Paul|Weiss

Economic Sanctions and Anti-Money Laundering Developments

2018 YEAR IN REVIEW

February 5, 2019

February 5, 2019

Economic Sanctions and Anti-Money Laundering Developments: 2018 Year in Review

Table of Contents

Executive Summary

This memorandum surveys economic sanctions and anti-money laundering ("AML") developments and trends in 2018 and provides an outlook for the year ahead. These areas remained a high priority last year, with the Trump administration making major changes in U.S. sanctions policy and federal and state agencies imposing over $2.7 billion in penalties for sanctions/AML violations. We also provide some thoughts concerning compliance and risk mitigation in this challenging environment.

After a period of relative quiet on the sanctions enforcement front, the last months of 2018 saw a $1.3 billion multi-agency resolution with Société Générale S.A., a burst of enforcement actions by Treasury's Office of Foreign Assets Controls ("OFAC"), and Treasury Under Secretary Sigal Mandelker's announcement that OFAC will soon publish guidance on the "hallmarks of an effective sanctions compliance program" and incorporate these principles in future settlements. Last year also witnessed significant and constant changes to the sanctions policy landscape. In a dramatic break from the Obama administration's policy towards Iran, President Trump withdrew the United States from the Joint Comprehensive Plan of Action ("JCPOA") in May 2018, and fully revoked JCPOA-era sanctions relief by November 2018, creating new sanctions risks for U.S. and non-U.S. companies across industries, generating conflict-of-law issues, and

straining relations with U.S. allies. The administration also took a number of significant actions with respect to Russia/Ukraine sanctions, including designating a number of Russian "oligarchs" and their global companies and taking further steps to implement the Russian secondary sanctions regime enacted by Congress in the 2017 Countering America's Adversaries through Sanctions Act ("CAATSA"). The administration also imposed several new sanctions against the Maduro regime in Venezuela (and recently sanctioned Venezuela's national oil company), continued its campaign of "maximum pressure" on North Korea, implemented Global Magnitsky Act sanctions targeting human rights abuses and corruption worldwide, and established new sanctions programs targeting the Nicaraguan regime and non-U.S. interference in U.S. elections.

Enforcement of the Bank Secrecy Act/anti-money laundering ("BSA/AML") laws—or their state analogues—remained a high priority for a panoply of agencies, including the Department of Justice ("DOJ"), Treasury's Financial Crimes Enforcement Network ("FinCEN"), the federal banking agencies, the Securities and Exchange Commission ("SEC"), the Financial Industry Regulatory Authority ("FINRA"), and the New York Department of Financial Services ("DFS"). Last year saw significant multi-agency resolutions against U.S. Bancorp and Rabobank N.A, a series of enforcement actions against broker-dealers (including the first BSA criminal charge against a broker-dealer), and actions by the DFS against Western Union and Mashreqbank.

Agencies also issued a flurry of guidance and advisories, effectively raising expectations for private sector compliance efforts consistent with Under Secretary Mandelker's recent warning that companies "must do more to make sure [their] compliance systems are airtight."[1] This detailed guidance covered a variety of topics, such as recommendations for better identifying North Korea and Iran's sanctions evasion tactics (including identifying supply chain links to North Korea), adopting risk-based approaches to the Financial Action Task Force's ("FATF") identification of jurisdictions with anti-money laundering and combating financial terrorism ("AML/CFT") deficiencies, and strategies for recognizing human rights abuses by corrupt non-U.S. political figures.

Last year, regulators and the private sector also placed increasing focus on several hot topics that will only grow in importance. First, in the area of virtual currencies, OFAC issued additional guidance and announced its inclusion for the first time of digital currency addresses for persons added to its List of Specially Designated Nationals and Blocked Person (the "SDN List"); FinCEN and FATF also signaled increased focus on this area. Second, with the continued state-level cannabis legalization efforts in the United States—and the legalization of recreational cannabis in Canada in October 2018—financial institutions and other companies continued to grapple with the regulatory consequences of different types of engagement with this growing industry. Third, FinCEN and the federal banking agencies issued a joint statement encouraging financial institution innovation in compliance technology, including artificial-intelligence based approaches.[2] Meanwhile, Congress continued to evaluate proposals to modernize and

enhance the BSA, although the prospects for such legislation in the current political environment remain unclear.

Treasury's Office of Foreign Assets Control

Last year saw important changes to various sanctions programs administered by OFAC, particularly the Iran, Russia/Ukraine, Global Magnitsky, North Korea, and Venezuela programs, as described in greater detail below.

Additionally, in November, the Trump administration introduced a new sanctions program targeting the Nicaraguan government for its systematic dismantling and undermining of democratic institutions, its use of indiscriminate violence and repressive tactics against civilians, and its corruption leading to the destabilization of Nicaragua's economy.[3] OFAC also added to the SDN List two of President Ortega's closest associates, the Vice President of Nicaragua and First Lady, Rosario Maria Murillo De Ortega, and Nestor Moncada Lau, who has acted as national security advisor.[4]

In September, President Trump also signed a new executive order targeting interference in U.S. elections.[5] This order establishes an interagency framework for determining whether election interference has occurred and adopts a two-track approach, one for designating non-U.S. persons engaged in election interference and another for adopting broader measures targeting states behind those efforts. The new program's reach is not limited to Russia, and so far it is unclear whether the 2018 mid-term elections will trigger any sanctions under the executive order.

On the enforcement front, after a lull in activity, OFAC issued a spate of enforcement actions in the last part of 2018, resulting in a total of $72 million in civil penalties (including settlements) for the year, compared to $120 million in 2017 and $21 million in 2016. OFAC's seven enforcement actions included its second-ever penalty for violations of its 50 percent rule, which was assessed against a U.S. technology company.[6] Notably, although OFAC has yet to announce a change in its long-standing policy of crediting payments made to other agencies against its fines for the same conduct, the agency did not credit payments to other agencies in two 2018 resolutions. Also, as described further below, in December, Sigal Mandelker, the Under Secretary of the Treasury for Terrorism and Financial Intelligence (who supervises OFAC and FinCEN) announced that OFAC intends to issue guidance in the near-term regarding OFAC's compliance expectations.[7]

In September, Andrea Gacki, a long-serving OFAC employee who had previously served in various capacities, including Acting Director, Deputy Director, and Associate Director of Compliance and Enforcement, was named OFAC Director. Director Gacki had served as Acting Director since May. In November, Bradley Smith was named Deputy Director; he had previously served for five years as OFAC Chief Counsel.

OFAC's Strengthened Approach on Compliance Expectations

At a December conference, Under Secretary Mandelker announced that OFAC intends to issue guidance in the near-term that will outline the "hallmarks of an effective sanctions compliance program." She outlined five areas that will be covered by the guidance: (1) ensuring senior management commitment to compliance; (2) conducting frequent risk assessments to identify and mitigate sanctions-specific risks within an institution and its products, services, and customers; (3) developing and deploying internal controls, including policies and procedures, to identify, interdict, escalate, report, and maintain records pertaining to activity prohibited by OFAC's regulations; (4) engaging in testing and auditing—both on specific elements of a sanctions compliance program and across the organization—to identify and correct weaknesses and deficiencies; and (5) ensuring all relevant personnel, particularly those in high-risk areas or business unites, are provided tailored training on OFAC sanctions in general and the organization's sanctions compliance program in particular. As noted by Under Secretary Mandelker, OFAC has already started incorporating these themes into its recent settlements.[8] She further stated that OFAC's intent in including such language in its settlement agreements is to convey its compliance expectations to the private sector, including its expectation of strict compliance with settlement agreements.

Although OFAC has previously signaled certain compliance expectations in enforcement actions and various FAQs, its forthcoming attempt to outline the hallmarks of an effective OFAC compliance program signals a new approach and one complicated by the fact (as OFAC has repeatedly recognized) that there is no one-size-fits-all approach and that the "right" compliance program much depends on the particular nature of a company's business and risk profile. Further, OFAC's decision to incorporate compliance commitments in its settlement agreements, while bringing OFAC more in line with the approach of other agencies, may raise the price of settling with OFAC and further complicate future settlement discussions.

Changes in OFAC Sanctions Programs

Iran. As detailed in a prior memorandum,[9] on May 8, 2018, President Trump announced the unilateral withdrawal of the United States from the JCPOA. OFAC issued a final rule effective November 5, 2018, that fully reinstated sanctions on Iran that had been suspended during implementation of the JCPOA. OFAC announced that the "United States is engaged in a campaign of maximum financial pressure on the Iranian regime and intends to enforce aggressively these sanctions that have come back into effect."[10]

As of November 5, 2018, all U.S. sanctions that were lifted or waived in connection with the JCPOA have been re-imposed. With respect to primary sanctions, General License H–which had provided sanctions relief pursuant to the JCPOA for non-U.S. companies owned or controlled by U.S. companies conducting business with Iran–was revoked and the associated wind-down period ended November 4, 2018. OFAC also revoked its JCPOA-era authorizations for the importation of certain Iranian-origin carpets and foodstuffs and the export of certain commercial passenger aircraft and related parts and services. Likewise, all secondary sanctions have been re-imposed, including but not limited to those targeting: (1) transactions

by non-U.S. financial institutions with the Central Bank of Iran and other sanctioned Iranian financial institutions (and other sanctions targeting Iran's banking sector); and (2) Iran's energy, automotive, shipping, insurance, gold, and metals sectors. However, under the "significant reduction exception," eight countries that the U.S. Secretary of State determined have significantly reduced their oil imports from Iran can temporarily continue to engage in certain activities, such as buying petroleum and petroleum products from Iran, without risking sanctions.[11] OFAC guidance also provides that non-U.S., non-Iranian persons may continue to receive certain limited payments or repayments after the expiration of the applicable wind-down periods.[12] These allowances are intended to allow non-U.S., non-Iranian persons to be "made whole" for debts and obligations owed or due to them for goods or services fully provided or delivered or loans or credit extended to an Iranian party prior to the conclusion of the applicable wind-down period.

Also effective November 5, OFAC added over 700 Iran-related persons to the SDN List, meaning that non-U.S. persons, including non-U.S. financial institutions, are now threatened with secondary sanctions for knowingly engaging in certain significant transactions with these persons.[13] This 700 includes more than 400 persons OFAC had previously removed from the SDN List to allow non-U.S. persons to conduct business with these persons without the risk of secondary sanctions. Among the persons added to the SDN List on November 5 were 70 Iran-linked financial institutions and their foreign and domestic subsidiaries, many of which OFAC determined have provided support to, or are owned or controlled by, SDNs designated in connection with the Iranian regime's support to international terrorism, proliferation of weapons of mass destruction or their means of delivery, and human rights abuses, and are subject to secondary sanctions.[14]

As of November 5, specialized financial messaging systems like the Society for Worldwide Interbank Financial Telecommunication or SWIFT (the leading international financial messaging service facilitating cross-border payments among financial institutions) are subject to secondary sanctions if they provide services to Iranian banks triggering secondary sanctions (*i.e.*, the Central Bank of Iran or those that are designated in connection with their support of terrorism or the development of weapons of mass destruction). According to Treasury Secretary Steven Mnuchin, the United States advised SWIFT that it must disconnect those Iranian financial institutions as soon as feasible or become subject to U.S. sanctions.[15] SWIFT announced on November 5, 2018, that it would comply, specifying that it was acting based on its commitment to "the stability and integrity of the wider global financial system."[16]

In reaction to the withdrawal of the United States from the JCPOA, the European Commission implemented on August 7, 2018, countermeasures aimed at protecting the interests of EU companies doing business in Iran.[17] The EU Blocking Regulation, as amended, prohibits any "EU operator" (generally, any person or entity residing or incorporated in the EU[18]) from complying, whether directly or indirectly or through a subsidiary or other intermediary person, with certain of the re-imposed U.S. secondary sanctions against Iran; requires EU operators to notify the European Commission of any effects on their economic or financial interests caused by the covered U.S. sanctions on Iran; provides assurance that EU courts will not enforce

U.S. court judgments enforcing such sanctions against EU operators; and entitles EU operators to recover damages caused by the application of the covered U.S. sanctions against Iran.

This results in potential conflict of laws between the United States and the EU that has created uncertainty and risk for EU companies, including EU companies that are owned or controlled by U.S. companies. Although EU operators are able to request an authorization to comply with U.S. sanctions, this procedure has been seldom used since the EU Blocking Regulation was first established in 1996, so the standards for approval are unclear. In addition, although EU Member States are responsible for implementing the EU Blocking Regulation at the national level and imposing penalties, not all Member States have implemented national legislation and enforcement has been quite limited. To date, the new Iran-related prohibitions have not been enforced, and many global firms have opted to respect U.S. sanctions despite the legal risks arising from the EU Blocking Regulation. In an effort to mitigate their potential EU exposure, a number of companies have framed their decision to withdraw from Iran business in terms of broader risk considerations that attend doing business with Iran.

On January 31, 2019, France, Germany, and the United Kingdom announced the creation of a special purpose vehicle, the Instrument in Support of Trade Exchanges ("INSTEX").[19] INSTEX will serve as a payment channel designed to allow EU companies can conduct trade in humanitarian goods with Iran. While such humanitarian trade is generally authorized by OFAC, creation of INSTEX demonstrates the EU's commitment to maintaining the JCPOA.[20] If INSTEX were to broaden its scope beyond humanitarian transaction, that could trigger U.S. sanctions.

Russia/Ukraine Sanctions. The conventional wisdom at the start of 2018 was that President Trump would resist expansion of U.S. sanctions against Russia. Various factors, however, including pressure from Congress and international outrage over Russia's use of chemical weapons in the U.K., prompted the Trump administration to take tough actions towards Russia, including by implementing certain parts of the Countering America's Adversaries Through Sanctions Act ("CAATSA"). The result has been new risks and uncertainties for companies engaged in Russia-related business.

In January 2018, the Treasury Department submitted a report to Congress pursuant to Section 241 of CAATSA on Russian oligarchs, senior political figures, and parastatal entities.[21] As detailed in our prior memorandum,[22] on April 6, 2018, OFAC designated seven "oligarchs" listed in the January report, as well as twelve companies they owned or controlled, some of which are publicly traded companies with significant international operations.[23] This inclusion of wealthy businessmen and large companies with extensive Western financial ties on the SDN List was a significant action felt throughout the global economy. At the same time, the administration lessened the impact of the designations on U.S. persons and U.S. allies via a series of general licenses authorizing certain wind down, maintenance, and divestment activities related to several of the designated entities.

On December 19, OFAC notified Congressional leaders of OFAC's intent to terminate sanctions against three companies designated for being owned or controlled by one of the designated oligarchs, Oleg Deripaska: En+ Group plc, UC Rusal plc, and JSC EuroSibEnergo.[24] According to OFAC, the three companies have agreed to undertake significant restructuring and corporate governance changes to address the circumstances that led to their designation, including reducing Deripaska's direct and indirect shareholding in those entities to below 50 percent; overhauling the composition of their boards of directors; taking restrictive steps related to their corporate governance; and agreeing to ongoing auditing, certification, and reporting requirements. OFAC has also extended the general licenses until March 7, 2019 authorizing certain transactions involving a fourth designated entity (Gaz Group) owned or controlled by Deripaska, suggesting that OFAC is in ongoing communications with this entity regarding similar restructuring and governance changes that could warrant delisting.[25] Despite substantial bipartisan opposition to the Administration's actions, Congress's efforts to pass legislation that would halt the delisting of En+ Group plc, UC Rusal plc, and JSC EuroSibEnergo stalled in the Senate and OFAC's delisting proceeded on January 27, 2019.

All told, OFAC made over 140 Russia-related designations in 2018 (including the oligarch-related designations described above), related, among other things, to attempted interference in the 2016 U.S. election, efforts to undermine international organizations through cyber-attacks, and Russia's ongoing occupation of Crimea.[26]

Two of these designations marked the first time the U.S. government imposed secondary sanctions under Section 231 of CAATSA. OFAC designated China's Equipment Development Department ("EDD"), a branch of the Chinese military, and its director, Li Shangfu, pursuant to Section 231 of CAATSA, which mandates the imposition of sanctions upon anyone engaging in a "significant transaction" with any entity that appears on a list of persons associated with the Russian defense or intelligence sectors.[27] The U.S. government determined that EDD and Mr. Li negotiated deals with Rosoboronexport, which is Russia's main arms export entity. This deal involved the receipt by China of 10 Sukhoi fighter aircraft and a batch of S-400 surface-to-air missile systems or related equipment from Rosoboronexport after Section 231 came into force. Notably, the deals were signed prior to the enactment of CAATSA. EDD and Mr. Li were also added to the State Department's CAATSA section 231 List of Specified Persons for being a part of, or operating for or on behalf of, the defense or intelligence sectors of the Government of the Russian Federation.[28]

Separately, on August 6, 2018, the U.S. State Department invoked the Chemical and Biological Weapons Control and Warfare Elimination Act of 1991 ("CBW") following Russia's use of a "Novichok" nerve agent in an attempted assassination of former Russian spy Sergei Skripal and his daughter Yulia in the United Kingdom. The CBW determination[29] triggered "initial sanctions" on August 27 that relate to the sales and financing of arms sales, extending U.S government credit to the Russian government, and exporting national security-sensitive goods and technology.[30] The Trump administration opted to waive certain other initial sanctions authorized by the CBW. On December 19, the Department of State added twelve

individuals and entities to the List of Specified Persons under Section 231 of CAATSA for being part of, or operating for or on behalf of, the defense or intelligence sector of the Russian Federation.[31] The State Department explained that the December 19 listings were made in response to Russian intelligence services' cyber operations and "use of a military grade nerve agent to carry out an assassination attempt inside the borders of our closest ally, a violation of Russia's obligations under the Chemical Weapons Convention."[32]

North Korea. North Korea remained a focus for both the Trump administration and Congress in 2018. While the United States continued to increase sanctions against North Korea, adding 123 individuals and entities to the SDN List—including designations targeting the country's shipping and trading companies and vessels, arms, oil, and luxury goods trade, money laundering in support of North Korea, and designations in response to cyber-attacks, human rights abuses, and censorship—the Trump administration also took historic steps to engage with the North Korean regime. Specifically, in the first ever meeting between leaders of the United States and North Korea, President Trump and North Korean Supreme Leader Kim Jong-un met in Singapore on June 12, 2018, and signed a document establishing, in broad terms, that the United States will normalize relations with North Korea in exchange for the denuclearization of the Korean Peninsula. The document does not specify a process for implementation of these terms, and while the Trump administration has maintained that North Korea must denuclearize before sanctions will be lifted, North Korea has asserted that the denuclearization process must be linked to a gradual removal of U.S. sanctions. Accordingly, the impact of this meeting remains unclear, and the Trump administration "continue[d] to push for maximum pressure on nefarious actors" by imposing new sanctions against North Korea in the second half of 2018.[33]

The sophistication of the North Korean regime in using front companies poses unique compliance challenges. Among other things, the Trump administration has emphasized the need for banks (and especially Chinese banks) to bolster their efforts at identifying and shutting down North Korea-related activity. Treasury Assistant Secretary for Terrorist Financing Marshall Billingslea testified twice before Congress in September 2018, during which he was questioned about why the United States has only sanctioned small Chinese banks (such as the Bank of Dandong and Banco Delta Asia) for conducting business with North Korea, but has not been tougher on large institutions. Assistant Secretary Billingslea responded that "no bank is too big for us to sanction if we determine it is in our national security interest to do so…we are working with a number of the very large banks to ensure that they are aware of and taking action against accounts that we believe are associated with North Korean front companies."[34]

Additionally, OFAC and other agencies issued detailed guidance to the private sector on certain sanctions and other risks posed by North Korea:

- *North Korean Deceptive Shipping Practices*. OFAC, the U.S. Department of State, and the U.S. Coast Guard, issued an advisory on February 23, 2018, regarding the deceptive shipping practices used by North Korea to evade sanctions. The advisory lists examples of the type of tactics used by North Korea to obfuscate the identity of the vessels, the goods being shipped, and the origin or destination of cargo,

such as: physically altering vessel identification; ship-to-ship transfers; falsifying cargo and vessel documents; disabling automatic identification systems ("AIS"), and manipulating data being transmitted by AIS.[35] The advisory stresses the significant sanctions risk for parties involved in the shipping industry. It recommends measures such as monitoring for AIS manipulation, conducting appropriate due diligence prior to engaging in ship-to-ship transfers, reviewing all applicable shipping documentation, ensuring clear communication with international partners, and leveraging all available resources for due diligence.

- *Supply Chain Links to North Korea*. OFAC, the Department of State, and the Department of Homeland Security's (DHS) Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE), issued a joint advisory on July 23, 2018, highlighting risks for businesses with supply chain links to North Korea.[36] The advisory describes the agencies' expectation that businesses be aware of the deceptive practices employed by North Korea in order to implement effective due diligence policies, procedures, and internal controls to ensure compliance with applicable legal requirements across their entire supply chains. The advisory identifies two primary areas of risk: (1) inadvertent sourcing of goods, services, or technology from North Korea; and (2) the presence of North Korea citizens or nationals in companies' supply chains, whose labor generates revenue for the North Korean government. The agencies identify indicia of North Korean labor (including sectors and high-risk jurisdictions) and provide a list of joint ventures known to be operating in or to have previously operated in North Korea. Companies may consider adding these joint ventures to their screening programs.

Venezuela. In response to ongoing human rights abuses and corruption in Venezuela, President Trump issued a series of executive orders in 2018 and early 2019 that have significantly increased sanctions pressure on the Venezuelan government, including the imposition of restrictions on transactions related to Venezuelan cryptocurrencies and on efforts by the Venezuelan government to raise money by selling or otherwise transferring assets.

On March 19, 2018, after the Maduro regime launched a cryptocurrency known as the "petro" in an effort to circumvent sanctions, President Trump issued E.O. 13827, which prohibits U.S.-nexus transactions in any Venezuelan "digital currency, digital coin, or digital token."[37]

On May 21, 2018, in response to the reelection of Venezuelan President Maduro, President Trump issued E.O. 13835, which prohibits transactions with a U.S. nexus related to dealings in: (1) the purchase of any debt owed to the Venezuelan Government, including accounts receivable; (2) any debt owed to the Venezuelan Government that is pledged as collateral after May 21, 2018, including accounts receivable; and (3) the sale, transfer, assignment, or pledging of collateral by the Venezuelan Government of any equity interest in which the Venezuelan Government has a 50 percent or greater ownership interest.[38] Notably, OFAC did not issue a general license that exempts transactions relating to U.S.-based CITGO Holding, Inc. ("Citgo") and its subsidiaries from the prohibitions of E.O. 13835. On July 19, 2018, OFAC issued General

License 5 to authorize U.S. persons to engage in all transactions related to dealings in the Petróleos de Venezuela S.A. ("PDVSA") 2020 8.5 Percent Bond that would otherwise be prohibited by E.O. 13835 (including efforts to exercise security interests associated with this debt), but it has not issued a similar authorization for other bonds.[39]

The Trump administration made 25 Venezuela-related designations in 2018, including a number of high-ranking current and former government and military officials, members of Maduro's inner circle (such as his wife Celia Flores and Executive Vice President Delcy Rodriguez), and affiliates of the aforementioned individuals.[40] Given the large number of government official designations, OFAC issued guidance stating that, while the "designation of an official of the Government of Venezuela does not mean that the government itself is also blocked . . . U.S. persons should be cautious in dealings with the government to ensure that they are not engaged in transactions or dealings, directly or indirectly, with an SDN."[41]

On November 1, 2018, President Trump issued E.O. 13850, authorizing sanctions against any person determined by the Treasury Secretary and Secretary of State to operate in the Venezuelan gold sector, or other sectors of the Venezuelan economy, and to be responsible or complicit in transactions involving deceptive practices or corruption in Venezuela.[42] In a speech discussing the new sanctions, National Security Advisor John Bolton stated: "The new sanctions will target networks operating within corrupt Venezuelan economic sectors and deny them access to stolen wealth."[43]

On January 23, 2019, the United States recognized Maduro opposition leader and Venezuelan National Assembly President Juan Guaidó as the Interim President of Venezuela.[44] Less than a week later the Trump administration determined that persons operating in Venezuela's oil sector are subject to sanctions pursuant to E.O. 13850 and designated PDVSA for operating in the oil sector of the Venezuelan economy.[45] OFAC issued nine general licenses in connection with this action, including certain authorizations for transactions with U.S.-based PDV Holding Inc. and Citgo, and certain maintenance and wind down activities with PDVSA.[46] Treasury Secretary Mnuchin stated that this designation will help prevent further diverting of Venezuela's assets by Maduro and preserve these assets for the people of Venezuela. The path to sanctions relief for PDVSA is through the expeditious transfer of control to the Interim President or a subsequent, democratically elected government."[47] The same day, President Trump issued a second executive order revising the definition of "Government of Venezuela" in all prior Venezuela sanctions-related executive orders to include "the Central Bank of Venezuela and [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."[48]

Global Magnitsky Sanctions. On December 20, 2017, President Trump issued an executive order implementing the Global Magnitsky Human Rights Accountability Act, which authorized the imposition of sanctions against human rights abusers and those who facilitate government corruption anywhere in the world, as well as persons who materially assist or support such activities.[49] Between December 2017 and December 2018, OFAC designated 101 individuals and entities from over twenty countries pursuant to this

new sanctions program, a number of whom have been connected to DOJ and SEC Foreign Corrupt Practices Act enforcement actions, and including a number of high profile individuals and wealthy business persons.[50]

The Global Magnitsky program allows for the sanctioning of individuals and entities without the wholesale targeting of a particular regime. For example, the U.S. government has designated seventeen individuals for serious human rights abuse relating to their roles in the killing of American journalist Jamal Khashoggi at the Consulate of Saudi Arabia in Istanbul, while largely retaining friendly relations with Saudi Arabia.

Given the broad designation criteria and global reach of the Global Magnitsky sanctions program, companies conducting international business would be well served to recalibrate their due diligence practices regarding counterparties and business partners to account for human rights abuses and corruption.

OFAC Enforcement Actions

OFAC's 2018 enforcement actions highlight the agency's broad jurisdictional reach as well as its continued focus on non-financial companies. OFAC also continued to make use of Findings of Violation – public enforcement actions that involve no assessment of a monetary penalty. We outline some of the more significant aspects of these enforcement actions below.

Société Générale S.A. On November 19, 2018, OFAC settled 1,077 apparent[51] violations of Cuba, Iran, and Sudan sanctions with Société Générale ("SocGen") for over $53 million dollars.[52] This was part of a broader $1.3 billion resolution with DOJ, the Federal Reserve, and the DFS. According to the settlement agreement, for a period of at least five years up to and including 2012, SocGen processed transactions through the United States that involved sanctioned countries or persons in a manner that "removed, omitted, obscured, or otherwise failed to include references to OFAC-sanctioned parties in the information sent to the U.S. financial institutions that were involved in the transactions." OFAC characterized the apparent violations as egregious. Notably, OFAC did not follow its historic practice of deeming its penalty satisfied by payments to other agencies. OFAC's settlement with SocGen also includes a representation that SocGen has terminated the violative conduct and "has established, and agrees to maintain, policies and procedures that prohibit, and are designed to minimize the risk of the recurrence of similar conduct in the future." Additional information regarding the other agencies' actions against SocGen is provided below.

Cobham Holdings, Inc. As discussed in our prior memorandum,[53] on November 27, 2018, Cobham Holdings, Inc. ("Cobham"), a U.S.-based technology company in the aviation, electronics, communications, and defense sectors, on behalf of its former subsidiary, Aeroflex/Metelics, Inc. ("Metelics"), settled with OFAC apparent violations of Russia/Ukraine sanctions for nearly $90,000.[54] According to OFAC, Metelics made three shipments of goods through distributors in Canada and Russia to an entity that did not appear on the SDN List, but was blocked under OFAC's "50 percent rule" because it was 51% owned by a Russian SDN. This is the second OFAC action of which we are aware that has relied on the 50 percent rule. The

apparent violations appear to have been caused by Metelics's (and Cobham's) reliance on deficient third-party screening software, which used "all word" match criteria and failed to return any matches or warnings for the entity on the SDN List, despite the fact the names of the blocked party and its subsidiary, whose name was run through the program, both contained several of the same uncommon words, and Cobham had selected "fuzzy" search criteria to detect partial matches. While difficult to predict, OFAC's decision to pursue this action in these circumstances—involving only three shipments, a violation of the 50 percent rule, and deficient third-party screening software—may signal a raising of OFAC's compliance expectations. Also, as an indication of OFAC's new approach, OFAC gave more detail than normal about the remedial measures taken by Cobham, which included acquiring and implementing a new tool capable of identifying persons known to be owned by parties on the SDN List; implementing a process of enhanced due diligence for transactions that are high risk from an OFAC perspective; and circulating a "lesson learned bulletin" to all U.S.-based international trade compliance personnel.[55]

Yantai Jereh Oilfield Services Group Co. On December 12, 2018, Chinese entity Yantai Jereh Oilfield Services Group Co. and its worldwide affiliates (the "Jereh Group") agreed to pay OFAC $2,774,972 to settle apparent violations of Iran sanctions.[56] According to OFAC, between October 2014 and March 2016, the Jereh Group exported or reexported on at least eleven occasions U.S.-origin goods, including oilfield equipment, to Iran through China with knowledge that such transactions violated U.S. law. The Jereh Group concurrently settled related export control violations with the Department of Commerce's Bureau of Industry and Security ("BIS") for $600,000; the BIS settlement also imposes and suspends a five year denial period on U.S. exports. OFAC determined the apparent violations were egregious and noted that the Jereh Group did not cease its violative behavior until the Commerce Department added several Jereh Group companies and related individuals to its entity list in March 2016. OFAC also highlighted the remedial actions taken by the Jereh Group, including the retention of a qualified third party to perform an internal review of the company and develop and implement a trade and sanctions compliance program, hiring of a U.S. trained chief legal officer and other persons with experience working at global companies with a commitment to compliance, and requiring its suppliers to make compliance certifications with respect to U.S. laws. These remedial actions, among other compliance commitments, are included as conditions in the settlement agreement. In another deviation from its historic practice, OFAC did not credit the Jereh Group's payments to BIS.

Zoltek Companies, Inc. On December 20, 2018, Zoltek Companies, Inc. ("Zoltek"), a U.S. holding company and owner of U.S.-based Zoltek Corporation ("Zoltek U.S.") settled with OFAC 26 apparent violations of Belarus sanctions for $7,772,102.[57] According to OFAC, Zoltek U.S. approved 26 purchases of acrylonitrile, a chemical used in the production of carbon fiber, between a Hungarian Zoltek subsidiary and a Belarusian designated entity. OFAC determined that some of these violations were egregious and noted that the Hungarian subsidiary's purchase decisions were reviewed and approved by senior level executives of the U.S. subsidiary, including the Chief Executive Office and other senior managers. OFAC noted that Zoltek U.S.'s Chief Operations Officer was questioned as to the impact of sanctions on the transactions at

issue, and multiple U.S. management personnel engaged in discussions regarding sanctions against the Belarusian entity; nonetheless, the U.S. subsidiary continued to review and approve the Hungarian subsidiary's transactions with the sanctioned entity. In its web notice, OFAC stated that this action highlights the need for U.S. companies to avoid facilitating transactions or activities of their non-U.S. affiliates with U.S.-sanctioned countries and persons. As part of the settlement agreement, Zoltek represented that it has terminated the violative conduct and implemented certain compliance commitments designed to minimize the risk of recurrence.

Epsilon Electronics, Inc. On September 13, 2018, U.S.-based Epsilon Electronics, Inc. ("Epsilon") agreed to pay $1,500,000 to settle liability arising from alleged violations of Iran sanctions, resolving a prior penalty notice for $4,073,000 and subsequent litigation.[58] The U.S. Court of Appeals for the District of Columbia concluded that a U.S. exporter may be found liable if it ships goods to a third country with reason to know that those goods are specifically intended for re-export to Iran, even if the goods never arrive in Iran or if OFAC is unable to prove that the goods were re-exported to Iran.[59] "Reason to know" can be established "through a variety of circumstantial evidence," including "course of dealing, general knowledge of the industry or customer preferences, working relationships between the parties, or other criteria far too numerous to enumerate."[60] OFAC determined, based largely on the website of the Dubai-based entity to which Epsilon distributed, that during the majority of the time period at issue, Epsilon knew or had reason to know that the Dubai-based entity sent most, if not all, of its products to Iran.[61] For the final five transactions, which occurred after the Dubai-based entity broadened its distribution area (which transactions OFAC had previously determined to be egregious violations), the Court of Appeals found that the evidence did not meet the "reason to know" standard and remanded the case to the D.C. District Court with instructions to remand to OFAC for recalculation of its penalty. The settlement reflects the outcome of the court challenge: OFAC reversed its initial determination that the five final transactions were egregious and provided greater mitigation credit.

JPMorgan Chase Bank, N.A. and JPMorgan Chase & Co. On October 5, 2018, JPMorgan Chase Bank N.A. ("JPMC") agreed to pay OFAC $5,263,171 to settle apparent violations of Cuba, Iran, and Weapons of Mass Destruction sanctions.[62] JPMC, a U.S. person, operated a net settlement mechanism—that resolved billings among various participants in the airline industry—on behalf of a U.S.-entity client and the client's members, and a non-U.S. entity and its members. According to OFAC, between January 2008 and February 2012, JPMC processed 87 transactions through the net settlement mechanism that may have contained interests attributable to a U.S. sanctioned party. OFAC determined that each such transaction represented a net settlement payment between JPMC's client and the non-U.S. person entity, whose members included eight airlines that were at various times on the SDN List, otherwise blocked pursuant to OFAC sanctions, or located in OFAC sanctioned countries. OFAC also determined that JPMC did not appear to have a process in place to evaluate the OFAC sanctions risk of the members of the non-U.S. entity participating in the net settlement mechanism but did, on two occasions, receive express notifications from its client regarding OFAC sanctioned entities participating in the settlement mechanism.

On the same day, OFAC issued a Finding of Violation to JPMorgan Chase & Co. ("JPMCC") for violations of Foreign Narcotics Kingpin and Syria sanctions.[63] According to OFAC, between August 2011 and April 2014, JPMCC processed 85 transactions and maintained eight accounts on behalf of six customers who were on the SDN list. From 2007 to October 2013, JPMCC employed a vendor screening system that failed to identify these individuals as SDNs despite strong similarities between the accountholder's names, addresses, and dates of birth in JPMCC account documentation and on the SDN list, because the system's screening logic capabilities failed to identify customer names with hyphens, initials, or additional middle or last names as potential matches to similar or identical names on the SDN List. OFAC found that JPMCC identified weaknesses in the system as early as 2010 and implemented a series of improvements between 2010 and 2012. In 2013, JPMCC transitioned to a new screening system and rescreened the records of 188 million clients. The new system identified the 85 transactions and eight accounts and JPMCC reported the same to OFAC. OFAC stressed the "importance of financial institutions remediating known compliance program deficiencies in an expedient manner, and when that is not possible, the importance of implementing compensating controls to mitigate risk until a comprehensive solution can be deployed." OFAC listed as mitigating factors the fact that this was JPMCC's first violation and JPMCC's cooperation with OFAC.

e.l.f. Cosmetics, Inc. As discussed in our prior memorandum,[64] on January 31, 2019, California-based e.l.f. Cosmetics, Inc. ("ELF") agreed to pay OFAC $996,080 to settle apparent violations of North Korea sanctions.[65] According to OFAC, between April 1, 2012 and January 28, 2017, ELF imported 156 shipments of false eyelash kits from two China-based suppliers that contained materials sourced by those suppliers from North Korea. The apparent violations appear to have resulted from ELF's "either non-existent or inadequate" OFAC compliance program.[66] OFAC did not note any specific red flags or other information that suggested that ELF's Chinese suppliers were incorporating North Korean materials. As a result, this action is a reminder of OFAC's willingness to apply a strict liability standard in certain circumstances. As OFAC explained, and consistent with the above described advisory regarding risks associated with North Korea supply chain links,[67] this action highlights the risks for companies that do not conduct "full-spectrum supply chain due diligence" when sourcing products from overseas, "particularly in a region in which [North Korea] as well as other comprehensively sanctioned countries or regions, is known to export goods."[68]

Treasury's Financial Crimes Enforcement Network

FinCEN issued $200 million in penalties in 2018 (compared to $323 million in 2017 and $20 million in 2016) and its final rule on customer due diligence and beneficial ownership ("CDD Rule") went into effect. The agency was also active in issuing guidance on Iran's attempts to exploit the U.S. financial system, FATF findings, and human rights abuses by political figures.

FinCEN Rules and Guidance

Customer Due Diligence Rule, FAQs, and Exceptive Relief. On May 11, 2018, FinCEN's CDD Rule became effective, following a two-year transition period. The rule codifies new and existing customer due diligence requirements under the BSA for covered financial institutions, namely, banks, broker-dealers, mutual funds, and futures commission merchants and introducing brokers in commodities.[69] On April 3, 2018, FinCEN issued 37 frequently asked questions about the rule covering a variety of topics, including the categories of customers excluded from the beneficial ownership requirement.[70] FinCEN has also issued exceptive relief regarding application of the rule to the following: the rollover of certificates of deposits; the renewal, modification, or extension of loans, commercial lines of credit, and credit card accounts, where the renewal, modification, or extension does not require underwriting review and approval; and the renewal of safe deposit box rentals.[71]

Advisory on Iran's Attempts to Exploit the U.S. Financial System. On October 11, 2018, FinCEN published a detailed advisory on the "Iranian Regime's Illicit and Malignant Activities and Attempts to Exploit the Financial System."[72] The advisory is intended to assist financial institutions (particularly banks; money services businesses, including virtual currency administrators and exchangers; and dealers in precious metals, stones, and jewels) in better detection and reporting of potentially illicit Iran-related activity. The advisory notes that Iran may increase its efforts surreptitiously to access the international and U.S. financial systems given the increased pressure it will experience in light of the United States' withdrawal from the JCPOA. FinCEN observed that the advisory will also help non-U.S. financial institutions better understand the obligations of their U.S. correspondents, avoid exposure to U.S. sanctions, and address broader AML concerns that Iran poses to the international financial system.

The advisory describes, citing illustrative OFAC designations of Iranian parties, various techniques used by Iran to evade sanctions and access the international financial system. These are: Central Bank of Iran officials' use of regional banks to fund Iran Guard Corps-Qods Force (IRGC-QF) and Lebanese Hizballah; the misuse of exchange houses; procurement networks that utilize front or shell companies to acquire technology and other goods (relating, for example, to currency counterfeiting, dual-use equipment, and aviation); suspicious funds transfers; the use of precious metals, including gold; and the limited but potentially growing use of virtual currency. The advisory then describes 21 "red flags" relating to these techniques. Among other things, the advisory recommends that: (1) financial institutions continue to implement robust and multi-tiered levels of screening and review for transactions originating from or otherwise involving jurisdictions in close proximity to Iran; and (2) financial institutions engaged in cross-border wire activity be aware of transactions involving jurisdictions with strong geographical and economic ties to Iran. FinCEN notes that implementation of these practices generally results in significant oversight of correspondent bank accounts that may involve Iranian interests.

Advisory on Financial Action Task Force Findings. On October 19, 2018, FATF updated its list of jurisdictions with strategic AML/CFT deficiencies. To help U.S. financial institutions adjust their risk-

based approaches in accordance with FATF's guidance, FinCEN issued an advisory on October 31, 2018.[73] The advisory notes that both North Korea and Iran are included in FATF's "Public Statement," which identifies jurisdictions with such serious strategic deficiencies that FATF calls on its members and non-members to apply counter-measures and enhanced due diligence.[74] The advisory also notes that FATF has updated its "Improving Global AML/CFT Compliance: On-going process" list, which identifies jurisdictions with strategic weaknesses in their AML/CFT measures that have provided high-level commitments to carrying out action plans developed with FATF.[75] The Bahamas, Botswana, and Ghana were added to the list "due to the lack of effective implementation of their framework."[76]

Taking into consideration these updates to FATF's lists, the advisory reiterates previous guidance calling for countermeasures against North Korea to protect the international financial system from money laundering and terrorist financing risk and enhanced due diligence on transactions with a nexus to Iran, with a particular focus on terrorist financing risk. Further, with respect to the three jurisdictions newly added to the "Improving Global AML/CFT Compliance: On-going process" list, the advisory calls for appropriate risk-based due diligence programs (and, where necessary, enhanced policies) reasonably designed to detect and report suspected money laundering involving U.S. correspondent bank accounts.[77]

Advisory on Human Rights Abuses by Corrupt Foreign Political Figures. On June 12, 2018, FinCEN issued an advisory regarding human rights abuses enabled by corrupt senior non-U.S. political figures and their financial facilitators.[78] The advisory highlights the connection between corrupt senior non-U.S. political figures and the enabling of human rights abuses by describing a number of typologies used to access the U.S. financial system and obscure and further illicit activity, including misappropriation of state assets, use of shell companies, and corruption in the real estate sector. Appendix 1 to the advisory includes several case studies that highlight these typologies. The advisory also discusses several red flags to assist financial institutions in identifying the methods used by corrupt senior non-U.S. political figures, Politically Exposed Persons ("PEPs"), and their facilitators and reminded financial institutions that no single red flag necessarily indicates suspicious activity. The red flags include the use of third parties or corporate vehicles when used to shield the identity of a PEP; a PEP or facilitator repeatedly moving funds to or from countries where they do not appear to have ties; and a PEP or facilitator having substantial control over, or access to, state funds and resources.[79]

Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing. As a result of a working group established by the U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence and the federal bank regulators, FinCEN, the Federal Reserve, the Office of the Comptroller of the Currency ("OCC"), the Federal Deposit Insurance Corporation ("FDIC"), and the National Credit Union Administration ("NCUA"), issued a joint statement on December 3, 2018, to encourage banks to "consider, evaluate, and, where appropriate, responsibly implement innovative approaches to meet their BSA/AML compliance obligations, in order to further strengthen the financial system against illicit financial activity."[80] The joint statement notes that FinCEN will consider requests for

exceptive relief to facilitate the testing and potential use of new technologies and other innovations, provided that banks maintain the overall effectiveness of their BSA/AML compliance programs. It also stresses that "when banks test or implement artificial intelligence-based transaction monitoring systems and identify suspicious activity that would not otherwise have been identified under existing processes, [the agencies] will not automatically assume that the banks' existing processes are deficient."[81] FinCEN is also launching an innovation initiative, and intends to engage in outreach efforts that include dedicated times for financial institutions, technology providers, and other firms involved in financial services innovations to discuss the implications of their products and services and their future applications or next steps. Similarly, each of the other agencies has, or will establish, projects or offices that will work to support the implementation of responsible innovation and new technology in the financial system.

Interagency Statement on Sharing Bank Secrecy Act Resources. On October 3, 2018, FinCEN, the Federal Reserve, the OCC, the FDIC, and the NCUA published a statement identifying the circumstances under which banks may enter into collaborative arrangements to share resources to manage their BSA/AML obligations more efficiently and effectively, noting that such arrangements are "most appropriate" where a bank has "a community focus, less complex operations, and lower-risk profiles for money laundering or terrorist financing."[82] The statement advises banks to approach the establishment of collaborative arrangements with due diligence and thorough consideration of the risks and benefits.

FinCEN Enforcement Actions

U.S. Bancorp. As described in additional detail below, on February 15, 2018, FinCEN,[83] DOJ,[84] the OCC,[85] and the Federal Reserve[86] announced $613 million in penalties against U.S. Bancorp and its subsidiary, U.S. Bank N.A. (the "Bank"), for willful violations of the BSA. For its part, FinCEN assessed a $185 million civil money penalty. This penalty was satisfied by a $70 million payment, with the remainder satisfied by payments required by DOJ.

UBS Financial Services, Inc. On December 17, 2018, FinCEN, the SEC, and FINRA announced the imposition of a total of $15 million in fines against UBS Financial Services, Inc. ("UBS").[87] FinCEN determined that UBS failed to implement an appropriate, risk-based AML program that adequately addressed the risks associated with the use of securities accounts for banking-like services, such as the movement of funds, rather than trading securities. FinCEN determined that UBS failed to implement appropriate policies and procedures to ensure the detection and reporting of suspicious activity through all accounts—particularly those accounts that exhibited little to no securities trading. FinCEN also found that UBS failed to provide sufficient resources to ensure day-to-day AML compliance, resulting in inadequate staffing that led to a significant backlog of alerts and decreased ability to timely file suspicious activity reports ("SARs").

Department of Justice

Last year, DOJ had four significant corporate resolutions, and several individual prosecutions, involving sanctions and AML criminal violations. Notably, two of those actions, against Rabobank and U.S. Bancorp and U.S. Bank N.A., involved alleged efforts by those banks to conceal information from their primary regulator, the OCC. As Acting Assistant Attorney General John P. Cronan explained, Rabobank's guilty plea "is a warning to financial institutions that there are significant consequences for banks that engage in obstructive conduct in an effort to hide their anti-money laundering program failures."

New Policies on Corporate Criminal Prosecutions. As discussed in prior memoranda, DOJ announced several policies relating to corporate criminal prosecutions, including a new policy to coordinate the imposition of corporate penalties to avoid "piling on;" changes to DOJ's existing policies for granting companies credit for cooperating with criminal investigations; and new guidance for prosecutors in determining whether to impose independent compliance monitors.[88]

DOJ's new policy to coordinate the imposition of corporate penalties in cases where more than one regulator or law enforcement authority is investigating the same conduct is of particular interest to companies that may face simultaneous sanctions and/or AML investigations by multiple government agencies. In a speech announcing the new policy, then-Deputy Attorney General Rod Rosenstein referred to the "piling on" of fines and penalties by multiple regulators and law enforcement agencies "in relation to investigations of the same misconduct."[89] He noted that the "aim" of the new policy "is to enhance relationships with our law enforcement partners in the United States and abroad, while avoiding unfair duplicative penalties." Specifically, the new policy requires DOJ attorneys to "coordinate with one another to avoid the unnecessary imposition of duplicative fines, penalties, and/or forfeiture against [a] company," and further instructs DOJ personnel to "endeavor, as appropriate, to . . . consider the amount of fines, penalties and/or forfeiture paid to other federal, state, local, or foreign enforcement authorities that are seeking to resolve a case with a company for the same misconduct."[90] DOJ appears to have resolved the Rabobank, U.S. Bancorp, and SocGen investigations under this new policy, but DOJ did not detail how the policy impacted the resolutions.[91] As noted above, OFAC appears to have departed from its well-established policy of crediting payments made to other agencies for the same conduct, although it has not made an announcement to that effect. If OFAC is in fact changing its policy, this may be in tension with the goals behind DOJ's new policy.

Rabobank, N.A. As described in our prior memorandum,[92] on February 7, 2018, DOJ[93] and the OCC announced the imposition of $368.7 million in penalties on Rabobank, N.A., ("Rabobank"), the California-based subsidiary of the Dutch financial services company. In addition to agreeing to a substantial forfeiture and civil money penalty, Rabobank pled guilty to one count of conspiracy to obstruct the OCC's attempts to identify deficiencies in Rabobank's BSA/AML compliance program. Although Rabobank had become aware of activity at branches along the U.S.-Mexico border that was indicative of money laundering, narcotics trafficking, and organized crime, Rabobank implemented policies and procedures that "precluded and

suppressed" the investigation and reporting of this activity. These policies included a so-called "Verified List" of customers deemed per se non-suspicious, even when a customer's transaction activity deviated from previous levels, and a policy that certain evidently structured transactions under $10,000 were non-suspicious, because the accountholders claimed they wanted to minimize the necessary paperwork when crossing the U.S.-Mexico border with cash. The bank also failed to allocate sufficient staff to investigate suspicious activity (for example, at certain times, Rabobank devoted only three employees to investigate more than 2,300 alerts per month); failed to file continuing activity SARs; and failed to keep up with enhanced due diligence reviews of customers, transactions, and accounts.[94] Rabobank compounded these issues by allegedly marginalizing the executive responsible for managing the BSA/AML program.

The bank's guilty plea was based on its concealment of BSA/AML failures from the OCC. In the same period in which the compliance executive was sidelined, the OCC requested that Rabobank turn over reports drafted by consultants retained to evaluate the bank's BSA/AML program—reports which were highly critical of the program. According to the Statement of Facts, Rabobank's management withheld those reports from the OCC for nearly a month and made a number of false or misleading statements to the OCC, including that (1) the consultant had not produced an assessment when, in fact, it had done so, and that (2) the consultant had given a presentation to management, but had not left any documents behind when, in fact, the report authored by the consultant was in Rabobank's possession. Notably, although Rabobank was not charged with a criminal violation of the BSA, the $368,701,259 forfeiture amount appears predicated on the amount of "suspicious transactions that were either unreported or reported untimely."[95]

U.S. Bancorp and U.S. Bank N.A. As described in our prior memorandum,[96] on February 15, 2018, DOJ,[97] FinCEN,[98] the OCC,[99] and the Federal Reserve[100] announced $613 million in penalties against U.S. Bancorp and its subsidiary, U.S. Bank N.A., for willful violations of the BSA. Among other deficiencies cited by the government, U.S. Bank (1) failed to devote sufficient resources to its BSA/AML compliance program; (2) artificially capped the number of alerts generated by its transaction monitoring system based on staffing levels and resources, and made efforts to avoid disclosing this practice to the OCC, its primary regulator; (3) failed to conduct any transaction monitoring of non-customer Western Union transactions at its branches; (4) failed to file SARs as a result of deficient customer due diligence, transaction monitoring, and investigation procedures; and (5) failed to timely report suspicious banking activities of a significant customer, Scott Tucker, who used U.S. Bank to launder more than $2 billion of proceeds from an illegal payday lending scheme. According to the U.S. Attorney for the Southern District of New York, the Bank operated its BSA/AML compliance program "on the cheap" and "concealed its wrongful approach from the OCC" resulting in a failure to identify and report on "large numbers" of suspicious transactions.

DOJ's $528 million penalty was imposed pursuant to a deferred prosecution agreement ("DPA") and was collected through U.S. Bancorp's payment of a $453 million civil forfeiture to DOJ, with the remaining $75 million satisfied by the payment of a civil money penalty assessed by the OCC. FinCEN and the Federal

Reserve assessed $185 million and $15 million penalties, respectively, with $115 million of FinCEN's penalty deemed satisfied by DOJ forfeiture.

MoneyGram International Inc. On November 8, 2018, Moneygram International Inc. ("Moneygram") agreed to extend an existing DPA and forfeit $125 million dollars as a result of weaknesses in its anti-fraud and AML compliance programs.[101] Moneygram initially entered into the DPA on November 9, 2012, in connection with charges of willfully failing to maintain an effective AML program and aiding and abetting wire fraud; the DPA was set to end in November 2017.[102] On November 8, 2018, Moneygram agreed that it was not in compliance with the terms of that DPA and agreed to extend the DPA through May 2021. Specifically, Moneygram admitted that, in April 2015, it implemented a new fraud interdiction system that "ultimately proved to be ineffective." As a result, between April 2015 and October 2016 (when a new consumer fraud interdiction system was implemented), Moneygram processed at least $125 million in transactions associated with consumers it had previously identified as having received fraudulent transactions. In connection with the extended DPA, Moneygram agreed, among other things, to (1) develop and implement enhanced due diligence on high-risk agents; (2) ensure that all money transfers originating in the United States will be monitored by Moneygram's anti-fraud program; (3) develop and implement a risk-based program to test and verify the accuracy of information in its transaction database; and (4) provide monthly reports to DOJ noting, among other things, Moneygram agents who are terminated or are suspected of AML-related or other compliance violations and data about high-risk transactions.

Société Générale S.A. As described above, DOJ entered into a DPA with SocGen on November 19, 2018, as part of a multi-agency resolution.[103] Under the DPA, SocGen agreed to forfeit $717.2 million and stipulated to the accuracy of an extensive statement of facts, and the government agreed to defer prosecution for a period of three years assuming the bank's compliance with the agreement. The U.S. Attorney for the Southern District of New York alleged that, from 2003 through 2010, SocGen willfully engaged in 3,100 sanctions violations totaling $15 billion dollars mainly by processing transactions involving Cuban credit facilities through the U.S. financial system. It further alleged that, as a general practice, SocGen would omit references to Cuba from the related SWIFT messages. U.S. financial regulators began investigating SocGen after other U.S. financial institutions blocked two SocGen transactions in 2012, and SocGen voluntarily disclosed some transactions, separate and apart from the Cuban credit transactions, in February 2013. The DPA further states that SocGen did not disclose the Cuban credit transactions at either time and continued not to disclose them during ongoing discussions with U.S. regulators and that it was only after SocGen performed a detailed forensic analysis, in October 2014, that SocGen disclosed these transactions. The U.S. Attorney's Office's press release stated that SocGen's enhancement of its sanctions compliance program, its thorough internal investigation, and its production of voluminous evidence located in other countries weighed in favor of a DPA and "outweighed in this particular case [SocGen's] failure to self-report all of its [sanctions violations] in a timely manner."[104]

Central States Capital Markets, LLC. On December 19, 2018, DOJ brought the first ever criminal BSA charge against a broker-dealer, which was resolved in a DPA that imposed a forfeiture of $400,000. The U.S. Attorney for the Southern District of New York charged Central States Capital Markets, LLC ("CSCM") with one felony violation of the BSA, based on CSCM's willful failure to file a SAR regarding the illegal activities of its customer.[105] The customer, Scott Tucker (who, as noted above, also allegedly used U.S. Bank in furtherance of his illegal activities), was convicted in October 2017 of racketeering, wire fraud, and money laundering for his role in perpetrating a multibillion dollar payday lending scheme that started as far back as the late 1990s.[106] CSCM ignored numerous red flags concerning the customer, including a prior fraud conviction, news reports from 2011 alleging that the customer was running a payday lending scheme, and a Federal Trade Commission investigation. Furthermore, CSCM received 103 alerts from its AML software, but never checked them. Finally, despite producing documents in connection with the U.S. Attorney's Office's criminal investigation, CSCM did not file a SAR until well after the customer was convicted. In its press release, the U.S. Attorney's Office stated that this charge "makes clear that all actors governed by the Bank Secrecy Act—not only banks—must uphold their obligations."[107] The SEC brought a parallel cease-and-desist proceeding against CSCM.[108]

Huawei Technologies Co., Ltd. On January 28, 2019, a 13-count indictment was unsealed in the U.S. District Court for the Eastern District of New York against Huawei Technologies Co., Ltd. ("Huawei"), U.S.-based Huawei Device USA Inc., Skycom Tech Co. Ltd. ("Skycom"), and Wazhou Meng ("Meng").[109] Meng, Huawei's Chief Financial Officer, is currently under house arrest in Canada and subject to a U.S. extradition request. The indictment alleges long-running conspiracies to violate Iran sanctions, commit bank fraud and money laundering, and defraud the United States. It also alleges substantive criminal bank fraud, wire fraud, and Iran sanctions violations. Specifically, the government alleges that Huawei, a Chinese company, engaged in an elaborate scheme to deny its actual ownership of Skycom, which allegedly functioned as Huawei's Iranian-based subsidiary.[110] Huawei allegedly informed several victim financial institutions with U.S. operations that Huawei did not violate applicable U.S. laws, including the U.S. sanctions regime applicable to Iran.[111] As a result, the victim financial institutions continued to do business with Huawei, and at least one such financial institution provided financial services to Iran or the Government of Iran involving millions of dollars.[112] Huawei allegedly carried out this scheme in part through Meng, who allegedly represented to a victim financial institution executive that Huawei operated in strict compliance with U.S. sanctions, and that Huawei's relationship with Skycom was normal "business cooperation."[113] The government alleges that had the victim financial institutions known about Huawei's sanctions violations, they would have reevaluated their banking relationships with Huawei, including the provision of U.S.-dollar clearing services to Huawei.[114] In addition, Huawei allegedly obstructed the grand jury investigation by moving witnesses with knowledge of Huawei's Iran-related business to China and by destroying and concealing evidence relating to that business.[115]

Sanctions Prosecution of Ali Sadr Hashemi Nejad. On March 20, 2018, an indictment was unsealed charging Ali Sadr Hashemi Nejad ("Sadr") for his alleged involvement in a scheme to evade U.S. sanctions

against Iran in which more than $115 million in payments for a Venezuelan housing complex were illegally funneled through the U.S. financial system for the benefit of Iranian individuals and entities.[116] In 2005, the Governments of Iran and Venezuela entered into a memorandum of understanding regarding a housing infrastructure project in Venezuela. The project was led by Stratus Group, an Iranian conglomerate controlled by Sadr and his family. The Stratus Group, through an Iranian company, entered into a contract with a subsidiary of a Venezuelan state-owned energy company to build approximately 7,000 housing units in Venezuela in exchange for approximately $475 million. Sadr allegedly took steps to evade U.S. economic sanctions and to defraud U.S. banks by concealing the role of Iran and Iranian parties in U.S. dollar payments connected to the project sent through the U.S. banking system. For example, Sadr and a conspirator allegedly used St. Kitts and Nevis passports and a United Arab Emirates address to incorporate two entities outside Iran that would receive U.S. dollar payments related to the housing project. As in other recent individual prosecutions, in addition to conspiracy to violate sanctions, the U.S. Attorney's Office for the Southern District of New York charged Sadr with defrauding the government, defrauding banks, money laundering, and related conspiracy charges. Sadr is awaiting trial.

Sanctions Prosecution of Arash Sepehri. On November 7, 2018, Arash Sepehri, an Iranian citizen, pleaded guilty in the U.S. District Court for the District of Columbia to conspiracy to unlawfully export U.S. goods to Iran and to defraud the United States.[117] Sepehri, through an Iranian company and associated companies, conspired to obtain high-resolution sonar equipment, data input boards, rugged laptops, acoustic transducers, and other controlled technology from the United States without obtaining proper licenses and in violation of sanctions. Sepehri and his co-conspirators sought to evade legal controls through various means, including the use of a variety of aliases, UAE-based front companies, and an intermediary shipping company based in Hong Kong. Sepehri is awaiting sentencing.

Federal Banking Agencies

Sanctions/AML compliance continues to be an area of important focus by the federal banking agencies. For example, in its most recent Semiannual Risk Perspective, the OCC noted that compliance risk remains "elevated" as banks continue to manage money laundering risks in light of the "dynamism of money laundering and terrorism-financing methods."[118] The OCC added that "bank offerings using new or evolving delivery channels may increase customer convenience and access to financial products and services, but banks need to maintain a focus on refining or updating BSA compliance programs to address any vulnerabilities created by these new offerings, which criminals can exploit."[119]

Federal Banking Agency Guidance

As described above, the federal banking agencies and the Treasury Department have coordinated on BSA/AML issues and have issued two joint statements—one encouraging technological innovation in BSA/AML compliance and the other addressing the sharing of BSA/AML resources between financial institutions. Testifying before Congress, Comptroller of the Currency Joseph Otting mentioned this

ongoing interagency coordination and noted that "the process for complying with current BSA/AML laws and regulations has become inefficient and costly."[120] He outlined some of the OCC's proposals for improving BSA/AML regulation—some of which require regulatory or legislative changes—including allowing the scheduling and scoping of BSA/AML exams on a risk-based basis and considering changes to SAR and currency transaction reporting thresholds and simplifying such reports.

The Federal Reserve, FDIC, and the OCC also recently announced a new commitment to coordinating interagency enforcement investigations and penalties in multi-agency resolutions.[121] In a joint policy statement, the three agencies stated that "if two or more [of the agencies] consider bringing a complementary action (e.g., action involving a bank and its parent holding company), those [agencies] should coordinate the preparation, processing, presentation, potential penalties, service, and follow-up of the enforcement action."[122]

The federal banking agencies are also working with FinCEN to revise the Federal Financial Institutions Examination Council ("FFIEC") BSA/AML Examination manual to further define application of the agencies' risk-based approach to supervision.[123] Revisions are expected to be published in the first quarter of 2019.[124]

Federal Banking Agency Enforcement Actions

The federal banking agencies' continued focus on sanctions and BSA/AML enforcement is reflected in several actions brought against financial institutions by the Federal Reserve and the OCC.

SocGen, Rabobank, and U.S. Bancorp. As discussed above, the Federal Reserve was part of the multi-agency sanctions resolution with SocGen; the OCC was part of the multi-agency BSA/AML resolution with Rabobank; and the Federal Reserve and the OCC were both part of the multiagency BSA/AML resolution with U.S. Bancorp and U.S. Bank. Notably, in the Rabobank matter, Rabobank pled guilty to conspiracy to obstruct the OCC's supervision of the bank, and the OCC fined the bank for BSA/AML program failures and for concealing documents from OCC examiners.[125]

Mega International Commercial Bank Co., Ltd. On January 17, 2018, the Federal Reserve and the Illinois Department of Financial and Professional Regulation announced a $29 million penalty against Taiwan's Mega International Commercial Bank and certain of its U.S. operations ("Mega Bank") for BSA/AML violations, as well as violations of Illinois law.[126] The consent order includes a number of requirements, including the submission of plans to create a consolidated framework for BSA/AML and OFAC compliance across the bank's U.S. operations (including the bank's New York, Chicago, and Silicon Valley branches) and to enhance oversight by U.S. senior management and the bank's board of directors. Mega Bank and its New York Branch are also required to engage an independent third party to conduct a lookback review of U.S. dollar clearing transaction activity for a six-month period to determine whether suspicious activity involving high risk customers or transactions was properly identified and

reported. While the consent order does not detail specific findings, Mega Bank paid a $180 million penalty to the NY DFS in August 2016 based on a number of alleged AML deficiencies, including the failure to identify and report suspicious transactions with its Panama branches.

Capital One, N.A. and Capital One (USA), N.A. On October 23, 2018, the OCC announced its assessment of a $100 million civil money penalty against Capital One, N.A. and Capital One Bank (USA), N.A. (collectively, the "bank") for alleged deficiencies in the bank's BSA/AML program and failure to achieve timely compliance with the OCC's prior July 2015 consent order. The prior consent order cited various weaknesses in the bank's BSA/AML compliance program and the failure to file certain SARs.[127]

Bank of China. On April 24, 2018, the OCC and Bank of China's New York Branch ("BOC") entered into a consent order assessing a $12.5 million penalty for deficiencies in BOC's BSA/AML and OFAC compliance programs, including inadequate internal controls, insufficient training, deficiencies in transaction monitoring systems resulting in a failure to timely file SARs, and systematic deficiencies in its customer due diligence and risk rating processes.[128] On the same day, the OCC and BOC entered into a separate consent order stemming from the OCC's determination that BOC failed to adopt and implement adequate BSA/AML and OFAC compliance programs, and failed to timely file SARs. [129] Under the second consent order, BOC was required to submit an action plan for the completion of risk assessments of its BSA/AML and OFAC compliance programs; an assessment of the risk BOC is willing to assume; a plan for the development and implementation of enterprise-wide policies and procedures for gathering customer due diligence and enhanced due diligence information; a plan for the development and implementation of enterprise-wide policies and procedures to ensure timely SAR filing; and a plan for the development and implementation of a written enterprise-wide program to ensure ongoing compliance with OFAC regulations. BOC also agreed to devise an acceptable BSA/AML audit program, hire a permanent, qualified, and experienced BSA officer. No lookback review of transactions was required.

Resolutions without Penalties. As in prior years, the federal banking agencies also issued BSA/AML-related consent orders or written agreements that imposed a number of remedial requirements but lacked monetary penalties. For example, the Federal Reserve entered into consent orders against Industrial and Commercial Bank of China Ltd. ("ICBC") and its New York Branch, and Hua Nan Commercial Bank Limited ("Hua Nan"), following the identification of significant deficiencies in the banks' risk management and BSA/AML compliance.[130] Both orders required the financial institutions to develop and implement plans for strengthening BSA/AML compliance and to engage independent third parties to conduct lookbacks.

Securities and Exchange Commission and Financial Industry Regulatory Authority

SEC and FINRA have continued to pursue AML-related enforcement actions, including against individuals. A number of these actions involved failing to file SARs related to low-priced securities transactions. One of these actions is the SEC's closely-watched federal court litigation against Alpine Securities Corporation.

Both the SEC and FINRA have stressed their commitment to AML compliance. On December 20, 2018, the SEC's Office of Compliance Inspections and Examinations issued its 2019 Examination Priorities, which highlights the SEC's continued prioritization of "examining broker-dealers for their AML obligations, including whether they are meeting their SAR filing obligations, implementing all elements of their AML program, and robustly and timely conducting independent tests of their AML program."[131] Likewise, FINRA stated in its 2018 Report on Examination Findings that it "continues to find problems with the adequacy of some firms' overall AML programs; allocation of AML monitoring responsibilities, particularly responsibilities for trade monitoring; data integrity in AML automated surveillance systems, especially in suspense accounts for processing foreign currency money movements and conversions; firm resources for AML programs; and independent testing of AML monitoring programs."[132]

UBS Financial Services, Inc. As described above, the SEC and FINRA were both part of the multiagency resolution with UBS for AML violations.

***SEC* v. *Alpine*.** As detailed in our prior memorandum,[133] on December 11, 2018, the SEC secured a victory in its enforcement action against Alpine Securities Corporation, a clearing broker that allegedly failed to file SARs relating to certain microcap securities transactions.[134] Judge Cote of the U.S. District Court for the Southern District of New York partially granted the SEC's motion for summary judgment, finding Alpine liable for thousands of violations of Rule 17a-8 of the Securities Exchange Act of 1934, which requires broker-dealers to report potentially illegal activity by filing SARs.[135] The decision is notable as a rare instance of a court's ruling on various types of SAR violations, whereas most SAR-related enforcement actions are resolved without litigation. Broker-dealers and potentially other financial institutions subject to SAR-filing requirements may wish to review this decision as guidance regarding the adequacy of SAR narratives and other issues. The decision is also notable for again rejecting Alpine's argument that the SEC lacks authority to pursue SAR violations, holding that the Exchange Act grants the SEC "independent authority to require broker-dealers to make reports" and "enforcement authority over those broker-dealer reporting obligations."[136] Alpine may continue to pursue its arguments, including those about the SEC's lack of BSA enforcement authority, in an appeal to the Second Circuit, despite having previously unsuccessfully sought mandamus on the issue.[137]

Morgan Stanley Smith Barney LLC. On December 26, 2018, FINRA announced a $10 million settlement with Morgan Stanley Smith Barney LLC ("Morgan Stanley") for alleged AML program and supervisory failures that spanned a period of more than five years.[138] Specifically, FINRA determined that: (1) Morgan Stanley's automated AML surveillance system did not receive critical data from several systems, undermining the firm's surveillance of wire and non-U.S. currency transfers, including those involving countries known for having high money-laundering risk; (2) Morgan Stanley failed to devote sufficient resources to review alerts generated by its automated AML surveillance system, and thus often closed alerts without sufficient investigation; and (3) the AML Department did not reasonably monitor customers' deposits and trades in penny stocks for potentially suspicious activity, despite the fact that its customers

deposited approximately 2.7 billion shares of penny stocks involving subsequent sales of approximately $164 million during the relevant time period. FINRA recognized the firm's "extraordinary corrective measures."

Aegis Capital Corporation. On March 28, 2018, the SEC and FINRA announced settlements totaling $1.3 million in penalties with Aegis Capital Corporation ("Aegis"), a registered broker-dealer, in connection with the firm's failure to file SARs regarding low-priced securities transactions.[139] Between late 2012 and early 2014, Aegis "knew, suspected, or had reason to suspect" that hundreds of transactions it processed were being used to manipulate the market and "to facilitate fraudulent activity" with "no business or apparent lawful purpose."[140] The transactions at issue were in low-priced securities made through Delivery Versus Payment/Receive Versus Payment accounts ("DVP/RVP"). The transactions were structured such that customers would deposit their shares in another firm's custody account. Various clearing firms with which Aegis had relationships would then assist in effectuating the transactions. In many situations, the underlying customers were non-U.S. financial institutions that were effectuating transactions on behalf of their own customers who were unknown to Aegis. According to the SEC, even though AML red flags were identified, Aegis did not file SARs or create written analyses or other records of the transactions. In its settlement with the SEC, Aegis admitted the SEC's allegations and agreed to pay a $750,000 fine and retain an expert in compliance procedures.[141] On the same day, Aegis agreed to pay a $550,000 penalty to FINRA, but neither admitted nor denied the charges.[142]

Several Aegis employees also reached settlements with the SEC, without admitting or denying the SEC's findings. Kevin McKenna, a former AML Compliance Officer with the firm, and Robert Eide, the owner and Chief Executive Officer, were found to have aided and abetted the firm's failure to file SARs.[143] McKenna agreed to pay a $20,000 penalty and Eide agreed to pay a $40,000 penalty. McKenna also agreed to an eighteen month prohibition from serving in roles related to compliance or AML in the securities industry. In a separate settlement with the SEC on July 6, 2018, Eugene Terracciano, another Aegis AML Compliance Officer, agreed to pay a $20,000 fine without admitting or denying the alleged conduct.[144]

Chardan Capital Markets LLC, Chardan's AML Officer, and Industrial and Commercial Bank of China Financial Services LLC ("ICBCFS"). The SEC reached settlements with Chardan Capital Markets LLC ("Chardan"), Chardan's AML Officer, Jerard Basmagy, and Industrial Commercial Bank of China Financial Services LLC ("ICBFS") on May 16, 2018.[145] The SEC alleged that Chardan liquidated over 12.5 billion penny stock shares for seven customers between October 2013 and June 2014 and that ICBCFS then cleared the transactions. Though many of these transactions allegedly presented red flags, such as heavy trading in low priced securities, large volume trading, and sales in issuers without any revenues or products, Chardan and ICBCFS did not file any SARs.[146] According to the SEC, Jerard Basmagy, Chardan's AML officer, aided and abetted the firm's conduct by failing to investigate red flags and file SARs.

As part of the settlement, the SEC imposed fines of $1 million against Chardan, $860,000 against ICBCFS, and $15,000 against Basmagy.[147] Basmagy agreed to industry and penny stock bars for at least three

years.[148] FINRA also reached a settlement with ICBCFS, under which ICBCFS would pay a $5.3 million penalty and agreed to retain an independent compliance consultant.

LPL Financial, LLC. On October 30, 2018, FINRA announced a settlement with LPL Financial, LLC ("LPL"), which included a $2.75 million penalty for, among other things, failure to properly investigate and report unauthorized attempts to gain access to its electronic systems.[149] FINRA alleged that these attempts should have led the firm to file over 400 SARs. FINRA found that the firm's compliance employees consulted a "fraud case chart" that contained inaccurate guidance regarding SAR reporting requirements.[150] FINRA recognized LPL's "extraordinary cooperation."[151]

New York Department of Financial Services

DFS remained active in the sanctions/AML space in 2018, issuing significant consent orders against SocGen, Mashreqbank, and Western Union. Additionally, DFS-regulated banks, check cashers, and money transmitters subject to DFS's Part 504 regulation[152] faced their first certification deadline on April 15, 2018, and are now making preparations for their second annual certification. Meanwhile, little is known about DFS's potential enforcement approach to Part 504. DFS also recently issued guidance on principles and best practices for ensuring a robust whistleblower program, which may have implications for sanctions/AML compliance.

In late December 2018, Superintendent Maria Vullo announced that she will be leaving DFS, effective February 1, 2019. Governor Cuomo has nominated his long-time chief of staff, Linda Lacewell, to become the new Superintendent. Ms. Lacewell previously served as a federal prosecutor in the U.S. Attorney's Office for the Eastern District of New York.[153]

Société Générale. As described above, on November 19, 2018, as part of a broader $1.3 billion multi-agency sanctions resolution,[154] DFS fined SocGen and its New York branch $325 million for executing nearly $13 billion in "illegal and non-transparent" transactions to parties in countries subject to embargoes or otherwise sanctioned by the United States, including Iran, Sudan, Cuba and Libya, during the period 2003 to 2013.[155] Even though many of these transactions may have satisfied OFAC's "U-turn" exception, which was in place until November 2008, DFS alleged that SocGen put "customer service over compliance" and prevented DFS from fully understanding and examining this conduct.[156]

In a separate consent order, DFS fined SocGen $95 million for alleged BSA/AML compliance violations.[157] In 2009, SocGen entered into an agreement with DFS and the Federal Reserve to remediate AML deficiencies. While DFS found that SocGen had "made substantial gains in improving its compliance program between 2009 and 2013," DFS stated that, more recently, SocGen's compliance "had fallen off precipitously."[158] In fact, SocGen received "an unacceptable rating for its compliance function for four consecutive [DFS] examination cycles," from 2014 through 2017.[159] DFS found that SocGen's New York branch struggled to remediate deficiencies repeatedly identified during prior examinations, including

inadequate program testing, outdated policies, and flaws in customer due diligence protocols.[160] In addition to imposing a $95 million monetary penalty and a set of remedial requirements, the consent order requires SocGen to engage the independent consultant that had already been hired pursuant to a December 2017 Federal Reserve cease and desist order to review its BSA/AML compliance programs in eighteen months. Moreover, DFS stated that it may require SocGen to engage an independent monitor for up to two additional years after reviewing the independent consultant's report on the bank's compliance status.[161]

Both consent orders referenced SocGen's "substantial cooperation" during DFS's investigation and noted that DFS gave "substantial weight to the commendable conduct of the Bank" in agreeing to the terms of the consent orders.[162]

Mashreqbank PSC. On October 10, 2018, DFS entered into a consent order with Mashreqbank PSC ("Mashreq")—the largest private bank in the U.A.E.—and its New York branch, fining the bank $40 million for alleged deficiencies in its BSA/AML and OFAC compliance programs.[163] The consent order arose from examinations conducted in 2016 and 2017 by the DFS and the Federal Reserve. Although DFS noted that the branch "made some progress in remediation," DFS initiated this enforcement action after the branch received consecutive low ratings during its last two examinations.[164]

The 2016 and 2017 examinations identified various deficiencies, including: (1) for both transaction monitoring and sanctions screening, the branch had inadequate rationales for closing alerts and investigations and inadequate documentation of the progress of specific investigations identified in the branch's OFAC Investigation Log; (2) for "Know Your Customer" or KYC requirements, the branch used the same analyst to conduct first and second level reviews, lacked "robust information" regarding non-U.S. correspondent banking customers' markets, and "failed to document specific information regarding the analyses performed of expected-versus-actual transactional activity."; and (3) Mashreq's Head Office engaged a third-party BSA/AML auditor, but the Head Office's internal audit function "did not provide sufficient oversight" of that auditor, which omitted "numerous issues uncovered by [DFS] examiners."[165] Notably, however, DFS did not identify any violative transactions in either examination.

In addition to the $40 million penalty and a host of remedial requirements, the consent order required a six-month lookback on U.S. dollar clearing activity and the hiring of an independent consultant to oversee remediation.[166] DFS acknowledged Mashreq's "strong cooperation" and noted that it gave "substantial weight" to this cooperation in agreeing to the terms and remedies of the consent order.[167]

Western Union. On January 4, 2018, DFS issued a consent order against Western Union that imposed a $60 million penalty for allegedly failing to maintain an effective AML program and failing to exercise reasonable supervision over its agents.[168] This order followed a multi-agency resolution from January 2017 involving DOJ, FinCEN, and the FTC. In the order, DFS alleged that several Western Union "executives and managers" willfully ignored suspicious transactions undertaken by Western Union agents in New York, or intervened on their behalf when faced with potential disciplinary action, and that none of this misconduct

was timely disclosed to DFS.[169] While DFS's findings were broad in scope, the consent order specifically centered on nearly $3 billion in China transactions conducted by three agents located in New York City. According to DFS, "[t]he sheer number and size of transactions processed by these agents, which were small independent stores each with a small number of employees, stood out as clear indicators of increased money laundering risk."[170]

DFS faulted Western Union for failing to disclose to DFS the alleged misconduct of its agents until March 2017, even though Western Union was "in a position to disclose its understanding about" the China-related misconduct of its New York agents by 2015 and a related DOJ investigation commenced in 2012.[171]

In addition to the $60 million penalty, DFS notably required Western Union to submit a written plan designed to ensure its agents, "regardless of their location," adhere to U.S. regulatory and AML standards, "unless in direct conflict with local law."[172] DFS also required Western Union to file SARs for any suspicious activity in customer-to-customer transfers of over $2,000 "to, from, or through the United States, regardless of where in the world the suspicious transactions originate or are received."[173] The order does not, however, impose a monitor or independent consultant or require a lookback.

Whistleblower Program Guidance. On January 7, 2019, DFS issued guidance that a "robust" whistleblowing program is an essential component of a comprehensive compliance program for financial services companies.[174] Acknowledging that there is no "one-size-fits-all" approach given the breadth of entities under its jurisdiction, DFS outlines ten "principles and best practices" that all DFS-regulated entities should account for in designing their programs. These include reporting channels that are independent, well-publicized, easy to access, and consistent; strong anonymity, confidentiality, and anti-retaliation protections; established procedures for identifying and managing potential conflicts of interest; strong training and procedures for investigating allegations of wrongdoing; and a "top-down culture of support" for the whistleblowing function. Risk managers may wish to consider how this guidance relates to particular compliance areas, including sanctions/AML compliance.

Additional Developments

Increasing Focus on Virtual Currency. The emergence and proliferation of virtual currencies present a number of challenges related to BSA/AML and sanctions compliance.

In 2018, OFAC and FinCEN took some notable steps with respect to virtual currency. First, OFAC issued eight FAQs on virtual currency and digital wallets, including guidance on OFAC compliance obligations for virtual currency transactions. Second, on November 28, 2018, OFAC identified for the first time virtual currency addresses associated with persons added to the SDN list. The newly sanctioned individuals, Iran-based Ali Khorashadizadeh and Mohammad Ghorbaniyan, were found by OFAC to have converted digital currency payments into Iranian rial as part of a widespread ransomware scheme. Third, FinCEN provided an informative analysis of how virtual currency could emerge in importance as a means of Iranian money

laundering and sanctions evasion.[175] For example, virtual currency can be accessed in Iran and used to evade sanctions through Iran-located, Internet-based virtual currency exchanges and peer-to-peer (P2P) exchangers. Fourth, in August 2018, FinCEN's Director, Kenneth Blanco, stated in prepared remarks that FinCEN and the IRS had examined over 30 percent of all registered virtual currency exchangers and administrators since 2014 with the goal that all virtual currency money transmitters undergo regular, routine compliance examinations—just like every other U.S. financial institution.[176]

At the state level, New York continues its efforts to be a leader in addressing virtual currency. For example, the New York State Office of the Attorney General ("NY AG") launched the Virtual Markets Integrity Initiative, a fact-finding inquiry into the policies and practices of virtual asset trading platforms, and sent letters and questionnaires to thirteen major trading platforms. On August 9, 2018, the NY AG released a Virtual Markets Integrity Report addressing areas of particular concern to the transparency, fairness, and security of virtual asset trading platforms.[177] The DFS has also continued its efforts to expand its regulation of virtual currency businesses that operate in New York through the continued issuance of virtual currency licenses, also known as BitLicenses.[178]

At the international level, FATF announced that it is preparing updated guidance detailing a risk-based approach to regulating virtual asset service providers, and guidance for law enforcement authorities on identifying and investigating illicit activity involving virtual assets.[179]

Virtual currency exchanges are increasingly scrutinized by regulators due to their integral role in the virtual currency marketplace. Currently, virtual currency exchanges that operate "wholly or in substantial part within the United States" are considered money service businesses ("MSBs") that are subject, at the federal level, to the requirements of the BSA and must register with FinCEN.[180] Among other things, financial institutions should consider applying their customer identification programs to all virtual currency exchange clients, confirm the exchange's FinCEN registration status and compliance with state and local licensing requirements, and conduct a BSA/AML risk assessment to determine the level of risk associated with the account and whether further due diligence is necessary.

These developments illustrate the increasing need for financial institutions and other companies to devote resources to understanding and managing compliance risks related to virtual currencies.[181]

Cannabis/Marijuana-Related Developments. Last year saw a number of developments with respect to the legalization of cannabis (or marijuana, which we use interchangeably), leading financial institutions and other companies to wrestle further with their potential relationships to this industry in light of the BSA, the substantive money laundering statutes, the Controlled Substances Act, and other legal requirements.[182] In 2018, Michigan, Utah, and Missouri voted to legalize cannabis for medicinal or recreational purposes.[183] To date, 33 states and the District of Columbia in the United States have legalized either medical or recreational uses of marijuana, and a number of additional states have some limited protections for cannabidiols (CBD) only.[184] Additionally, President Trump signed the 2018 Farm Bill, which effectively

legalized hemp and hemp-derived products at the federal level. Of note, in October 2018, Canada legalized recreational cannabis, fueling a projected $6.1 billion (CAD) industry that has already seen four marijuana-focused public companies with U.S. market caps of over $32 billion. It appears that while large financial institutions continue to evaluate risks regarding providing services to cannabis growers and distributors operating in the United States (and continue to grapple with how, if at all, to work with service providers, employees, and customers of marijuana growers/distributors), many are now providing services to marijuana companies operating in Canada.

Notwithstanding U.S. state-law legalization efforts, marijuana and marijuana-derived CBD remain illegal under federal law.[185] The long-standing federal prohibition on marijuana arises under the federal Controlled Substances Act (CSA), a series of federal criminal statutes that govern the possession, distribution, and sale of "controlled substances," including marijuana.[186] Based on the statutory definition of marijuana,[187] certain parts of the cannabis plant are considered to be Schedule I "controlled substances," while others are not.[188]

Conflicting guidance by federal and state officials. Federal and state governmental actors continue to create a complex and contradictory landscape of guidance and pronouncements regarding the risks of conducting business with the U.S. marijuana industry. On the one hand, on January 4, 2018, then-Attorney General Jeff Sessions rescinded[189] two memoranda issued by then-Deputy Attorney General James Cole during the Obama Administration, which stated that in those states that legalized marijuana and that have strong and effective regulatory and enforcement systems, federal prosecutors should focus enforcement of the Controlled Substances Act (as well as the BSA and the money laundering statutes) only on certain types of marijuana-related cases that implemented eight federal enforcement priorities.[190] When he rescinded these memoranda, then-Attorney General Sessions stated that "prosecutors should follow the well-established principles that govern all federal prosecutions,"[191] thus removing some degree of comfort that those in the state-legal cannabis sector—and those involved in banking such persons and entities—had enjoyed. In January 2019, Bill Barr, President Trump's Attorney General nominee, testified that his approach "would be not to upset settled expectations and the reliance interests that have arisen as a result of the Cole memoranda," and that he would not "go after [marijuana] companies that have relied on the Cole memoranda."[192] However, he characterized the current state/federal dynamic as "untenable" and stated that the federal government should either have a "federal law that prohibits marijuana everywhere," which he personally supports, or if there was desire for a federal approach to permit states "to have their own [marijuana] laws," then the federal government should pursue that path and "get there the right way."[193]

Meanwhile, FinCEN's guidance on Marijuana Banking issued in 2014[194] remains in place, despite its reliance on the now-revoked Cole memoranda.[195] That guidance intended to clarify how banks can provide services to marijuana-related businesses consistent with their BSA obligations and enhance the availability of financial services for, and the financial transparency of, such businesses. In late November 2018,

FinCEN's Director Blanco stated in Senate testimony that FinCEN is having ongoing interagency conversations about marijuana banking and continues to inform financial institutions that they should be following FinCEN's 2014 guidance to meet their BSA requirements.[196]

Other agencies and officials, including Treasury Secretary Mnuchin and Comptroller Otting, have spoken on marijuana-related banking issues.[197] Among the less formal announcements are Senator Cory Gardner's (R-Colo.)'s statement, following his holds on several DOJ nominees, that President Trump assured him that DOJ would not target the marijuana industry in Colorado and that President Trump would "support a federalism-based legislative solution to fix this states' rights issue once and for all."[198] In addition, pending in Congress is the Secure and Fair Enforcement Banking Act or the SAFE Banking Act, which, if enacted, would provide an avenue for financial institutions to provide financial services to marijuana-related businesses and their employees in the United States without risk of liability under federal law.[199]

Making matters more complicated, certain state regulators have actively encouraged their regulated financial institutions to provide services to marijuana companies operating in compliance with state law, notwithstanding federal law. For example, New York's Governor Cuomo and Superintendent Vullo announced that DFS would encourage New York State chartered banks and credit unions to consider providing services to medical marijuana businesses operating in compliance with New York law and with industrial hemp businesses.[200] Among other things, DFS's guidance, while recognizing the rescission of the Cole memoranda, indicated that it was not aware of any actual changes in priorities of the four U.S. Attorneys covering New York State.[201]

The 2018 Farm Bill. On December 20, 2018, President Trump signed into law the Agriculture Improvement Act of 2018 (the "2018 Farm Bill"), which amended the CSA to exclude "hemp" from the statutory definitions of marijuana and THC, effectively legalizing hemp at the federal level.[202] The 2018 Farm Bill defines "hemp" as the plant Cannabis sativa L., and any derivatives of such plant, that have a THC concentration of "not more than .3 percent on a dry weight basis."[203] Thus, hemp and hemp-derived CBD—provided they meet the statutory requirements of the 2018 Farm Bill—will no longer be considered Schedule I controlled substances.

With respect to the production and growth of hemp, the 2018 Farm Bill permits any state or Indian tribe to submit to the Secretary of Agriculture a plan under which the state or Indian tribe would monitor or regulate the production of hemp within its jurisdiction, and any proposed plan shall be approved or disapproved by the Secretary of Agriculture within 60 days' of its submission.[204] A proposed plan must contain the following, among other things: (1) a practice to record the locations where hemp is grown; (2) a procedure for testing the hemp annually to ensure it does not exceed 0.3% THC, and for disposing of plants produced in violation of the 2018 Farm Bill; (3) a procedure for enforcement and to report violations to the Secretary of Agriculture; and (4) a certification that the jurisdiction has adequate resources and personnel to enforce the plan.[205] Notably, the 2018 Farm Bill primarily leaves the regulation of hemp production to states and Indian tribes, and does not preempt them from prohibiting hemp production or imposing more stringent

requirements than those at the federal level.[206] But where a state or Indian tribe does not submit a plan or does not prohibit the production of hemp, the Secretary of Agriculture may establish a plan, and any production of hemp in a state or Indian tribal territory must be consistent with the Secretary's plan.[207] Further, the 2018 Farm Bill prevents a state from prohibiting the transport of hemp through that state, thus permitting interstate commerce of hemp and hemp-derived products throughout the United States.[208]

The 2018 Farm Bill also limits who may obtain a license to be a hemp producer and provides that negligent violations of a state or tribal plan will not be criminally enforced at the federal level, but may render a producer ineligible to produce hemp depending on the number of violations within a five-year period. Violations by hemp producers that are determined by the state or Indian tribe to be more than negligence must be reported by the state or tribe to the U.S. Attorney General and chief law enforcement officer of the jurisdiction, and may be subject to federal criminal prosecution.[209] The 2018 Farm Bill requires the Secretary of Agriculture, in consultation with the Attorney General, to promulgate regulations and guidelines pertaining to hemp.[210]

Considerations for Strengthening Sanctions/AML Compliance

In light of the developments described above, senior management, general counsel, and compliance officers should consider the follow points in strengthening their institutions' sanctions/AML compliance:

1. **Be Prepared to Review and Respond to OFAC's Forthcoming Guidance on Sanctions Compliance Programs**. With OFAC planning to issue guidance early in 2019 regarding its compliance expectations—and in light of multiple recent sanctions and BSA/AML-related enforcement actions highlighting compliance deficiencies—companies would be well-served to be prepared to review their programs and implement any necessary adjustments following the release of OFAC's forthcoming guidance.

2. **Test and Address Sanctions Screening Software Limitations.** OFAC's Cobham settlement makes clear that the utilization of defective screening software will not provide a shield against regulatory enforcement. Companies should devote resources to understanding the functionality and limitations of their sanctions screening software, ensure sufficient staff training, update the software accordingly, and periodically evaluate the software with test data to ensure that it sufficiently flags transactions even absent an exact match. The Cobham settlement also suggests that, depending on their risk profile, companies should consider investing in systems for identifying entities that are treated as SDNs under OFAC's fifty percent rule.

3. **Pay Particular Attention to Staffing**. Compliance resources have also been a recent focus of enforcement, as evidenced by the Rabobank, U.S. Bancorp, and UBS resolutions, which highlight the focus of prosecutors and bank regulators on BSA/AML compliance staffing levels and experience. Agencies expect that financial institutions maintain appropriately qualified staff in the numbers

required to operate an effective compliance program in light of each financial institutions' volume of transactions, historic level of alerts, risk profile, and other factors. Financial institutions should consider undertaking a periodic staffing analysis to ensure that their staffing is sufficient and in line with industry benchmarks. Further, as demonstrated by the U.S. Bancorp and UBS resolutions, financial institutions should ensure there is no policy or practice that can be perceived to operate as a cap on SARs.

4. **Renewed Focus on Iran**. Following JCPOA withdrawal, the Trump administration has indicated its intent to aggressively pursue both U.S. and non-U.S. persons that run afoul of U.S. sanctions. National Security Adviser John Bolton has warned that increased sanctions are forthcoming and that the United States will "have very strict, tight enforcement of the sanctions that exist."[211] Likewise, Under Secretary Mandelker has advised companies to be "sure your [Iran sanctions] compliance programs are airtight."[212] Coupled with the FinCEN advisory on detecting illicit transactions related to Iran, these statements indicate that U.S. and non-U.S. entities alike face renewed enforcement and reputational risks, and non-U.S. entities face secondary sanctions risk for a broad range of Iran-related activities.

5. **Consider the Impact of the EU Blocking Regulation**. As noted, the United States' withdrawal from the JCPOA and the amended EU Blocking Regulation have created a potential conflict of laws between the United States and the EU, creating compliance and risk concerns for companies operating in both jurisdictions. Companies operating in the EU should monitor new developments relating to the EU Blocking Regulation carefully, and should review whether their activities are subject to the covered U.S. sanctions on Iran. This potential conflict of laws presents special concern for U.S. companies with EU subsidiaries, as those subsidiaries are treated as U.S. persons under U.S. sanctions and as EU persons under the EU Blocking Regulations. While it may be possible for an affected entity to obtain a specific license from OFAC or an exception from the EU, it is unclear whether either jurisdiction will be amendable to granting such requests. Going forward, companies should keep a close watch on developments related to the EU Blocking Regulation and should consider updating their sanctions-related contractual provisions to manage the risk of primary and secondary sanctions.

6. **Strengthen Processes Regarding Regulatory Communication**. In light of recent enforcement actions alleging that banks have obstructed, deceived, or failed to inform regulators—and fired or silenced compliance staff—financial institutions should consider reviewing and strengthening their processes. Areas for enhancement may include: central tracking of regulator/monitor requests and submissions to ensure timely and complete flow of information and to create a record; regularly scheduled check-ins with regulators/monitors to ensure a regular flow of information; documenting regulator/monitor meetings and communications; additional training on regulatory interactions and duties of truthfulness; consistent consideration of the need to share new information and developments with other regulators (and the need to seek permission to share confidential information); steps to ensure that the above actions are not perceived as *impeding* regulatory cooperation and transparency;

and documenting the basis of personnel actions relating to compliance officers and considering potential pre-notification to regulators.

7. **Enhancing Controls for Transactions Involving Higher Risk Jurisdictions**. As evidenced by recent enforcement actions, DOJ and banking regulators continue to focus on transactions involving geographies that are perceived as carrying a higher risk of financial crime. For example, one of the more recent DOJ BSA/AML resolutions—Rabobank—involved business done at or across the U.S.-Mexico border; Epsilon and several individual criminal prosecutions demonstrate that the UAE remains a higher-risk jurisdiction for Iran-related transactions; and the resolutions with Jereh, ELF, and Western Union involved transactions with China. And FinCEN's advisory on Iran's attempts to exploit the U.S. financial system recommends enhanced due diligence for transactions originating from or otherwise involving jurisdictions in close proximity to Iran. These enforcement actions and guidance underscore the need to implement and maintain sanctions and BSA/AML controls commensurate with the risks posed by transactions involving higher risk geographies. Non-financial institutions will likely also face increased scrutiny related to transactions in higher risk jurisdictions, and may consider implementing enhanced compliance measures for such transactions (including transactions involving the jurisdictions flagged in the guidance by FinCEN and other regulators focused on North Korean supply chain links). Finally, OFAC's ELF settlement underscores the need for companies, depending on their risk profiles, to employ "full spectrum supply chain due diligence" to identify the use of goods, services, technology, and labor from sanctioned jurisdictions.

8. **Adapting Compliance for Emerging Technologies Such as Virtual Currencies**. Recent regulator emphasis on the potential risks posed by virtual currency transactions underscores the importance of ensuring that policies and procedures appropriately address sanctions and BSA/AML risk for emerging technology. Among other things, financial institutions should ensure that due diligence procedures, customer identification programs, risk assessments, and transaction monitoring and screening are updated to consider the unique risks of virtual currencies, including virtual currency exchangers.

9. **Assess Risks With Respect to the Cannabis Industry**. As cannabis production, distribution, and sales become more important to the economies of states where such conduct is permitted by state law, financial institutions should periodically assess their compliance with the BSA including with respect to customer due diligence and SAR reporting. FinCEN has set forth its BSA expectations for financial institutions that provide financial services to cannabis-related businesses, including criteria FinCEN views as relevant to assessing customer risk. FinCEN has not, however, provided comprehensive BSA guidance with respect to ancillary persons, such as service providers to, or employees of, marijuana companies. Financial institutions should also periodically analyze their risk exposure under the federal substantive money laundering statutes, the Controlled Substances Act, and other legal restrictions.

Financial institutions should likewise consider periodic risk assessment with respect to any business connected to the Canadian cannabis industry.

We will continue to monitor sanctions and AML developments and look forward to providing you with further updates this year.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Jessica S. Carey
+1-212-373-3566
jcarey@paulweiss.com

Michael E. Gertzman
+1-212-373-3281
mgertzman@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Brad S. Karp
+1-212-373-3316
bkarp@paulweiss.com

Richard S. Elliott
+1-202-223-7324
relliott@paulweiss.com

Rachel M. Fiorill
+1-202-223-7346
rfiorill@paulweiss.com

Karen R. King
+1-212-373-3784
kking@paulweiss.com

Associates Matthew J. Carhart, Emily Cox, Udi Karklinsky, Joseph Kolatch, Sofia Martos, Ethan R. Merel, Evan J. Meyerson, James R. Simmons, Jr., Jacobus Schutte, Anand Sithian, Katherine S. Stewart, Bailey Williams, and Hongru Xu contributed to this Client Memorandum.

---

1 U.S. Dep't of the Treasury, Press Release, *Under Secretary Sigal Mandelker Speech before the Foundation for the Defense of Democracies* (June 5, 2018), *available* here. *See, e.g.*, U.S. Dep't of State, U.S. Dep't of the Treasury, and U.S. Dep't of Homeland Sec., *North Korea Sanctions & Enforcement Actions Advisory: Risks for Businesses with Supply Chain Links to North Korea* (July 23, 2018), *available* here; U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, *Advisory on Human Rights Abuses Enabled by Corrupt Senior Foreign Political Figures and their Financial Facilitators* (June 12, 2018), *available* here.

2 Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, and Office of the Comptroller of the Currency, *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing* (Dec. 3, 2018), *available* here.

3 Exec. Order 13851, *Blocking Property of Certain Persons Contributing to the Situation in Nicaragua* (Nov. 27, 2018), *available* here.

[4] U.S. Dep't of the Treasury, Press Release, *Treasury Targets Nicaraguan Vice President and Key Advisor over Violent Response to Protests* (Nov. 27, 2018), *available* here.

[5] Exec. Order 13848, Executive Order 13848, 83 Fed. Reg. 179, *Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election* (Sept. 14, 2018), *available* here.

[6] *See* U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Cobham Holdings, Inc. Settles Potential Civil Liability for Apparent Violations of the Ukraine Related Sanctions Regulations* (Nov. 27, 2018), *available* here.

[7] U.S. Dep't of the Treasury, Press Release, *Under Secretary Sigal Mandelker Remarks ABA/ABA Financial Crimes Enforcement Conference December 3, 2018* (Dec. 3, 2018), *available* here.

[8] *See e.g.*, U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Settlement with Zoltek Companies* (Dec. 20, 2018), *available* here; U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Settlement with Société Générale S.A.* (Nov. 19, 2018), *available* here.

[9] Paul, Weiss, *President Trump Withdraws the United States from the Iran Nuclear Deal* (May 9, 2018), *available* here.

[10] U.S. Dep't of the Treasury, *Resource Center: Iran Sanctions*, *available* here.

[11] These waivers are scheduled to expire in May 2019 and it is unclear whether they will all be renewed. *See* Remarks of U.S. Special Representative for Iran Brian Hook, Atlantic Council 2019 Global Energy Forum (Jan. 12, 2019), *available* here; Florence Tan, *U.S. likely to cut number of Iran oil sanctions waivers in May analysts* (Jan. 17, 2019), *available* here.

[12] *See* U.S. Dep't of the Treasury, Office of Foreign Assets Control, Frequently Asked Questions Related to the "Snap-back" of Iranian sanctions in November, 2018, Question 631, 634 (Nov. 5, 2018), *available* here.

[13] *See* U.S. Dep't of the Treasury, Office of Foreign Assets Control, Frequently Asked Questions Related to the "Snap-back" of Iranian sanctions in November, 2018, Question 636, 638 (Nov. 5, 2018), *available* here. Non-U.S. persons, including non-U.S. financial institutions, are subject to the threat of secondary sanctions (such as SDN designation or some other sanction) for knowingly engaging in certain significant transactions involving certain Iranian persons on the SDN List (unless the SDN is an Iranian financial institution that is blocked solely pursuant to E.O. 13599 and identified with the "IRAN" tag), or a person designated in connection with Iran's support for international terrorism or proliferation of weapons of mass destruction. Such persons will have a notation of "Additional Sanctions Information – Subject to Secondary Sanctions" in their SDN List entry in addition to the tag for the other sanctions program(s).

[14] Some of the banks added to the SDN list have, according to OFAC, served as financial conduits for the IRGC-QF, the Ministry of Defense and Armed Forces Logistics (MODAFL), the Islamic Republic of Iran Broadcasting (IRIB), the Martyrs Foundation, Mahan Air, and Iran's Law Enforcement Forces ("LEF")—all entities that remained designated throughout the JCPOA. *See* OFAC Press Release, *available* here. OFAC initially designated Credit Institution for Development, Hekmat Iranian Bank, Middle East Bank, Kish International Bank and Mehr Iran Credit Union Bank as subject to secondary sanctions on November 5, 2018, but removed the secondary sanctions tag from these banks on November 8, 2018. *Iran-related Administrative Updates* (Nov. 8, 2018), https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20181108.aspx.

[15] U.S. Dep't of State, *Briefing on Iran Sanctions* (Nov. 2, 2018), *available* here.

[16] Michael Peel, *Swift to comply with U.S. sanctions on Iran in blow to EU*, Financial Times (Nov. 5, 2018), *available* here.

[17] Council Regulation (EC) No 2271/96 of November 22, 1996, protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom. As enacted in 1996, the EU Blocking Regulation related to U.S sanctions legislation against Cuba, Libya and Iran, as specified in the Annex thereto. The EU published and made effective three documents on August 7, 2018: (1) the Commission Delegated Regulation (EU) 2018/1100 of June 6, 2018, which amended the Annex to the EU Blocking Regulation to include the covered U.S. sanctions on Iran; (2) the Commission Implementing Regulation (EU) 2018/1101 of August 3, 2018, which sets out the criteria for EU operators to apply for an authorization from the Commission to permit compliance with the covered U.S. sanctions where they can demonstrate that "non-compliance would seriously damage their interests or those of the Community;" and (3) the "Guidance Note—Questions and Answers: adoption of update of the Blocking Statute."

[18] The accompanying EU guidance note provides a more specific definition of "EU operators" for whom the regulation applies, and clarifies that EU subsidiaries of U.S. companies that are formed in accordance with the law of an EU Member State and have their registered office, central administration or principal place of business within the EU are considered EU operators subject to the EU Blocking Regulation. Subsidiaries of EU companies incorporated in the United States are subject to the law under which they are incorporated, and therefore are not considered to be EU operators subject to the EU Blocking Regulation.

[19] John Irish and Riham Alkousaa, *Skirting U.S. Sanctions, Europeans Open New Trade Channel to Iran*, REUTERS (Jan. 31, 2019), *available* here.

[20] *Id.*

[21] U.S. Dep't of the Treasury, Press Release, *Treasury Releases CAATSA Reports, Including on Senior Foreign Political Figures and Oligarchs in the Russian Federation* (Jan. 29, 2018), *available* here. *See also* H.R. 3364, 115th Cong. (1st Sess. 2017), *available* here. For an overview of Russia-Ukraine sanctions following CAATSA, see Paul, Weiss, *U.S. Sanctions Relating to Russia and Ukraine: Navigating the Current Landscape*, (Dec. 20, 2017), *available* here. During his recent testimony before the Senate Banking, Housing and Urban Affairs Committee, Secretary Mnuchin stated that the classified annex was "hundreds of pages" in volume. Donna Borak and Nicole Gaouette, *Mnuchin vows additional Russia sanctions will be imposed in 'near future'*, CNN.com (Jan. 30, 2018), *available* here.

[22] Paul, Weiss, *Trump Administration Imposes New Sanctions on Russian Oligarchs and Government Officials* (Apr. 10, 2018), *available* here.

[23] U.S. Dep't of the Treasury, Press Release, *Treasury Designates Russian Oligarchs, Officials, and Entities in Response to Worldwide Malign Activity* (Apr. 6, 2018), *available* here.

[24] *See* U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Notice of Intended Removals* (Dec. 19, 2018), *available* here.

[25] *See* U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Temporary Extension of Ukraine-related General Licenses* (Dec. 20, 2018), *available* here.

[26] U.S. Dep't of the Treasury, Press Release, *Treasury Targets Russian Operatives over Election Interference, World Anti-Doping Agency Hacking, and Other Malign Activities* (Dec. 19, 2018), *available* here.

[27] *See* OFAC Recent Actions, CAATSA - Russia-related Designations, available here. While this appears to be the first time a Chinese government agency has been added to the SDN List, state sponsored entities have been listed before on the SDN List. For example, China Great Wall Industry Corporation was placed on the SDN List in the past for its Iran-related activities (and was subsequently removed).

[28] The State Department, in consultation with the Treasury, added EED and Mr. Li to its CAATSA Section 231 List after determining that China took delivery from Russia of ten Su-35 combat aircraft in December 2017 and an initial batch of S-400 (a.k.a. SA-21) surface-to-air missile system-related equipment in 2018. *See* Dep't of State, *CAATSA Section 231: Addition of 33 Entities and Individuals to the List of Specified Persons and Imposition of Sanctions on the Equipment Development Department* (Sept. 20, 2018), *available* here. Section 231 of CAATSA requires the President to impose five or more of the sanctions described in CAATSA Section 235 with respect to a person the President determines knowingly, on or after such date of enactment, engages in a significant transaction with a person that is part of, or operates for or on behalf of, the defense or intelligence sectors of the Government of the Russian Federation. The President delegated to the Secretary of State, in consultation with the Secretary of the Treasury, the authority to implement Section 231 on September 29, 2017.

[29] State Department Press Statement, *Imposition of Chemical and Biological Weapons Control and Warfare Elimination Act Sanctions on Russia* (Aug. 8, 2018), *available* here.

[30] *See* 83 C.F.R. § 43723, *available* here.

[31] U.S. Dep't of State, Press Release, *Sanctions Announcement on Russia* (Dec. 19, 2018), *available* here.

[32] *Id.*

[33] U.S. Dep't of the Treasury, Press Release, *Under Secretary Sigal Mandelker Remarks ABA/ABA Financial Crimes Enforcement Conference* (Dec. 3, 2018), *available* here.

[34] House Financial Services Committee, Monetary Policy and Trade Subcommittee, Hearing on Administration Goals for Major Sanctions Programs, 115th Cong. 14 (Sept. 26, 2018) (testimony of Marshall Billingslea, Assistant Secretary of the Treasury for Terrorist Financing).

[35] U.S. Dep't of the Treasury, U.S. Dep't of State, and U.S. Coast Guard, North Korea Sanctions Advisory, *Sanctions Risks Related to North Korea's Shipping Practices* (Feb. 23, 2018), *available* here.

[36] U.S Dep't of Treasury, Dep't of State, and Dep't of Homeland Sec., *North Korea Sanctions & Enforcement Actions Advisory: Risks for Businesses with Supply Chain Links to North Korea* (Jul. 23, 2018), *available* here.

[37] *See* E.O. 13827 of March 19, 2018, Taking Additional Steps to Address the Situation in Venezuela, 83 Fed. Reg. 55 (Mar. 21, 2018), *available* here.

[38] E.O. 13835 of May 21, 2018, Prohibiting Certain Additional Transactions With Respect to Venezuela, 83 Fed. Reg. 101 (May 24, 2018), *available* here.

[39] *See* OFAC, General License No. 5 (July 19, 2018), *available* here.

[40] *See* U.S. Dep't of the Treasury, Press Release, *Treasury Sanctions Four Venezuelan Government Officials Associated with Corruption and Oppression* (Jan. 5, 2018), *available* here; U.S. Dep't of the Treasury, Press Release, *Treasury Sanctions Four Current or Former Venezuelan Officials Associated with Economic Mismanagement and Corruption* (Mar. 19, 2018), *available* here; U.S. Dep't of the Treasury, Press Release, *Treasury Targets Influential Former Venezuelan Official and*

His Corruption Network (May 18, 2018), *available* here; U.S. Dep't of the Treasury, Press Release, *Treasury Targets Venezuelan President Maduro's Inner Circle and Proceeds of Corruption in the United States* (May 18, 2018), *available* here.

41 U.S. Dep't of the Treasury, Frequently Asked Questions: Other Sanctions Programs, Venezuela Sanctions, No. 505 (Jul. 19, 2018), *available* here.

42 *See* E.O. 13850 of November 1, 2018, Blocking Property of Additional Persons Contributing to the Situation in Venezuela, 83 Fed. Reg. 213 (Nov. 2, 2018), *available* here.

43 White House, Press Release, *Remarks by National Security Advisor Ambassador John R. Bolton on the Administration's Policies in Latin America* (Nov. 2, 2018), *available* here.

44 White House, Press Release, *Statement from President Donald J. Trump Recognizing Venezuela National Assembly President Juan Guaidó as the Interim President of Venezuela* (Jan. 23, 2019), available here.

45 U.S. Dep't of the Treasury, Press Release, *Issuance of a New Venezuela-related Executive Order and General Licenses; Venezuela-related Designation* (Jan. 28, 2019), *available* here. On February 1, 2019, OFAC issued two amended (*available* here and here) and eleven new FAQs (available here) related to this action.

46 U.S. Dep't of the Treasury, *Issuance of a New Venezuela-related Executive Order and General Licenses; Venezuela-related Designation* (Jan. 28. 2019), *available* here.

47 U.S. Dep't of the Treasury, Press Release, *Treasury Sanctions Venezuela's State-Owned Oil Company Petroleos de Venezuela, S.A.* (Jan. 28. 2019), *available* here.

48 Executive Order, *Taking Additional Steps to Address the National Emergency with Respect to Venezuela* (Jan. 25, 2019), *available* here. This Executive Order broadens the definition of the term "Government of Venezuela" to include persons that have acted, or have purported to act, on behalf of the Government of Venezuela, including members of the Maduro regime, for purposes of Executive Orders 13692, 13808, 13827, 13835, and 13850.

49 Executive Order 13818, *Blocking the Property of Persons Involved in Serious Human Rights Abuse or Corruption*, Dec. 20, 2017, *available* here.

50 Two of these individuals were delisted on November 2, 2018. *See* U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Global Magnitsky Designations Removals* (Nov. 2, 2018), *available* here.

51 OFAC defines "apparent violation" to mean "conduct that constitutes an actual or possible violation of U.S. economic sanctions laws." In practice, OFAC describes violations as "apparent" unless it issues a pre-penalty notice in a matter, after which it describes violations as "alleged." If OFAC issues a Penalty Notice or a Finding of Violation, it will refer to the conduct at issue merely as "violations."

52 U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Société Générale S.A. Settles Potential Civil Liability for Apparent Violations of Multiple Sanctions Programs* (Nov. 19, 2018), *available* here. The OFAC and Société Générale Settlement Agreement is available here.

53 Paul, Weiss, *OFAC Reaches Settlement with Cobham Holdings, Inc. for Violations Resulting from Deficient Screening Software* (Nov. 29, 2018), *available* here.

54 *See* U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Cobham Holdings, Inc. Settles Potential Civil Liability for Apparent Violations of the Ukraine Related Sanctions Regulations* (Nov. 27, 2018) *available* here.

[55] *Id.* at 3.

[56] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Yantai Jereh Oilfield Services Group Co., Ltd. Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations* (Dec. 12, 2018), *available* here. The OFAC and Jereh Group Settlement Agreement is available here.

[57] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Zoltek Companies, Inc. Settles Potential Civil Liability for Apparent Violations of the Belarus Sanctions Regulations* (Dec. 20, 2018), *available* here.

[58] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Epsilon Electronics, Inc. Settles Potential Civil Liability for Alleged Violations of the Iranian Transactions and Sanctions Regulations and Related Claims* (Sept. 13, 2018), *available* here. In July 2014, OFAC issued Epsilon a penalty notice alleging that between August 2008 and May 2012 Epsilon issued 39 invoices for sales to a company it knew or had reason to know distributed most, if not all, of its products to Iran. Epsilon challenged the penalty notice in the U.S. District Court of the District of Columbia, which granted summary judgement in favor of OFAC. Epsilon appealed to the U.S. Court of Appeals for the District of Columbia, which affirmed in part and revered in part the order granting summary judgement and remanded the case to the district court with instruction to remand the case to OFAC for further consideration.

[59] Eps*ilon Elecs., Inc. v. U.S. Dep't of the Treasury, Office of Foreign Assets Control*, 857 F.3d 913, 925 (D.C. Cir. 2017).

[60] *Id.*

[61] The District Court pointed to the Dubai-based entity's website to support the finding that Epsilon knew or should have known about the Iranian ties. The website: (1) "listed addresses on its 'Contact Us page for one location in Dubai, United Arab Emirates, and one location in Tehran, Iran [;]" (2) "touted" the entity's success "in the Iranian car audio and video market and listed dealers located exclusively in Iran" on the "About Us" page; and (3) displayed photographs of what appeared to be car shows in various Iranian cities." *Epsilon Elecs., Inc. v. U.S. Dep't of the Treasury*, 168 F. Supp. 3d 131, 140 (D.D.C. 2016), *aff'd in part, rev'd in part sub nom. Epsilon Elecs., Inc. v. U.S. Dep't of the Treasury , Office of Foreign Assets Control*, 857 F.3d 913 (D.C. Cir. 2017).

[62] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *JPMorgan Chase Bank, N.A. Settles Potential Civil Liability for Apparent Violations of Multiple Sanctions Programs* (Oct. 5, 2018), *available* here.

[63] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Separately, JPMorgan Chase & Co. Receives a Finding of Violation Regarding Violations of the Foreign Narcotics Kingpin and Syrian Sanctions Regulations* (Oct. 5, 2018), *available* here.

[64] Paul, Weiss, *OFAC Reaches Settlement with e.l.f. Cosmetics, Inc. for North Korea Sanctions Violations Resulting from Inadequate Supply Chain Due Diligence* (Feb. 4, 2019), *available* here.

[65] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *e.l.f. Cosmetics, Inc. Settles Potential Civil Liability for Apparent Violations of North Korea Sanctions Regulations* (Jan. 31, 2019), *available* here.

[66] *Id.*

[67] U.S Dep't of Treasury, Dep't of State, and Dep't of Homeland Sec., *North Korea Sanctions & Enforcement Actions Advisory: Risks for Businesses with Supply Chain Links to North Korea* (Jul. 23, 2018), *available* here.

[68] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *e.l.f. Cosmetics, Inc. Settles Potential Civil Liability for Apparent Violations of North Korea Sanctions Regulations* (Jan. 31, 2019), *available* here.

[69] Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29397 (May 11, 2016).

[70] U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, *Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions, FIN-2018-G001 (Apr. 3, 2018), available* here.

[71] U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, *Exceptive Relief from Beneficial Ownership Requirements for Legal Entity Customers of Rollovers, Renewals, Modifications, and Extensions of Certain Accounts, FIN-2018-R003* (Sept. 7, 2018), *available* here.

[72] U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System, FIN-2018-A006 (Oct. 11, 2018), *available* here.

[73] U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, *Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combatting the Financing of Terrorism Deficiencies* (Oct. 31, 2018), *available* here.

[74] *Id.*

[75] *Id.*

[76] Other countries on the list are Ethiopia, Pakistan, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, and Yemen.

[77] *Id.*

[78] U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, *Advisory on Human Rights Abuses Enabled by Corrupt Senior Foreign Political Figures and their Financial Facilitators*, FIN-2018-A003 (June 12, 2018), *available* here.

[79] *Id.* The advisory lists numerous other red flags including: the use of third parties when it is not a normal business practice; the use of family members or close associates as legal owners; the use of corporate vehicles to obscure ownership, involved industries, or countries; declarations of information from PEPs that are inconsistent with other information; a PEP tries to use services of the financial institution that do not normally cater to foreign or high-value clients; a PEP or facilitator has an ownership interest in or otherwise controls a counterparty in a transaction; transactions involving government contracts that direct companies to operate in an unrelated line of business; transactions involving government contracts that include shell corporations; over simplistic documentation corroborating transactions involving government contracts; payments involving government contracts that originate from non-governmental third parties; and transactions involving property or assets expropriated by corrupt regimes.

[80] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, and Office of the Comptroller of the Currency, *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing* (Dec. 3, 2018), *available* here.

[81] *Id.*

[82] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, and Office of the Comptroller of the Currency, *Interagency Statement on Sharing Bank Secrecy Act Resources* (Oct, 3, 2018), *available* here.

[83] U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, Assessment of Civil Money Penalty, *In the Matter of U.S. Bank National Association*, No. 2018-01 (Feb. 15, 2018), *available* here; U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, Press Release, *Bank Capped Number of Alerts Rather than Invest Resources to Investigate Suspicious Activity* (Feb. 15, 2018), *available* here.

[84] *United States* v. *U.S. Bank National Association*, No. 18-cv-1358 (S.D.N.Y.).; U.S. Dep't of Justice, Press Release, *Manhattan U.S. Attorney Announces Criminal Charges Against U.S. Bancorp For Violations Of The Bank Secrecy Act* (Feb. 15, 2018), *available* here.

[85] *In the Matter of U.S. Bank National Association*, No. AA-EC-2018-84.

[86] *In the Matter of U.S. Bancorp and USB Americas Holding Company*, Nos. 18-005-B-HC; 18-005- B-AC; 18-005-CMP-B-HC.

[87] U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, Press Release, *FinCEN Assesses $14.5 Million Penalty against UBS Financial Services for Anti-Money Laundering Failures* (Dec. 17, 2018) *available* here.

[88] *See* Paul, Weiss, *FCPA Enforcement and Anti-Corruption Developments: 2018 Year in Review* (Jan. 17, 2019), *available* here; Paul, Weiss, *DOJ Announces New Standards for Corporate Cooperation* (Dec. 5, 2018), *available* here; Paul, Weiss, *DOJ Announces New Guidance for Imposing Compliance Monitors in Criminal Division Matters* (Oct. 17, 2018), *available* here.

[89] See Rod J. Rosenstein, U.S. Deputy Att'y Gen., Dep't of Justice, Remarks to the New York City Bar White Collar Crime Institute (May 9, 2018) (hereinafter, "Rosenstein 'Piling On' Remarks"), *available* here; Memorandum from Rod J. Rosenstein, Deputy Att'y Gen., U.S. Dep't of Justice, to Heads of Dep't Components, U.S. Att'ys, (May 9, 2018) (hereinafter, "DOJ 'Piling On' Policy*"), available* here*; see also* Paul, Weiss, *DOJ Issues New Policy on Coordination of Corporate Penalties to Address "Piling On"* (May 10, 2018), *available* here.

[90] *Id.*

[91] Paul, Weiss, *DOJ Issues New Policy on Coordination of Corporate Penalties to Address "Piling On"* (May 10, 2018), *available* here.

[92] Paul, Weiss, *Rabobank Pleads Guilty to Obstructing OCC Supervision and Agrees to Pay $368 Million for Permitting and Concealing BSA/AML Failures* (Feb. 13. 2018), *available* here.

[93] *United States* v. *Rabobank, N.A.*, No. 18 Cr. 0614 (S.D. Cal.).

[94] Statement of Facts at ¶¶ 38, 43, *United States* v. *Rabobank, N.A.*, No. 18 Cr. 0614 (S.D. Cal. 2018), *available* here.

[95] Plea Agreement at ¶ 10, *United States* v. *Rabobank, N.A.*, No. 18 Cr. 0614 (S.D. Cal.), *available* here.

[96] Paul, Weiss, *U.S. Bancorp Enters into Deferred Prosecution Agreement and Related Resolutions and Agrees to Pay $613 million for BSA/AML Failures* (Feb. 21, 2018), *available* here.

[97] *United States* v. *U.S. Bank National Association*, No. 18-cv-1358 (S.D.N.Y.).

[98] *In the Matter of U.S. Bank National Association*, No. 2018-01.

[99] *In the Matter of U.S. Bank National Association*, No. AA-EC-2018-84.

[100] *In the Matter of U.S. Bancorp and USB Americas Holding Company*, Nos. 18-005-B-HC; 18-005-B-AC; 18-005-CMP-B-HC.

[101] U.S. Dept. of Justice, *MoneyGram International Inc. Agrees to Extend Deferred Prosecution Agreement, Forfeits $125 Million in Settlement with Justice Department and Federal Trade Commission* (Nov. 8, 2018), *available* here.

[102] *Id.*

[103] U.S. Dep't of Justice, Press Release, *Manhattan U.S. Attorney Announces Criminal Charges Against Société Générale S.A. For Violations Of The Trading With The Enemy Act* (Nov. 19, 2018), *available* here.

[104] *Id.*

[105] U.S. Dep't of Justice, Press Release, *Manhattan U.S. Attorney Announces Bank Secrecy Act Charges Against Kansas Broker Dealer* (Dec. 19, 2018), *available* here.

[106] *Id.*

[107] *Id.*

[108] *See* Sec. & Exch. Comm'n, Order Instituting Admin. and Cease-and-Desist Proceedings Against Cent. States Capital Mkts. (Dec. 19, 2018), *available* here.

[109] *See* Press Release, U.S. Dep't of Justice, *Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged with Financial Fraud* (Jan. 28, 2019), *available* here.

[110] Indictment, *United States* v. *Huawei Technologies Co. Ltd., et al.*, No. 18-cr-457 (E.D.N.Y. Jan 24., 2019).

[111] *Id.* at 13.

[112] *Id.* at 6.

[113] *Id.* at 7–8.

[114] *Id.* at 8–9.

[115] *Id.* at 26.

[116] U.S. Dep't of Justice, Press Release, Iranian National Arrested for Scheme to Evade U.S. Economic Sanctions by Illicitly Sending More Than $115 Million From Venezuela Through the U.S. Financial System (Mar. 20, 2018), *available* here.

[117] U.S. Dep't of Justice, Press Release, *Iranian National Pleads Guilty to Conspiring to Illegally Export Products From the United States to Iran* (Nov. 8, 2018), *available* here.

[118] U.S. Dep't of the Treasury, Office of the Comptroller of the Currency, *OCC Report Discusses Key Risks for Federal Banking System* (Jan. 18, 2018), *available* here.

[119] *Id.*

[120] U.S. Senate Committee on Banking, Housing, and Urban Affairs, Hearing: Update from the Comptroller of the Currency, 115th Cong. 19 (June 14, 2018) (testimony of Joseph M. Otting, Comptroller of the Currency), *available* here.

[121] Policy Statement on Interagency Notification of Formal Enforcement Actions, 83 Fed. Reg. 113 (June 12, 2018), *available* here.

[122] *Id.*

[123] U.S. Senate Committee on Banking, Housing, and Urban Affairs, Testimony of Grovetta N. Gardineer, Senior Deputy Comptroller for Compliance and Community Affairs (Nov. 29, 2018), *available* here.

[124] Rachel Witkowski, *Fed Not an Impediment to Fintech's Charter Ambitions: OCC's Otting*, AMERICAN BANKER (Jan. 16, 2019), *available* here.

[125] Paul, Weiss, *Rabobank Pleads Guilty to Obstructing OCC Supervision and Agrees to Pay $368 Million for Permitting and Concealing BSA/AML Failures* (Feb. 13, 2018), *available* here.

[126] *See* Bd. Of Governors of the Fed. Reserve System, Cease and Desist Order and Order of Assessment of a Civil Money Penalty Issued Upon Consent Pursuant to the Federal Deposit Insurance Act, as amended, *In the Matter of Mega International Commercial Bank* (Jan 17, 2018), *available* here.

[127] Consent Order, *In the Matter of Capital One, N.A.*, AA-EC-2018-62 (Oct. 23, 2018), *available* here. The OCC also found that the bank subsequently failed to file certain SARs and sent wire transfers in violation of the Travel Rule.

[128] Consent Order for a Civil Money Penalty, *In the Matter of Bank of China, New York Branch*, AA-EC-2018-19 (Apr. 24, 2018), *available* here.

[129] Consent Order, *In the Matter of Bank of China, New York Branch,* AA-EC-2018-18 (Apr. 24, 2018), *available* here.

[130] Consent Order, *In the Matter of Industrial and Commercial Bank of China Ltd.*, 18-013-B-FB, 18-013-B-FBR (Mar. 12, 2018), *available* here; Consent Order, *In the Matter of Hua Nan Commercial Bank Limited*, 18-012-B-FB, 18-012-B-FBR (Apr. 19, 2018), *available* here.

[131] U.S. Sec. and Exch. Comm., *2019 Examination Priorities*, *available* here.

[132] *See* Fin. Indus. Reg. Auth., *Report on FINRA Examination Findings* (Dec. 2018), *available* here. FINRA's 2019 Risk Monitoring and Examination Priorities Letter also notes that FINRA will continue to review for compliance with AML, which remains an ongoing area of focus for the agency. *See* Fin. Indus. Reg. Auth., *2019 Risk Monitoring and Examination Priorities Letter* (Jan. 2019), *available* here.

[133] Paul, Weiss, *Court Upholds SEC Authority and Finds Broker-Dealer Liable for Thousands of Suspicious Activity Reporting Violations* (Jan. 7, 2019), *available* here.

[134] For a more detailed discussion, *see id.*

[135] *See* Opinion and Order, *U.S. Sec. & Exch. Comm'n* v. *Alpine Securities Corp.*, No. 1:17-cv-04179 (S.D.N.Y. Dec. 11, 2018).

[136] *Id.* at 30-31.

[137] *In re Alpine Securities Corp.*, No. 18-1875 (2d Cir. Aug. 7, 2018).

[138] Fin. Indus. Reg. Auth., Press Release, *FINRA Fines Morgan Stanley $10 Million for AML Program and Supervisory Failures* (Dec. 26, 2018), *available* here.

[139] U.S. Sec. and Exch. Comm., Press Release, *Broker-Dealer Admits It Failed to File SARs* (Mar. 28, 2018), *available* here.

[140] U.S. Sec. and Exch. Comm., Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, Section 203(f) of the Investment Advisors Act of 1940, and Section 9(b) of the Investment Company Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Case-and-Desist Order, In the Matter of Aegis Capital Corporation (Mar. 28, 2018), *available* here.

[141] U.S. Sec. and Exch. Comm., Press Release, *Broker-Dealer Admits It Failed to File SARs* (Mar. 28, 2018), *available* here.

[142] Fin. Indus. Reg. Auth., Press Release, FINRA Fines Aegis Capital Corp. $550,000 for Anti-Money Laundering and Supervision Rule Violations (Mar. 28, 2018), *available* here.

[143] U.S. Sec. and Exch. Comm., Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, Section 203(f) of the Investment Advisors Act of 1940, and Section 9(b) of the

Investment Company Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Case-and-Desist Order, In the Matter of Kevin McKenna and Robert Eide (Mar. 28, 2018), *available* here.

144 U.S. Sec. and Exch. Comm., Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, Section 203(f) of the Investment Advisors Act of 1940, and Section 9(b) of the Investment Company Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Case-and-Desist Order, In the Matter of Eugene Terracciano (July 6, 2018), *available* here.

145 U.S. Sec. and Exch. Comm., Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing Remedial Sanctions and a Case-and-Desist Order, *In the Matter of Chardan Capital Markets, LLC* (May 16, 2018), *available* here; U.S. Sec. and Exch. Comm., Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing Remedial Sanctions and a Case-and-Desist Order, *In the Matter of Industrial and Commercial Bank of China Financial Services, LLC* (May 16, 2018), *available* here; U.S. Sec. and Exch. Comm., Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, Section 203(f) of the Investment Advisors Act of 1940, and Section 9(b) of the Investment Company Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Case-and-Desist Order, *In the Matter of Jerard Basmagy* (May 16, 2018), *available* here.

146 U.S. Sec. and Exch. Comm., Press Release, *SEC Charges Brokerage Firms and AML Officer with Anti-Money Laundering Violations* (May 16, 2018), *available* here.

147 Both firms consented to censures. None of the parties admitted or denied the SEC's findings.

148 U.S. Sec. and Exch. Comm., Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, Section 203(f) of the Investment Advisors Act of 1940, and Section 9(b) of the Investment Company Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Case-and-Desist Order, *In the Matter of Jerard Basmagy* (May 16, 2018), *available* here.

149 FINRA also determined that LPL did not file or amend Forms U4 or U5 for purposes of disclosing reportable customer complaints.

150 LPL consented to the entry of FINRA's findings without admitting or denying the charges.

151 Fin. Indus. Reg. Auth., Press Release, FINRA Fines LPL $2.75 Million for Complaint-Reporting and AML Program Failures (October 30, 2018), *available* here.

152 Paul, Weiss, *New York DFS Finalizes Stringent Anti-Money Laundering and Sanctions Regulation* (July 1, 2016), *available* here.

153 Governor Andrew M. Cuomo, Press Release, *Governor Cuomo Announces First Round of Term 3 Administration Appointments* (Jan. 4, 2019), *available* here.

154 Société Générale, Press Release, *Société Générale reaches agreements with U.S. authorities to resolve U.S. Economic sanctions and AML investigations* (Oct. 26, 2017), *available* here.

[155] N.Y. Dep't of Fin. Servs., Press Release, *DFS Fines Société Générale SA and Its New York Branch $420 Million for Violations of Laws Governing Economic Sanctions and Violations of New York Anti-Money Laundering and Recordkeeping Laws* (Nov. 19, 2018), *available* here.

[156] N.Y. Dep't of Fin. Servs., Press Release, *DFS Fines Société Générale SA and Its New York Branch $420 Million for Violations of Laws Governing Economic Sanctions and Violations of New York Anti-Money Laundering and Recordkeeping Laws* (Nov. 19, 2018).

[157] N.Y. Dep't of Fin. Servs., Consent Order Under New York Banking Law §§ 39 and 44 in the Matter of Société Générale SA, and Société Générale, New York Branch (Nov. 19, 2018) (BSA/AML Consent Order), *available* here.

[158] N.Y. Dep't of Fin. Servs., Press Release, *DFS Fines Société Générale SA and Its New York Branch $420 Million for Violations of Laws Governing Economic Sanctions and Violations of New York Anti-Money Laundering and Recordkeeping Laws* (Nov. 19, 2018), *available* here.

[159] N.Y. Dep't of Fin. Servs., Consent Order Under New York Banking Law §§ 39 and 44 in the Matter of Société Générale SA, and Société Générale, New York Branch (Nov. 19, 2018) (BSA/AML Consent Order), at 2, *available* here.

[160] *E.g.*, *id.* at 6-7.

[161] *Id.* at 13-15.

[162] *Id.* at 8.

[163] N.Y. Dep't of Fin. Servs., Consent Order Under New York Banking Law §§ 39 and 44 in the Matter of Mashreqbank, PSC and Mashreqbank, PSC, New York Branch (Oct. 10, 2018), *available* here.

[164] *Id.* at 3.

[165] *Id.* at 4-8.

[166] *Id.* at 12-17.

[167] *Id.* at 8-9.

[168] N.Y. Dep't of Fin. Servs., Consent Order Under New York Banking Law §§ 39 and 44 in the Matter of Western Union Financial Services, Inc. (Jan. 4, 2018), *available* here.

[169] *Id.* at 3.

[170] *Id.* at 8.

[171] *Id.* at 17-18.

[172] *Id.* at ¶ 69(b).

[173] *Id.* at ¶ 69(g)(i).

[174] N.Y. Dep't of Fin. Servs., Guidance on Whistleblowing Programs (Jan. 7. 2019), *available* here. The issuance of this guidance may be linked to DFS's December 18, 2018 consent order against Barclays Bank PLC and its New York branch.

[175] FinCEN Advisory, FIN-2018-A006, Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System, Oct. 11, 2018, *available* here.

[176] Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference, August 9, 2018, *available* here.

[177] Office of the New York State Attorney General, Press Release, *A.G. Underwood Issues Virtual Markets Integrity Report, Finding Many Platforms Vulnerable To Abusive Trading, Conflicts Of Interest, And Other Consumer Risks* (Aug. 9, 2018), *available* here.

[178] *See* N.Y. Dep't of Fin. Servs., Press Release, *DFS Grants Virtual Currency License to Coinsource, Inc.* (Nov. 1, 2018, *available* here.

[179] Fin. Action Task Force, *Regulation of Virtual Assets* (Oct. 19, 2018), *available* here.

[180] FinCEN Guidance, FIN-2013-G001, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, March 18, 2013, *available* here; *see also* In the Matter of BTC-e, Number 2017-03, *available* here.

[181] There are increasing indications of virtual currencies' use in money laundering operations. For example, on July 13, 2018, Robert S. Mueller III, special counsel investigating Russian interference in the 2016 election, issued an indictment of 12 Russian intelligence officers in the hacking of the Democratic National Committee and Hilary Clinton campaign. The officers were accused of laundering money through cryptocurrency transactions to avoid detection by using fictitious names and hundreds of email accounts.

[182] Among other things, federal law prohibits criminally the advertising of the sale or distribution of a CSA schedule I substance (21 U.S.C. § 843(c)), leasing or renting real property for the purpose of manufacturing, distributing or using a controlled substance (21 U.S.C. § 856), and selling or transporting drug paraphernalia in interstate commerce (21 U.S.C. § 863).

[183] Bill Chappell, *Voters Relax Marijuana Laws in 3 More States: Michigan, Utah, Missouri*, NPR (Nov. 7, 2018), *available* here.

[184] State Medical and Recreational Marijuana Laws Chart: Overview, Practical Law Practice Note Overview 7-523-7150.

[185] The Supreme Court has held that even marijuana-related activity that occurs entirely within a single state remains subject to federal law. *See Gonzales* v. *Raich*, 545 U.S. 1, 17 (2005).

[186] Congress has enacted a law—the Rohrabacher-Blumenauer amendment—to defund any federal prosecution of medical marijuana production or distribution in compliance with state law. Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, § 542, 129 Stat. 2242, 2332–33 (2015). But such funding restrictions do not decriminalize the underlying activity, but merely prevents DOJ from using appropriated funds to prosecute such offenses where the medical marijuana activity is legal under state law. As the Ninth Circuit Court of Appeals noted: "anyone in any state who possesses, distributes, or manufactures marijuana for medical or recreational purposes (or attempts or conspires to do so) is [still] committing a federal crime. . . . Congress currently restricts the government from spending certain funds to prosecute certain individuals. But Congress could restore funding tomorrow, a year from now, or four years from now, and the government could then prosecute individuals" for such conduct. *United States* v. *McIntosh*, 833 F.3d 1163, 1177, 1179 n.5 (9th Cir. 2016). The Rohrabacher-Blumenauer amendment expired in 2018 due to the partial lapse in federal appropriations, but was reinstated when President Trump signed a continuing resolution on January 25, 2019. The amendment is set to expire on February 15, 2019, absent an agreement on federal appropriations on or before that date.

[187] The statutory definition of "marijuana" is located at 21 U.S.C. § 812(c)(17).

[188] *See Hemp Industries Ass'n* v. *Drug Enforcement Admin.*, 357 F.3d 1012, 1017 (9th Cir. 2004) (holding that the products derived from the "mature stalks" or "oil and cake made from the seeds" of the cannabis plants "fit[] within the plainly stated exception in the CSA definition of marijuana").

189 Memorandum for All United States Attorneys: Marijuana Enforcement, U.S. Department of Justice, Office of the Attorney General, Jefferson B. Sessions, III, Jan. 4, 2018, *available* here.

190 These priorities include: "[p]reventing the distribution of marijuana to minors; [p]reventing revenue from the sale of marijuana from going to criminal enterprises, gangs, and cartels; and [p]reventing the diversion of marijuana from states where it is legal under state law in some form to other states," among other priorities. Guidance Regarding Marijuana Enforcement, U.S. Department of Justice, Office of the Deputy Attorney General, James M. Cole, Aug. 29, 2013, *available* here. Deputy Attorney General Cole later issued the 2014 Cole Memorandum, which instructed federal prosecutors to adhere to the eight priorities identified in the 2013 Cole Memorandum when contemplating marijuana-related Bank Secrecy Act and money laundering prosecutions. Guidance Regarding Marijuana Related Financial Crimes, U.S. Department of Justice, Office of the Deputy Attorney General, James M. Cole, Feb. 14, 2014, *available* here.

191 Memorandum for All United States Attorneys: Marijuana Enforcement, U.S. Department of Justice, Office of the Attorney General, Jefferson B. Sessions, III, Jan. 4, 2018, *available* here.

192 Testimony of Hon. William Pelham Barr before the Senate Committee on the Judiciary (Jan. 15, 2019), *available* here.

193 Testimony of Hon. William Pelham Barr before the Senate Committee on the Judiciary (Jan. 15, 2019), *available* here.

194 BSA Expectations Regarding Marijuana-Related Businesses, Guidance FIN-2014-G001, Department of the Treasury, Financial Crimes Enforcement Network, February 14, 2014, *available* here.

195 Letter from Drew Maloney, Ass't Sec'y for Leg. Aff., Financial Crimes Enforcement Network, to Hon. Denny Heck (Jan. 31, 2018), *available* here.

196 Testimony of Kenneth A. Blanco before The U.S. Senate Committee on Banking, Housing, and Urban Affairs (Nov. 29, 2018), *available* here.

197 Zachary Warmbrodt, *Bankers' Pot Push Gets Boost from Blue Wave, Sessions Ouster*, POLITICO (Nov. 27, 2018), *available* here; Tom Angell, *Trump Treasury Secretary Wants Marijuana Money In Banks*, FORBES (Feb. 6, 2018), *available* here; Omar Sacirbey, *Fourth Corner Credit Union Gets Conditional Approval from Federal Reserve for Marijuana-Related Banking*, Marijuana Business Daily (Feb. 6, 2018), *available* here.

198 Seung Min Kim, *Trump, Gardner Strike Deal on Legalized Marijuana, Ending Standoff over Justice Nominees*, THE WASHINGTON POST (Apr. 13, 2018), *available* here.

199 Congressman Ed Perlmutter, Press Release, *Congress Must Act to Reduce Public Safety Threat in Communities* (April 27, 2017), *available* here.

200 N.Y. Dep't of Fin. Servs., Press Release, *New York State Department of Financial Services, Governor Cuomo Announces Further Action to Support Development of Medical Marijuana and Industrial Hemp Businesses in New York* (July 3, 2018), *available* here.

201 Memorandum to Chief Executive Officers or Equivalents of New York State-Chartered Banks & Credit Unions: Guidance on Provision of Financial Services to Medical Marijuana & Industrial Hemp-Related Businesses in New York State, New York State Department of Financial Services, Superintendent of Financial Services, Maria T. Vullo (July 3, 2018), *available* here.

202 Agricultural Improvement Act of 2018, Pub. L. No. 115-334, § 12619, 132 Stat. 4490, 5018 (2018).

203 Agricultural Improvement Act of 2018, Pub. L. No. 115-334, § 10113, 132 Stat. 4490, 4907 (2018).

[204] Agricultural Improvement Act of 2018, Pub. L. No. 115-334, § 10113, 132 Stat. 4490, 4908-09 (2018). States or Indian tribes whose plans are disapproved may resubmit an amended state plan that complies with the requirements set forth in the 2018 Farm Bill.

[205] Agricultural Improvement Act of 2018, Pub. L. No. 115-334, § 10113, 132 Stat. 4490, 4908-09 (2018).

[206] Agricultural Improvement Act of 2018, Pub. L. No. 115-334, § 10113, 132 Stat. 4490, 4909 (2018).

[207] Agricultural Improvement Act of 2018, Pub. L. No. 115-334, § 10114, 132 Stat. 4490, 4912-13 (2018).

[208] Agricultural Improvement Act of 2018, Pub. L. No. 115-334, § 10114, 132 Stat. 4490, 4913 (2018).

[209] Agricultural Improvement Act of 2018, Pub. L. No. 115-334, § 10113, 132 Stat. 4490, 4909-10 (2018).

[210] Agricultural Improvement Act of 2018, Pub. L. No. 115-334, § 10113, 132 Stat. 4490, 4914 (2018).

[211] Emily Birnbaum, *Bolton: Even More Iran Sanctions Planned*, The Hill (Nov. 5, 2018), *available* here.

[212] Sigal Mandelker, Under Sec'y for Terrorism and Fin. Intelligence, U.S. Dep't of the Treasury, Speech before the Foundation for the Defense of Democracies (June 5, 2018), *available* here.