legitimate financial activities, financial institutions should evaluate indicators of potential CVC misuse in combination with other red flags and the expected transaction activity before determining that a particular transaction is suspicious. Due to the technical nature of blockchain analysis and other frameworks of analyzing CVC activity, FinCEN encourages communication within financial institutions among AML, fraud, and information technology."

When filing SARs, financial institutions should provide all pertinent available information in the SAR form and narrative, the guidance says. The following information is particularly helpful to law enforcement: virtual currency wallet addresses; account information; transaction details (including virtual currency transaction hash and information on the originator and the recipient); relevant transaction history; available login information (including IP addresses); mobile device information; and information obtained from analysis of the customer's public online profile and communications.

FinCEN urges communication among financial firms in determining transactions' potential suspiciousness related to terrorist financing or money laundering activities and in filing SARs, as appropriate.

The advisory also notes that Office of Foreign Assets Control sanctions rules include not only screening against its Specially Designated Nationals (SDN) list, but also undertaking appropriate steps to prohibit persons in sanctioned countries and jurisdictions from opening accounts and trading in digital currency.

Businesses and entities dealing in digital currency should implement policies and procedures that allow them to: block IP addresses associated with a sanctioned country or region; disable the accounts of all holders identified from a sanctioned country or region; install a dedicated compliance officer with authority to ensure compliance with all OFAC-administered sanctions programs; screen all prospective users to ensure they are not from geographic regions subject to U.S. sanctions; and ensure OFAC compliance training for all relevant personnel. ■

FedEx sues Feds over export control burdens related to Huawei dispute

Shipping giant FedEx is suing the federal government in an effort to reverse what it says are impossible-to-achieve compliance burdens imposed by the Department of Commerce. **Joe Mont** has more.

Shipping giant FedEx is suing the federal government in an effort to reverse what it says are unreasonable—if not impossible to adhere to—compliance burdens imposed by the Department of Commerce.

The lawsuit comes on the heels of the Commerce Department's May 2019 addition of controversial Chinese telecom giant Huawei to a list of targeted entities and restricted exports. FedEx and Huawei have subsequently battled over what the latter claims are illegally undelivered shipments.

The Memphis-based company is suing the Commerce Department, Secretary of Commerce Wilbur Ross, and the agency's Bureau of Industry and Security (BIS) in U.S. District Court in the District of Columbia for "injunctive relief to secure its constitutional due process and other rights which are imminently threatened."

The lawsuit claims it's "virtually impossible" for package delivery companies like FedEx to police the content of each and every package it handles.

As a common carrier, FedEx is subject to a variety of statutory and regulatory regimes, among them the Export Control Reform Act of 2018 (ECRA) and its implementing regulations, the Export Administration Regulations (EAR).

The EAR, enforced by the BIS, sets out the United States Government's principal export control regime, restricting the international transfer of certain commodities, technology, information, and software for reasons of national security and foreign policy.

To meet these requirements, FedEx, in the lawsuit, says it "has developed a sophisticated proprietary risk-based compliance system to perform such screening and takes seriously its responsibility to comply with the law."

"However, the Export Controls—specifically, the EAR—require considerably more screening than possible from common carriers like FedEx," the lawsuit claims.

The determination of whether the tendered package contains an "item subject to the EAR" and whether a license is required "are virtually impossible for common carriers to comply with" the company adds.

Typically, the law offers protection for common carriers, excepting them from liability for the contents of packages and communications they transmit, such as internet service providers and telecommunications companies. The EAR, however, defines common carriers such as FedEx as "forwarding agents" and offers no safe harbor provisions. To the contrary, it holds common carriers liable "as aiders and abettors" of EAR violations committed by their customers, with steep penalties.

"Thus, the EAR essentially deputize FedEx to police the contents of the millions of packages it ships daily even though doing so is a virtually impossible task, logistically, economically and, in many cases, legally. Indeed, the majority of transactions begin with the customer providing FedEx with a previously sealed package," the lawsuit says.

To put the business hazard and complexity of

such screening in perspective and scope, FedEx provided a glimpse into its extensive operations. The company receives approximately 15 million packages for shipment daily. To support its operations, it has developed a complex logistics system consisting of over 450,000 team members, 679 aircraft, 650 airports, 39 ground hubs, 600 ground facilities, and 180,000 motorized vehicles spanning more than 220 countries and territories.

Without a safe harbor, the EAR provides FedEx "just two options," the company says: continue to operate under threat of imminent enforcement actions or cease operations that may conceivably lead to enforcement and face possible legal consequences from customers and foreign governments.

"The Due Process Clause of the Fifth Amendment to the U.S. Constitution was enacted to prevent such oppression and deprivations of liberty," it argued.

Tough demands, stiff penalties

The ECRA requires strict compliance with the EAR, and the BIS may impose civil penalties for each individual violation.

Specifically, the ECRA imposes criminal penalties of up to $1 million and civil penalties of $300,000 or twice the value of the transaction per individual violation.

The lawsuit outlines additional burdens faced by FedEx by the export control regime.

"The EAR effectively forces FedEx to police the content of its packages in a manner it is not able to do," it wrote. "Even if FedEx were to inspect the contents of every package for reexport that it delivers, the company would not have enough information to make highly technical determinations to assess whether an item outside the U.S. is an 'item subject to the EAR.' "

FedEx also argues that the BIS Entity List imposes "an overbroad, disproportionate burden." As for government guidance, the shipping company says it is lacking.

"The only way for FedEx to even attempt to avoid inadvertently violating [prohibitions] would be to inspect the contents of every package tendered for shipment. Alternatively, FedEx would have to cease shipping to listed entities in any of the more than 200 foreign jurisdictions on the Commerce Country Chart, which would make it unable to operate as a common carrier," the company says.

Past violations

FedEx is currently operating under a settlement agreement with the BIS, entered into in April 2018. The BIS alleged FedEx committed 53 violations of the EAR. Specifically, that it "caused, aided or abetted acts prohibited by the EAR" when it transported "items subject to the [rules] valued in total at approximately $58,091, from the U.S. to France, or Pakistan, without the required BIS licenses."

The agreement required FedEx to pay a civil penalty of $500,000, plus interest. It was also required to "complete external audits of its export controls compliance program" covering fiscal years 2017-2020.

FedEx must report to the BIS where these audits "identify actual or potential violations of the regulations."

The settlement agreement further provides that "if FedEx should fail to ... complete any of the audits and submit the results in a full and timely manner, [the BIS] may issue an order denying all of FedEx's export privileges under the [EAR] for a period of one year." ■

"The Due Process Clause of the Fifth Amendment to the U.S. Constitution was enacted to prevent such oppression and deprivations of liberty."

FedEx

Industries are responding to U.S.-China trade war

While the escalating trade war and increasing tariff rate hikes between the United States and China can't be controlled, proactive firms are learning to swing with the punches, writes **Jaclyn Jaeger**.

According to two recent surveys, the U.S.-China trade war at a high level has raised costs, resulted in lost sales, and hindered many companies' operations in China. In one survey, conducted by the American Chamber of Commerce in China (AmCham China), 75 percent of 250 member companies said the increases in U.S. and Chinese tariffs are negatively impacting their businesses. They cited as their top three concerns decreased demand for products (52 percent), higher manufacturing costs (42 percent), and higher sales prices for products (38 percent).

In a separate survey, conducted by the U.S.-China Business Council (USCBC), 49 percent said they lost sales due to tariffs implemented by China, while 33 percent said they lost sales due to tariffs implemented by the United States. Moreover, 37 percent said they lost sales in China due to Chinese partners' concerns about doing business with U.S. companies.

When asked how tariffs are impacting their business strategies directly, 35 percent of respondents in the AmCham China survey said they're adopting an "In China, for China" strategy by localizing manufacturing and sourcing within China to mainly serve the China market, while 33 percent said they are delaying or canceling investment decisions. Others said they are adjusting their supply chain by seeking to source components and/or assembly outside the United States (25 percent) or outside of China (23 percent).

Both surveys also point to increased scrutiny by Chinese regulators as a result of the tariffs. In the USCBC survey, 33 percent reported being subject to increased scrutiny from Chinese regulators. In the

AmCham China survey, 20 percent of respondents said they've experienced increased inspections or slower customs clearance, while 14 percent reported experiencing slower approval for licenses or other applications.

Risk mitigation strategies

Despite the President's urging to cease operations in China, many U.S. companies indicated they have no plans to do so. In the AmCham China survey, for example, 60 percent said they have no plans to relocate manufacturing facilities. In the USCBC survey, 87 percent of companies said they, too, have no intention to pull out of China, and a further 66 percent of firms said they were optimistic about their business prospects in the country.

Nike is a prime example. "We are and remain a brand of China and for China," Nike CEO Mark Parker said in a June 27 earnings call. "Nike is proud of the investments we've made and the relationships we've developed in energizing this marketplace. We're confident that we will continue to grow sport and our business in China for decades to come."

Apple is another example of a company inextricably tied to China, and so it's little surprise that when asked in a July 30 earnings call whether the company was looking at or considering potential alternatives in moving parts of its production out of China, CEO Tim Cook basically dismissed the idea. "I know there's been a lot of speculation around the topic of different moves and so forth. I wouldn't put a lot of stock into those," he said. "The way that I view this is the vast majority of our products are kind of made everywhere. There is a significant level of content in the United States and a lot from Japan to Korea to China, and the European Union also contributes a fair amount. That's the nature of a global supply chain."

In numerous other earnings calls over the last two months, however, other executives have said they are, in fact, looking to diversify their supply chains. "As we reach scale with key vendors, we will have stronger partnerships, a greater control over product quality, and the ability to achieve better terms and lower cost. We also continue on a fast track to reduce our exposure in China," Bonnie Brooks, CEO of retail company Chico's, said in an Aug. 28 earnings call.

On a broader scale, according to the AmCham China survey, among those who said they're moving manufacturing out of China, the top three regions mentioned were Southeast Asia (24.7 percent), Mexico (10.5 percent), and the Indian Subcontinent of India, Bangladesh, Pakistan, and Sri Lanka (8.4 percent).

At Chico's, for example, Brooks said that, "Over the next 18 months, we anticipate we will be in the low 30 percent range compared to our current penetration of approximately 40 percent as we shift more of our sourcing to Vietnam, Indonesia, and India."

Significant shifts are happening within global supply chains, as well. "I would say, on the margin, I'm not aware of a single supplier who is not moving some form of manufacturing outside of China," Ted Decker, executive vice president of merchandising at Home Depot, said in an Aug. 20 earnings call. "We have suppliers moving production to Taiwan, to Vietnam, to Thailand, Indonesia, and even back into the United States."

Other companies are taking a middle-of-the-road approach. Toy company Hasbro, for example, is increasingly spreading its footprint and adding new geographies for production globally. "That includes new production in India and Vietnam," Brian Goldner, vice president of investor relations, said in a July 23 earnings call. "Having said all that, we also want to reaffirm that China continues to be a high-quality, low-cost place to make toys and games, and it will continue to be part of our global network in a major way."

As the trade war continues, companies that are thinking proactively generally practice the following risk mitigation strategies: Maintain ongoing communication with suppliers; gather relevant trade data from both internal and government sources to assess trade activity and potential duties costs; map import activity; consider where adjustments can be made in the supply chain; and reevaluate current product-pricing strategies. ■

Treasury issues Violation to State Street subsidiary

The Treasury Department says State Street Bank and Trust violated Iranian Transactions and Sanctions rules. **Jaclyn Jaeger** explores.

The Department of the Treasury's Office of Foreign Assets Control on May 28, 2019, issued a "Finding of Violation" to State Street Bank and Trust for violations of the Iranian Transactions and Sanctions Regulations. There is no monetary penalty.

Between 2012, and 2015, State Street Bank and Trust (SSBT) acted as trustee for a customer's employee retirement plan. SSBT processed at least 45 pension payments totaling $11,365.44 to a plan participant who was a U.S. citizen with a U.S. bank account, but who was a resident in Iran, according to OFAC.

"SSBT appears to have known that it was sending payments to account at the request of or for the benefit of a person in Iran, not only because its internal system indicated the beneficiary's address was located in Tehran, Iran, but also because the bank's sanctions screening software produced an alert on each of the 45 payments due to the Iranian address," OFAC said.

"SSBT's personnel overseeing the beneficiary payments, the Retiree Services Staff (RSS), were part of the SSBT business unit that had the business relationship with the retirement plan and utilized their own sanctions screening filter instead of SSBT's centralized sanctions screening system," OFAC said.

"Furthermore, the routine escalation procedures for the RSS staff dictated that they refer possible sanctions list matches to SSBT compliance personnel aligned with the line of business (i.e., compliance individuals who were not sanctions specialists), rather than SSBT's central sanctions compliance unit staff who have specialized sanctions expertise," OFAC said. "Accordingly, it was the business-aligned compliance personnel who were responsible for manually reviewing potential matches and approving the processing of the payments."

SSBT in 2015 "modified its process to ensure that all RSS payments are now screened by its central screening platform, eliminating disparities in the initial review process, and that alerts with a sanctions nexus are handled through its central alert dispositioning process, which includes escalation to SSBT's central sanctions compliance unit for potential true hits," the Treasury Department said.

OFAC has determined that the conduct constitutes violations of the prohibition against "the exportation, re-exportation, sale, or supply of services ... performed on behalf of a person in Iran" as set forth in sections 560.204 and 560.410 of the Iranian Transactions and Sanctions Regulations. OFAC said a Finding of Violation is appropriate given that SSBT:

- Processed transactions on behalf of an individual in Iran after being alerted to the Iran connection, and thus SSBT reasonably should have been put on notice that the conduct constituted a violation of U.S. law;
- Had actual knowledge that it was processing transactions on behalf of an individual who was a resident in Iran, as SSBT stopped, escalated, reviewed, and approved every one of the 45 distribution payments, each of which contained an explicit reference to Iran;
- Caused harm to the sanctions program objectives and the integrity of the ITSR by performing a service on behalf of an individual in Iran;
- Is a large and commercially sophisticated financial institution;
- Had escalation and review procedures for sanctions-related alerts that nonetheless failed to lead to correct decisions on 45 occasions; and
- Had compliance screening issues that continued for a year after the Federal Reserve Bank of Boston notified the bank of a related issue pertaining to inadequate escalation procedures.

SSBT has cooperated fully with OFAC's probe. ■

World-Check®

Uncover risk. Take action.

A powerful combination of data, technology and trusted human expertise to help:

- Simplify and accelerate risk screening
- Meet regulatory obligations
- Protect against financial crime risk

refinitiv.com/world-check

REFINITIV™

DATA IS JUST
THE BEGINNING™