Paul | Weiss

Economic Sanctions and Anti-Money Laundering Developments

2019 YEAR IN REVIEW

January 31, 2020

Economic Sanctions and Anti-Money Laundering Developments: 2019 Year in Review

Table of Contents

Executive Summary

This memorandum surveys economic sanctions and anti-money laundering ("AML") developments and trends in 2019 and provides an outlook for the year ahead. These areas remained a high priority last year, with the Trump administration continuing to strengthen sanctions across a number of areas and federal and state agencies imposing over $2.4 billion in penalties for sanctions/AML violations. We also provide some thoughts concerning compliance and risk mitigation in this challenging environment.

Last year witnessed a flurry of sanctions enforcement activity, including two significant multi-agency resolutions against non-U.S. financial institutions and a substantial increase in enforcement by Treasury's Office of Foreign Assets Control ("OFAC"). OFAC issued penalties totaling over $1.28 billion, a record high. OFAC also issued landmark guidance on the "hallmarks of an effective compliance program" and began requiring adherence to a list of 23 nearly-standard compliance commitments as part of its settlement agreements. The Department of Justice ("DOJ"), for its part, resolved and initiated major sanctions criminal prosecutions last year, and also revised its sanctions and export control criminal enforcement policy to further encourage self-reporting of potentially willful violations. And the SEC reached a consent order against a U.S. issuer finding violations under the Foreign Corrupt Practices Act's books and records provisions related to efforts to conceal violations of U.S. sanctions laws, signaling a willingness by the SEC to join an already crowded field of federal sanctions enforcement agencies.

Last year also witnessed significant and constant changes to the sanctions policy landscape. Throughout 2019, the Trump Administration continued its "maximum pressure" sanctions campaign against Iran, issuing new executive orders targeting entire sectors of the Iranian economy with secondary sanctions and making dozens of new sanctions designations. The year 2019 also featured a dramatic increase in the scope of Venezuela sanctions when, in January, the Administration recognized National Assembly President Juan Guaidó as the Interim President of Venezuela and, in August, the Administration imposed blocking sanctions on the Government of Venezuela and its subsidiaries, including state-owned oil giant, Petroleos de Venezuela, S.A. ("PDVSA"). Given the widespread presence of the Government of Venezuela in the Venezuelan economy, some sanctions compliance departments will need to consider whether, for risk-mitigation purposes, to treat Venezuela effectively as a comprehensively sanctioned country. The Administration also continued to make use of the Global Magnitsky Act to target human rights abuses and corruption worldwide and imposed additional restrictions on dealings with Cuba, further breaking from the Obama Administration's policy toward Cuba. The Trump Administration continues to wield sanctions as a powerful foreign policy tool.

Enforcement of the Bank Secrecy Act ("BSA")/AML laws, and their state law equivalents, made fewer headlines in 2019, and related fines receded from the multi-billion highs of just a few years ago. Nevertheless, Treasury's Financial Crimes Enforcement Network ("FinCEN"), the federal banking agencies, and the New York Department of Financial Services ("DFS") have made targeted organizational changes and/or issued new guidance suggesting that AML enforcement remains a priority.

Last year, the Securities and Exchange Commission ("SEC") and the Financial Industry Regulatory Authority ("FINRA") also continued to pursue AML-related enforcement actions against broker-dealers, with a particular emphasis on AML risk associated with low-priced securities trading. And, as we describe in our annual alert on anti-corruption and Foreign Corrupt Practices Act ("FCPA") developments, DOJ and U.S. Attorneys' Offices continued to bring actions under the criminal money laundering statutes in cases of alleged corruption overseas, even in the absence of FCPA charges. DOJ and other enforcement authorities are also investigating AML scandals that broke abroad, such as with Danske Bank's Estonian branch.

This memorandum also surveys additional developments that are of importance to regulators and the private sector. First, 2019 saw a dramatic and unprecedented use of the Department of Commerce's Bureau of Industry and Security ("BIS") Entity list, with designations of Huawei and several other Chinese technology companies that show that the Entity List is increasingly being used as an instrument of foreign policy. As a field adjacent to sanctions, we survey the most significant U.S. export control developments of last year. Additionally, we review guidance issued throughout 2019 from multiple agencies focused on the unique money-laundering risks associated with virtual currency transactions and businesses.

Treasury's Office of Foreign Assets Control

Last year saw important changes to various sanctions programs administered by OFAC, particularly the Iran, Venezuela, Cuba, Global Magnitsky, and Counter-Terrorism programs, as described in greater detail below. Meanwhile, the Trump Administration continued its "maximum pressure" campaign against North Korea, with OFAC making over a dozen North Korea-related designations of entities based in China, Taiwan, and Hong Kong and issuing revised guidance to address North Korea's illicit shipping practices. The Administration also made additional sanctions designations targeting Russia, including for Russia's efforts to interfere in the 2018 mid-term elections, and a second wave of sanctions in response to Russia's 2018 nerve agent attack in the United Kingdom, including by imposing restrictions on U.S. financial institutions' (including their non-U.S. branches) participation in Russian sovereign debt issuances.[1]

The Trump Administration continued to utilize sanctions as a targeted tool to address rapidly evolving foreign policy concerns. Notably, in connection with Turkey's October 2019 military operations in Syria, the Trump Administration sanctioned Turkey's Ministry of Energy and Natural Resources and Ministry of National Defense, as well as three senior officials, noting that the designations were the "result of the Turkish Government's actions that further deteriorate peace, security, and stability of the region" and stating that the United States was "prepared to impose additional sanctions on Government of Turkey officials and entities, as necessary."[2] Nine days after the designation, and after determining that Turkey had adhered to a ceasefire, OFAC delisted these entities and individuals, demonstrating a willingness to promptly remove sanctions when consistent with U.S foreign policy objectives.[3]

OFAC also engaged in record-breaking enforcement activity in 2019, with penalties totaling over $1.28 billion, the most assessed in any year to date, across 26 public enforcement actions (up from 7 in 2018).

The agency also issued various guidance documents, most notably its May 2019 guidance on the features of an effective sanctions compliance program. OFAC Director Andrea Gacki also clarified in a public appearance that OFAC will no longer "credit" all fines paid to other government agencies in multi-agency settlements, but will instead only credit payments toward penalties that "relate to the same pattern of conduct for the same period of time" as OFAC's assessed penalty.[4]

Last year also saw the departure of Sigal Mandelker, the Under Secretary of the Treasury for Terrorism and Financial Intelligence. Since joining the administration in 2017, Under Secretary Mandelker had supervised, among other things, the ramping up of sanctions targeting Iran after the Trump Administration withdrew from the Joint Comprehensive Plan of Action ("JCPOA"), as well as OFAC's new initiative to provide greater compliance guidance and to require compliance commitments in settlements. The Deputy Secretary of the Treasury, Justin Muzinich, is currently serving in the Under Secretary role on an acting basis.[5] In December 2019, the Trump Administration announced its intention to nominate Jessie Liu, who is currently serving as the U.S. Attorney for the District of Columbia, to the position.[6]

Guidance on Sanctions Compliance Programs

As discussed in our prior memorandum,[7] on May 2, 2019, OFAC issued guidance titled "A Framework for OFAC Compliance Commitments" (the "Framework"), that strongly encourages companies to "develop, implement, and routinely update" risk-based sanctions compliance programs. OFAC made clear that the guidance was intended for U.S. companies as well as non-U.S. companies that conduct business in or with the United States, with U.S. persons, or using U.S. origin goods or services. The guidance describes five "essential components" of an effective sanctions compliance program: (i) management commitment, (ii) risk assessment, (iii) internal controls, (iv) testing and audit, and (v) training.[8] As an appendix to the Framework, OFAC also describes some of the common "root causes" of the apparent violations that were the subject of its prior enforcement actions. This appendix is meant to assist companies in "designing, updating and amending" their compliance programs.[9]

The Framework, and the related "compliance commitments" in recent OFAC settlements, represent a new effort by OFAC to more clearly and comprehensively communicate its expectations about appropriate sanctions compliance practices. U.S. and non-U.S. companies would be well advised to review the Framework and the compliance commitments carefully.

The Framework is also notable because it explains how OFAC may apply its guidance in evaluating apparent violations and resolving investigations resulting in settlements. Consistent with OFAC's Enforcement Guidelines, the Framework emphasizes that in the event of an OFAC enforcement action, the agency will consider favorably that a company had an effective sanctions compliance program at the time of the apparent violation; it will also consider the Framework in evaluating a company's remedial actions. More notably, the Framework states that "OFAC may, in appropriate cases, consider the existence of an effective [sanctions compliance program] at the time of an apparent violation as a factor in its analysis as to whether

a case is deemed 'egregious.'"[10] While OFAC's Enforcement Guidelines have always made clear that the agency's egregious determination will be based on an analysis of the General Factors, historically, OFAC has focused this determination almost solely on Factors A ("willful or reckless violation of law"), B ("awareness of conduct at issue"), C ("harm to sanctions program objectives"), and D ("individual characteristics"), with, as prescribed by the Guidelines, "particular emphasis on General Factors A and B."[11] The Framework's explicit recognition of compliance as a factor for consideration in OFAC's egregiousness determinations was novel and reflective of OFAC's increased focus on compliance.

Changes in OFAC Sanctions Programs

Iran. Following the U.S. withdrawal from the JCPOA in May 2018 and over the course of 2019, the Trump Administration continued to ratchet up sanctions pressure on Iran. In April 2019, the Trump Administration allowed sanctions waivers to expire that had previously permitted eight countries (including China, India, and Turkey) to purchase Iranian petroleum. This and other actions were a part of the Trump Administration's "maximum pressure" sanctions campaign targeting Iran, which aim to essentially eliminate Iran's ability to export petroleum.[12] Additionally, on May 8, 2019, the President issued E.O. 13871, which authorized blocking sanctions targeting entities in the iron, steel, aluminum, and copper sectors of Iran as well as non-U.S. financial institutions that knowingly conduct or facilitate any "significant financial transaction" related to the iron, steel, aluminum, or copper sectors of Iran.[13] The Trump Administration described these sectors as, collectively, the second largest sector of the Iranian economy. On June 24, 2019, the President issued E.O. 13876, which imposed sanctions targeting the Supreme Leader of Iran as well as other high-ranking Iranian government officials.[14]

On December 11, 2019, the U.S. State Department announced the designation of the Islamic Republic of Iran Shipping Lines and E-Sail Shipping Limited pursuant to E.O. 13382, effective June 8, 2020.[15] While both of these entities had already been designated on the SDN List, their designation pursuant to E.O. 13382, the Weapons of Mass Destruction Proliferators sanctions program, will mean that U.S. persons will be prohibited from engaging in *all* transactions with these entities, including transactions related to agricultural commodities, food, medicine, or medical devices. As such, the designation under this additional authority prevents designated entities from being able to benefit from the humanitarian general licenses in the Iran sanctions program. In addition, non-U.S. persons that knowingly engage in certain transactions with these entities, even for the sale to Iran of agricultural commodities, food, medicine, or medical devices, are subject to secondary sanctions risks.

On January 10, 2020, OFAC announced that it was designating senior Iranian officials pursuant to E.O. 13876, as well as the largest steel, aluminum, copper, and iron manufacturers in Iran pursuant to E.O. 13871. OFAC also designated a network of three China- and Seychelles-based entities, along with a vessel involved in the transfer of Iranian metal products. U.S.-nexus transactions with these entities and individuals are now prohibited. In addition, non-U.S. persons that engage in certain non-U.S.-nexus transactions with these entities and individuals may be exposed to secondary sanctions. Any non-U.S.

financial institutions that facilitate significant transactions for or on behalf of these entities or individuals could be subject to U.S. correspondent or payable-through account sanctions.

Also on January 10, 2020, President Trump issued E.O. 13902, which authorized blocking sanctions on persons operating in "the construction, mining, manufacturing, and textile sectors of the Iranian economy, or any other sector of the Iranian economy as may be determined by the Secretary of the Treasury, in consultation with the Secretary of State." The executive order also provides for secondary sanctions targeting financial institutions that facilitate significant financial transactions in connection with these sectors or on behalf of any person whose property and interest in property are blocked pursuant to the order. The order does not apply to those persons engaged in humanitarian transactions with Iran, in line with existing authorizations in the Iran program. OFAC announced a 90-day wind-down period for transactions with the sanctioned sectors after the issuance of E.O. 13902, which expires on April 9, 2020.

Both E.O. 13871 and E.O. 13902 authorize blocking sanctions on non-U.S. persons who knowingly engage in significant transactions for the sale or supply of goods or services used in connection with one of the specified sectors of the Iranian economy. Similarly, secondary sanctions are also authorized for those who are found to materially assist or provide support for those persons directly targeted by the order as well as for those who are found to provide support for goods and services used in connection of these sectors or entities who are owned or controlled by any person whose property and interests in property are blocked pursuant to either E.O. 13871 or E.O. 13902.

As discussed in our prior year-in-review memorandum, in reaction to the withdrawal of the United States from the JCPOA in 2018, the European Commission implemented countermeasures that year aimed at protecting the interests of EU companies doing business in Iran.[16] The result of the revised EU Blocking Regulation is a 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. EU Member States are responsible for implementing the EU Blocking Regulation at the national level and imposing penalties, and EU Member States have taken a varied approach to the implementation of national legislation. For example, such legislative approaches include an unlimited fine for breaches in the UK, a maximum fine of approximately €60,000 in Spain, and both a maximum fine of €500,000 and a prison sentence of up to three years in the Republic of Ireland. Meanwhile, France has yet to enact national legislation implementing the EU Blocking Regulation.

Enforcement of the EU Blocking Regulation remains limited, with only a handful of recent private litigation cases that have revealed no consensus to date on the application of the regulation across EU Member States.[17] These cases suggest that EU companies currently face the added uncertainty of inconsistent enforcement across EU Member States.

In a further development, on January 14, 2020, France, Germany, and the United Kingdom (known as the "E3") triggered the dispute resolution mechanism under the JCPOA following Iran's announcement that it

would no longer comply with the JCPOA's uranium enrichment limits.[18] While EU and UN sanctions remain lifted during the dispute resolution process, eventually this process could result in the re-imposition of such sanctions under the JCPOA, which could also end the potential conflict of laws resulting from the EU Blocking Regulation.

Venezuela. On January 23, 2019, the United States recognized Maduro opposition leader and Venezuelan National Assembly President Juan Guaidó as the Interim President of Venezuela.[19] Less than a week later, on February 1, 2019, 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.[20] Accordingly, PDVSA was placed on the SDN List. OFAC issued nine general licenses in connection with this action, including certain authorizations for transactions with PDVSA's U.S.-based affiliates, PDV Holding Inc., and Citgo, and for certain maintenance and wind-down activities with PDVSA.[21] 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 . . .[t]he path to sanctions relief for PDVSA is through the expeditious transfer of control to the Interim President or a subsequent, democratically elected government."[22] The same day, President Trump issued a second executive order, E.O. 13857, 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."[23]

On August 5, 2019, the President issued E.O. 13884, which imposed blocking sanctions on the Government of Venezuela, including entities owned by the Government of Venezuela such as PDVSA.[24] These sanctions broadly prohibit any U.S.-nexus financial or commercial dealings, directly or indirectly, with the Government of Venezuela (as defined for purposes of E.O. 13884, which is quite broad) unless authorized by OFAC. The impact of these sanctions are far-reaching given the widespread presence of the Government of Venezuela (which includes any 50 percent or more state-owned entity in Venezuela) in the Venezuelan economy.

Additionally, E.O. 13884 authorizes OFAC to impose sanctions on non-U.S. persons found to have, among other things, materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, the Government of Venezuela and other persons included on the SDN List or that have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to E.O. 13884. OFAC's ability to impose such sanctions (which could be viewed as a form of secondary sanctions) increases the risks for non-U.S. companies involved in any transactions (including those without a U.S. nexus) involving the Government of Venezuela or any person designated on the SDN List pursuant to any executive order relating to Venezuela sanctions.

Cuba. On June 4, 2019, OFAC issued amendments to the Cuban Assets Control Regulations ("CACR") that continued to implement the Trump Administration's policy toward Cuba outlined in the National Security Memorandum titled "Strengthening the Policy of the United States Toward Cuba," which President Trump signed in June 2017.[25] These amendments to the CACR included removal of the authorization for group "people-to-people" educational travel and, along with amendments to the Export Administration Regulations ("EAR") administered by BIS, a removal of authorizations for exports of recreational vessels, passenger vessels, and private aircraft to Cuba.

The CACR had previously authorized U.S. financial institutions to process "U-Turn" funds transfers where a Cuban person had an interest so long as each transfer originated and terminated outside of the United States and so long as neither the originator nor the beneficiary of the transfer was a U.S. person (including citizens, permanent residents, and non-U.S. persons located in the United States). On September 6, 2019, OFAC amended the CACR to remove this authorization and, instead, authorize U.S. financial institutions to reject such transactions, subject to certain conditions.[26]

OFAC also amended CACR authorizations relating to family remittances to persons located in Cuba. The new authorization has a cap of $1,000 per quarter between one remitter and one Cuban national. The new authorization also excludes close relatives of prohibited Cuban government officials and members of the Cuban Communist Party (for each term, as defined by the CACR). The amendments to the CACR also included an authorization for unlimited remittances to any "self-employed individual" in the non-government sector[27] of Cuba.[28] These new authorizations are intended to encourage the development of the private sector in Cuba.

In April 2019, the Trump Administration announced that it will allow for the first time, pursuant to Title III of the Helms-Burton Act, U.S. persons and those subject to the jurisdiction of the United States to bring lawsuits in U.S. federal court against any person that traffics in property which was confiscated by the Cuban government on or after January 1, 1959.[29] Historically, this provision of the Helms-Burton Act was routinely suspended by every U.S. president since the law took effect in 1996. The statute's expansive application allows for lawsuits against foreign companies engaged in business deemed lawful in Cuba, in their home countries, and under international law to be subject to U.S. jurisdiction, and some countries have passed "blocking legislation" prohibiting cooperation with U.S. courts with respect to Title III cases.

Global Magnitsky Sanctions. The Trump Administration remained active in the area of Global Magnitsky sanctions in 2019, designating 87 individuals and entities from over 15 countries, a number of whom were connected to DOJ and SEC Foreign Corrupt Practices Act enforcement actions, and including a number of government officials and wealthy business persons.[30]

Notable Global Magnitsky designations in 2019 included the governor of Nayarit, Mexico for bribery in connection with narcotics trafficking[31] as well as four individuals (two of whom were former government officials) in Iraq who were "implicated in serious human rights abuse or corruption" in regions in Iraq in which persecuted religious communities were struggling to recover from abuse suffered under ISIS

control.[32] In 2019, OFAC also sanctioned the former Inspector General of Police of the Ugandan Police Force for having led a police force that engaged in serious human rights abuses against Ugandan citizens. [33] OFAC also sanctioned three members of the Gupta family and a business associate for involvement in a significant corruption network in South Africa that allegedly leveraged overpayments on government contracts, bribery, and other corrupt acts to fund political contributions and influence government actions.[34] Specifically, OFAC designated Ajay Gupta, Atul Gupta, Rajesh Gupta, and Salim Essa for "[using] their influence with prominent politicians and parties to line their pockets with ill-gotten gains."[35]

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.

Counter-Terrorism Sanctions. On September 10, 2019, President Trump issued Executive Order 13886, expanding global terrorism sanctions to authorize, among other things, the imposition of secondary sanctions—including the prohibition or imposition of strict conditions on the opening or maintaining of a correspondent account or pay through account—against any non-U.S. financial institution that knowingly conducts or facilitates any significant transaction on behalf of any specially designated global terrorist ("SDGT").[36] The accompanying press release noted that the new authority "serves to put all foreign financial institutions on notice that enabling terrorists and their financial backers to rely upon the international financial system to facilitate their malign activities will have consequences." Although the line between primary and secondary sanctions authorities is gray, the counterterrorism sanctions program is now the fifth U.S. secondary sanctions program implemented to date.

The Trump Administration simultaneously designated fifteen individuals and entities affiliated with HAMAS, the Islamic State of Iraq and Syria (ISIS), al-Qa'ida, and the Islamic Revolutionary Guard Corps Qods-Force (IRGC-QF).

Amendment of the Reporting, Procedures, and Penalties Regulations. On June 21, 2019, OFAC published an interim final rule amending the Reporting, Procedures, and Penalties Regulations (the "RPPR").[37] Among other things, the rule revised the RPPR to require all U.S. persons (not just U.S. financial institutions, as had previously been the case) to file rejection reports with OFAC. The rule also amends the RPPR to require rejection reports for all rejected transactions (not just fund transfers, as had previously been the case), including transactions relating to wire transfers, trade finance, securities, checks, foreign exchange, and goods or services. In addition to these new requirements, the interim final rule also expanded the scope of information that OFAC requires to be included on initial and annual reports of blocked property.[38]

OFAC Advisories

Syria Petroleum Shipping Advisory. In March 2019, OFAC issued an updated advisory regarding the U.S. sanctions risks surrounding petroleum shipments (including Iran-origin petroleum) to Syria to include

additional guidance regarding the risks to individuals and entities that facilitate such shipments.[39] The updated advisory stated that those "who in any way" facilitate such shipments (including shipping companies, vessel owners, managers, operators, insurers, and financial institutions) are at risk of being targeted for sanctions under Syria- (or Iran-) related sanctions authorities.[40] OFAC stated it is committed to disrupting financial and other support to the Government of Syria, including the transport of petroleum to it, regardless of the location or nationality of those involved in such shipments. Accordingly, any person providing support to the Government of Syria "will [be] aggressively target[ed] for designation."[41] OFAC particularly flagged the risk of dealings with Russian or Iranian companies that are involved in providing petroleum to Syria.

The advisory discussed several deceptive practices that have been used to obfuscate the Syrian destination of oil shipments in the Mediterranean Sea, including falsified cargo and vessel documents, ship-to-ship transfers, disablement of Automatic Identification System ("AIS") transponders, and vessel name changes. The advisory also identified several measures for reducing sanctions risk, including monitoring for AIS manipulation, reviewing all applicable shipping documents to understand the details of the underlying voyage, conducting know-your-customer diligence (including researching vessels' ISO numbers), and leveraging available resources (including organizations that provide commercial shipping data information). OFAC attached an annex with a non-exhaustive list of vessels that have delivered petroleum to Syria, engaged in ship-to-ship transfers of petroleum destined for Syria, or have exported petroleum to Syria since 2016.

Updated Guidance on North Korea's Illicit Shipping Practices. In March 2019, OFAC (along with the U.S. Coast Guard and U.S. Department of State) issued updated guidance regarding North Korea's deceptive shipping practices.[42] This guidance updated a previous OFAC advisory issued in February 2018 on the same topic. Among other things, OFAC included annexes that included: (i) an updated list of 28 North Korean tankers known to be able to engage in ship-to-ship transfers; (ii) an updated list of 18 third-country (*i.e.*, not U.S. or North Korean) vessels that are believed to have engaged in illicit ship-to-ship transfers of refined petroleum with North Korean tanker vessels, and (iii) an updated list of 49 vessels that are believed to have exported North Korea-origin coal.

Iran Petroleum Shipping Advisory. In September 2019, OFAC issued an advisory alerting the global shipping industry to U.S. secondary sanctions risks for parties involved in shipping petroleum or petroleum products from Iran after the expiration of any applicable "significant reduction exceptions" in May 2019.[43] The advisory stated that any such shipments are subject to significant sanctions risks for shipping companies, vessel owners, managers, operators, insurers, and financial institutions. OFAC explained that, in addition to sanctions enforcement risks, those persons or entities who engage in "significant transactions" for the purchase, acquisition, sale, transport, or marketing of petroleum or petroleum products from Iran (or knowingly provide significant support to an Iranian person on the SDN List) are at "serious risk of being targeted by the United States for sanctions, regardless of the location or nationality of those engaging in such activities."[44] OFAC specifically noted the sanctions-related risk of involvement in procuring petroleum products from Iran for Syria or China. The advisory described deceptive shipping practices and measures for mitigating risk, tracking the discussion in the March 2019 Syria advisory

discussed above. This advisory, however, added the recommendation that entities receiving petroleum or petroleum products shipments should conduct appropriate due diligence to corroborate the origin of such goods where there are suspicious indicia. In this regard, OFAC noted that "[t]esting samples of the cargo's composition can reveal chemical signatures unique to Iranian oil fields."

Iran-Related Civil Aviation Industry Advisory. On July 23, 2019, OFAC issued an advisory regarding deceptive practices by Iran with respect to the civil aviation industry.[45] The advisory described a number of deceptive practices that are used by Iranian airlines to procure U.S.-origin aircraft parts from across the world. These include using front companies and other pass-through entities based in Europe, the Middle East, Africa, and Asia to engage in procurement, as well as misrepresenting to suppliers, dealers, brokers, and other intermediaries that activities are authorized by OFAC by license or no longer subject to sanctions. The advisory noted the potential civil and criminal consequences for both U.S. and non-U.S. persons found to have engaged in unauthorized transfers of U.S.-origin aircraft or related goods, technology, or services to Iran. Additionally, the advisory noted that non-U.S. persons could be added to the SDN List pursuant to secondary sanctions for engaging in unauthorized activities with persons designated in connection with Iran's proliferation of weapons of mass destruction, support for international terrorism, or human rights abuses (which currently include a number of Iranian aviation companies such as Mahan Air, Caspian Air, Meraj Air, Pouya Air, and Dena Airways).

Litigation Matters

Exxon Case. In July 2017, OFAC imposed a $2 million civil penalty on the Exxon Mobil Corporation ("Exxon") for allegedly violating U.S. sanctions targeting Russia. According to OFAC, Exxon had violated U.S. sanctions by entering into a series of contracts with Rosneft OAO that had been signed by Igor Sechin, Rosneft's President, who was included on the SDN List at the time he signed the agreements with Exxon. Exxon challenged the civil penalty in federal court. On December 31, 2019, the U.S. District Court for the Northern District of Texas concluded that the OFAC civil penalty violated the Due Process Clause of the Fifth Amendment, because OFAC had not provided Exxon with sufficient notice that an SDN individual's signing of agreements on behalf of a company that was not listed on the SDN List involved the receipt of a "service" from an SDN, in violation of U.S. sanctions targeting Russia.

Intrater Case. In July 2019, Andrew Intrater, a U.S. citizen, and firms associated with Intrater filed a lawsuit in the U.S. District Court for the Southern District of New York challenging OFAC's blocking of his firms' funds due to OFAC's allegation that the funds at issue (although managed by Intrater and his funds) were ultimately beneficially owned 50 percent or more by Victor Vekselberg.[46] Vekselberg is Intrater's cousin and the founder of Renova Group; both Vekselberg and Renova Group were designated as SDNs in April 2018. Under OFAC's 50 percent rule, property owned 50% or more by one or more SDNs is treated as blocked. Intrater alleged that a significant portion of the funds were owned by Intrater and/or his business partners and, according to the complaint, do not have any relationship to Vekselberg. Intrater further alleged that OFAC's blocking of this portion of the funds (and its refusal to issue a specific license) constitutes an unlawful seizure under the Fourth Amendment, a due process violation under the Fifth

Amendment, and a violation of the Administrative Procedure Act. The case is pending in federal district court.

OFAC Enforcement Actions

OFAC penalties for 2019 exceeded $1.28 billion, the most assessed in any year. OFAC's 26 public enforcement actions highlight the agency's broad jurisdictional reach, the persistence of large-penalty bank enforcement actions, and an increasing focus on non-financial companies. Among other areas, OFAC had several actions emphasizing the importance of adequate due diligence pre- and post-acquisition of a non-U.S. company; OFAC also took its first enforcement action under the Russia/Ukraine-related sectoral sanctions. OFAC also continued to make use of Findings of Violation, public enforcement actions that involve no assessment of a monetary penalty. As discussed above, another major enforcement development in 2019 was OFAC's imposition of compliance commitments in its settlement agreements; these 23 nearly-standard commitments were also accompanied by a five-year certification requirement.

Below, we survey the key OFAC enforcement actions from 2019, grouped by category or theme.

Bank Enforcement Actions

UniCredit Group. As discussed in our prior memorandum,[47] on April 15, 2019, UniCredit Bank AG ("UCB AG"), headquartered in Munich, Germany, UniCredit Bank Austria AG ("Bank Austria"), headquartered in Vienna, Austria, and their corporate parent, UniCredit S.p.A., an Italian global banking and financial services company (collectively the "UniCredit Group"), resolved alleged violations of U.S. economic sanctions with federal and state agencies for a combined $1.3 billion payment and the imposition of a monitor. (The OFAC penalty was $611 million, of which $106 million was paid to OFAC and the remainder deemed satisfied by payments to DOJ and Federal Reserve.) UCB AG also pled guilty to federal and New York criminal charges. In addition to OFAC, DOJ, and the Federal Reserve, the settlement resolved investigations by the New York County District Attorney's Office and the New York State Department of Financial Services.

The UniCredit Group was alleged to have processed thousands of U.S. dollar transactions over a multi-year period (2007–2012) on behalf of countries, entities, or individuals (including certain SDNs) subject to U.S. economic sanctions, largely related to Iran.[48] OFAC found that UniCredit Group had failed to implement and deploy appropriate compliance measures to prevent the processing of sanctioned transactions. According to OFAC, UCB AG had a so-called "OFAC Neutral" internal procedure that instructed bank personnel to confirm that payment instructions were formatted in a manner that ensured that U.S. intermediary banks could not detect the involvement of OFAC-sanctioned parties or countries. Additionally, UCB AG removed certain entities from an internal "customer group" identifying all entities affiliated with the Islamic Republic of Iran Shipping Lines ("IRISL"), and did not have sufficient controls on intrabank transfers between the accounts of IRISL and these other entities. OFAC found that, although these entities were not owned by IRISL, IRISL was involved in opening and maintaining their accounts and therefore had an interest in their transactions, which were therefore considered blocked. With respect to

UniCredit S.p.A. and Bank Austria, OFAC found that they engaged in conduct to remove, omit, or otherwise not reveal the involvement of sanctioned countries or parties in USD transactions. OFAC determined that the vast majority of UniCredit Group's apparent violations constituted an egregious case.

The OFAC settlement was one of the first to include OFAC's 23 compliance commitments, which have now been incorporated regularly since December 2018.[49] The OFAC resolution also highlights the risk of a non-U.S. bank's sanctioned customers making intra-bank transfers to affiliates or third parties, which can then make U.S. dollar payments on the sanctioned customers' behalf.

Standard Chartered Bank. On April 9, 2019, Standard Chartered Bank ("SCB") agreed to pay a $1.1 billion resolution for alleged sanctions violations. This resolution encompassed settlements with OFAC, DOJ, the New York Department of Financial Services, New York County District Attorney's Office, the Federal Reserve, and the UK Financial Conduct Authority. The OFAC penalty of $639,023,750 was assessed for apparent violations of Iranian, Cuban, and Syrian sanctions and (now-repealed) Burmese and Sudanese sanctions, and the penalty was deemed satisfied by payments to other federal agencies.[50]

The enforcement action largely concerned pre-2012 conduct involving U.S. dollar payments processed by SCB's Dubai branches ("SCB Dubai") on behalf of customers that sent payment instructions to SCB Dubai while allegedly located and/or ordinarily resident in Iran. (As noted in a later section, one of the SCB Dubai relationship managers involved pled guilty to DOJ criminal sanctions charges.) OFAC also cited the bank's alleged delays in restricting sanctioned country access to its online banking platform and fax transmissions as a compliance failure that led to apparent sanctions violations.

British Arab Commercial Bank. As discussed in our prior memorandum,[51] on September 17, 2019, OFAC announced a $4 million settlement agreement with British Arab Commercial Bank plc ("BACB"), a commercial bank located in the United Kingdom, for apparent violations of OFAC's Sudanese Sanctions Regulations. OFAC determined that 72 bulk U.S. dollar payments processed by BACB through U.S. financial institutions were apparent violations of OFAC's Sudan regulations because they were used to fund a U.S. dollar account at a non-U.S. financial institution, which was in turn used to process payments for Sudanese parties with accounts at the same bank. As OFAC stated, this enforcement action "highlights the risks surrounding[] the use of complex payment structures, including bulk funding arrangements, to process payments on behalf of, or otherwise involving, U.S. sanctions targets."[52] The settlement agreement is also notable because OFAC determined, in consultation with one of the bank's UK regulators, to suspend all but $4 million of the proposed penalty of $228,840,000 in view of the bank's limited "operating capacity."

M&A Enforcement Actions and/or U.S. Parent Liability for Non-U.S. Subsidiary Business with Iran and Cuba

Multiple 2019 OFAC enforcement actions highlight the importance of performing adequate sanctions due diligence with regard to potential acquisition targets and implementing strong sanctions compliance procedures and ongoing monitoring mechanisms following acquisition. These cases also reflect OFAC's

increased willingness to hold U.S. parent companies liable for the Iranian or Cuban business conducted by their non-U.S. subsidiaries (although, as reflected below, sometimes OFAC will settle with the non-U.S. subsidiary alone or with both the U.S. parent and the non-U.S. subsidiary).

AppliChem GmbH. On February 14, 2019 OFAC assessed a penalty of $5,512,564 against German-based company AppliChem GmbH ("AppliChem") for violations of the Cuban Assets Control Regulations.[53] Under OFAC's Cuba sanctions program, the prohibitions apply to non-U.S. companies that are owned or controlled by U.S. companies. AppliChem was acquired by U.S.-based company Illinois Tool Works, Inc. (ITW) on January 1, 2012. Following the acquisition, between May 2012 and February 2016, AppliChem sold chemical reagents to Cuba on 304 occasions. ITW had sent AppliChem's former owners, who remained manager-employees, their guidelines for complying with U.S. sanctions. Nevertheless, AppliChem continued to complete and collect on existing orders with Cuban nationals under pre-acquisition contracts.[54] In April 2012, ITW's legal department submitted a third warning to AppliChem's manager-employees to cease all sales to Cuba and subsequently submitted a voluntary self-disclosure to OFAC in January 2013. In 2016, following an anonymous report made through ITW's ethics helpline, an investigation found that AppliChem manager-employees had continued business with Cuba by concealing the transactions from ITW through use of an intermediate entity in Germany. It was also discovered that AppliChem employees had reported to an ITW manager that there were indications of continued sales to Cuba and, although this manager reminded AppliChem of ITW's sanctions compliance policy, a fuller internal investigation was not initiated at that time.[55] OFAC determined that the apparent violations constituted an egregious case. OFAC noted that this case demonstrates the importance of compliance oversight over subsidiaries and performing follow-up due diligence after acquisitions of non-U.S. companies known to have engaged in historical transactions with sanctioned jurisdictions.

Kollmorgen Corporation. As discussed in our prior memorandum,[56] on February 7, 2019, OFAC announced a $13,381 settlement agreement with U.S.-based Kollmorgen Corporation ("Kollmorgen"), a technology and manufacturing company, regarding six apparent violations of OFAC's Iran sanctions regulations.[57] OFAC determined that Kollmorgen's Turkish subsidiary, Elsim Elektroteknik ("Elsim"), which it acquired in early 2013, serviced machines located in Iran and knowingly provided products, parts, or services to Iranian end-users. Under U.S. law, non-U.S. companies owned or controlled by U.S. companies are required to adhere to the embargo on Iran as if they were U.S. persons. Simultaneous with this settlement, OFAC designated Evren Kayakiran, the former Elsim managing director whom OFAC determined to be primarily responsible for directing the apparent violations and seeking to conceal them, as a foreign sanctions evader and added his name to the Foreign Sanctions Evaders List, thereby broadly cutting off his access to the U.S. economy. This marked the first time that OFAC has concurrently designated a foreign sanctions evader and announced a related settlement with a U.S. company. OFAC determined that Kollmorgen voluntarily self-disclosed the apparent violations, which constituted a non-egregious case. The Kollmorgen settlement makes clear that OFAC expects the immediate adoption and implementation of appropriate controls when U.S. companies acquire non-U.S. companies with preexisting relationships with sanctioned persons or jurisdictions. The concurrent sanctioning of Elsim's former managing director highlights increased personal risk for non-U.S. personnel that violate U.S. sanctions.

Stanley Black & Decker, Inc. As discussed in our prior memorandum,[58] on March 27, 2019, U.S.-based Stanley Black & Decker, Inc. ("Stanley Black & Decker") and its Chinese subsidiary, Jiangsu Guoqiang Tools Co., Ltd. ("GQ"), agreed to pay OFAC $1,869,144 to settle 23 apparent violations of OFAC's Iran sanctions regulations.[59] According to OFAC, between June 2013 and December 2014, GQ knowingly exported or attempted to export 23 shipments of power tools and spare parts to Iranian end-users. GQ utilized third-party intermediaries located in United Emirates and China to facilitate the shipments. Stanley Black & Decker conducted sanctions due diligence and required GQ to cease transactions with Iran during acquisition negotiations with GQ, and engaged in sanctions and compliance training and review after the acquisition completed. However, OFAC noted that "Stanley Black & Decker did not implement procedures to monitor or audit GQ's operations to ensure that its Iran-related sales did not recur post-acquisition." Unlike the *Kollmorgen* settlement, in which OFAC cited Kollmorgen's "extensive preventative and remedial conduct" as a mitigating factor, OFAC did not explicitly include any of Stanley Black & Decker's pre-acquisition sanctions due diligence or post-acquisition sanctions compliance integration activities in its list of mitigating factors and found the apparent violations to constitute an egregious case. Based upon OFAC's descriptions, the diligence conducted by Kollmorgen, both before and after acquisition, was far more extensive than the diligence conducted by Stanley Black & Decker. Kollmorgen's diligence efforts appear to have been a key factor in OFAC's determination that the conduct in that case was non-egregious.

PACCAR Inc. On August 6, 2019, OFAC announced a $1,709,325 settlement with U.S.-based PACCAR Inc. ("PACCAR"), relating to 63 apparent violations of Iran sanctions.[60] According to OFAC, between October 2013 and February 2015, a wholly owned subsidiary of PACCAR headquartered in Eindhoven, the Netherlands (DAF Trucks N.V. ("DAF")), sold or supplied 63 trucks to customers in Europe that it knew or had reason to know were ultimately intended for buyers in Iran. For example, a DAF dealer located in Germany placed an order with DAF's German subsidiary for 51 trucks with specifications for a customer located in Iran. After being informed that DAF Germany could not sell trucks destined for Iran, the German DAF dealer placed a virtually identical order (*e.g.*, same types of trucks, same specifications, same delivery point) on the same day, but stated that the trucks were for an unnamed Russian customer. DAF Germany, however, "failed to conduct an adequate inquiry and processed the order." The trucks were in fact re-sold by the dealer to a buyer in Iran. OFAC determined that PACCAR voluntarily disclosed the apparent violations, and that the apparent violations constitute a non-egregious case. Although OFAC noted that DAF personnel "ignored warning signs regarding potential sales involving OFAC-sanctioned countries," it considered as mitigating factors, among others, that DAF included contractual prohibitions on dealers and services partners regarding re-sale of DAF products in violation of U.S. sanctions; took remedial action by conducting an internal investigation regarding the apparent violations, and implemented enhanced trade compliance controls and training. OFAR noted that this enforcement action "highlights the benefits U.S. companies can realize in conducting sanctions-related training and in taking appropriate steps to audit and monitor foreign subsidiaries for OFAC compliance."

Acteon Group. On April 11, 2019, a UK-based subsea service provider in the oil and gas industry, Acteon Group Ltd. ("Acteon"), and Acteon's UK subsidiary 2H Offshore Engineering Ltd. ("2H Offshore") that has two Malaysian affiliates (2H Offshore Engineering Sdn Bhd and 2H Offshore Engineering (Asia Pacific) Sdn Bhd (collectively, "2H KL")) agreed to pay OFAC $227,500 to settle apparent violations of Cuba sanctions.[61]

OFAC noted that at all times during the period in which the apparent violations occurred, Acteon was subject to the jurisdiction of the United States as defined by the CACR, because it was previously owned (at the time of the apparent violations) by funds associated with a U.S. investment firm. According to OFAC, between May 2011 and October 2012, 2H KL performed engineering design analyses for oil exploration projects in Cuban territorial waters, and sent its engineers to Cuba to present these analyses. OFAC found that directors at 2H Offshore and 2H KL committed this conduct knowing that it was illegal, and deliberately concealed their dealings with Cuba in external and internal documents on multiple occasions (*e.g.*, by replacing "Cuba" with "Central America" in a post-trip expense report). OFAC determined that Acteon and 2H Offshore voluntarily self-disclosed the apparent violations, and that these apparent violations constitute an egregious case.

Separately, on the same day, Acteon agreed to pay $213,866 to resolve potential OFAC liability for itself and for KKR & Co., Inc.[62] (whose affiliated investment funds acquired a majority stake in Acteon as well as its subsidiaries Seatronics Ltd. and Seatronics Ptd. Ltd. (together, "Seatronics") in November 2012).[63] According to OFAC, between August 2010 and March 2012, Seatronics rented or sold equipment for oil exploration projects in Cuban territorial waters, and sent company engineers to service equipment on vessels operating in the same. In addition, between September 2014 and November 2014, Seatronics Ltd.'s Abu Dhabi, United Arab Emirates branch appears to have violated Iran sanctions when it rented or sold equipment to customers who appear to have embarked the equipment on vessels that operated in Iranian territorial waters. KKR-affiliated investment funds acquired a majority stake in Acteon in November 2012; OFAC determined that Acteon voluntarily self-disclosed the apparent violations, and that these apparent violations constitute a non-egregious case.

Cuba Travel Cases

Hotelbeds USA, Inc. On June 13, 2019, U.S.-based Hotelbeds USA, Inc. ("Hotelbeds USA"), the U.S. subsidiary of the Spain-based Hotelbeds Group, agreed to pay OFAC $222,705 to settle apparent violations of Cuba sanctions.[64] According to OFAC, between December 2011 to June 2014, Hotelbeds USA knowingly provided unauthorized Cuba-related travel services to 703 non-U.S. persons. Hotelbeds USA personnel believed that they could legally provide Cuba-related travel services if the clients and the bank accounts to which payments were made were both non-U.S. Partly due to this misunderstanding, Hotelbeds USA sold hotel accommodations to its clients and directed them to pay to an account in Spain, from which Hotelbeds USA was later reimbursed. During this period of time, Hotelbeds USA sought to unblock a payment related to a Cuba-travel transaction, but OFAC denied its application for the license and provided in its denial the relevant CACR prohibitions that required the payment to remain blocked. OFAC noted that this specific license denial put Hotelbeds USA on notice that its conduct violated sanctions.

Cubasphere Inc. Also on June 13, 2019, U.S.-based Cubasphere Inc. ("Cubasphere") and a U.S. person (the "Individual") who had acted on behalf of Cubasphere agreed to pay OFAC $40,320 to settle apparent violations of Cuba sanctions.[65] According to OFAC, between around December 30, 2013 and February 22, 2014, the Individual and Cubasphere provided unauthorized travel services to 104 persons on four trips to Cuba. Besides making travel arrangements for their clients in Cuba, the Individual and Cubasphere helped

them obtain visas and cover letters from U.S. religious organizations that cited Cuba-related general licenses, even though the actual travel itineraries focused on sightseeing and tourism instead of humanitarian or religious activities. Cubasphere and the Individual knew their conduct violated Cuba sanctions for more than a year, and they urged their clients to conceal those trips by avoiding interactions with U.S. government officials, getting rid of receipts and schedules from the trips, and lying about their activities in Cuba. OFAC's targeting of an individual in an enforcement action (outside of the situation of a U.S. person who travels to Cuba) is rare and appears to be the result of the individual's multiple attempts to conceal the apparent violations from OFAC.

Insurance Cases

ACE Limited. On December 9, 2019, Chubb Limited, the post-merger successor of ACE Limited ("ACE"), agreed to pay OFAC $66,212 to settle apparent violations of Cuba sanctions by ACE before the merger.[66] ACE was a Swiss insurance and reinsurance company, which had a U.S. subsidiary, ACE Group Holdings, Inc., which in turn had a European subsidiary, ACE Europe.[67] According to OFAC, between January 1, 2010 and December 31, 2014, ACE Europe processed a number of transactions, including premium payments and claims payouts for Cuba-related travel insurance. Most of these transactions involved global coverage policies issued to a European travel agency and its subsidiaries, which then issued the policies to insureds. OFAC considered as mitigating factors that ACE submitted a voluntary self-disclosure to OFAC, cooperated with the OFAC investigation, implemented remedial measures, and that many of the transactions would have been authorized by a general license had they occurred on or after January 16, 2015. OFAC determined that these apparent violations constituted non-egregious cases.

Allianz Global Risks US Insurance Company. Also on December 9, 2019, Allianz Global Risks US Insurance Company ("AGR US"), a U.S.-based property casualty insurer and the subsidiary of German-based Allianz SE ("Allianz"), agreed to pay OFAC $170,535 to settle apparent violations of Cuba sanctions.[68] According to OFAC, between August 20, 2010 and January 15, 2015, AGR Canada, AGR US's Canadian branch, provided travel insurance policies that resulted in the reimbursement of approximately $518,092 for 864 Cuba-related claims and the collection of approximately $23,289 in premiums.[69] Although OFAC acknowledged AGR US's voluntary self-disclosure and viewed these violations as non-egregious,[70] it found that AGR US and AGR Canada failed to address the compliance deficiency for several years after receiving notice in 2010 that AGR Canada had provided prohibited Cuba-related insurance coverage.[71] This corporate inaction constituted an aggravating factor.[72]

Sanctions Screening Issues

State Street Bank and Trust Co. On May 28, 2019, OFAC issued a Finding of Violation, with no monetary penalty, to State Street Bank and Trust Co. ("SSBT") for violations of the Iranian Transactions and Sanctions Regulations.[73] Between 2012 and 2015, SSBT acted as a trustee for a customer's employee retirement plan. One of the employees who received payments from the customer's benefit plan was a U.S. citizen but a resident of Iran. OFAC concluded that SSBT should have known it was sending payments for the benefit of a person in Iran because its internal system indicated the beneficiary's address was located in

Iran and the bank's screening software produced an alert on each of the 45 pension payments made. In 2015, after learning of and reporting to OFAC a deficiency in its compliance program, SSBT modified its program to ensure payments were screened by its personnel in its central screening program. Previously, alerts were reviewed by initial sanctions review teams within business units, and these teams had generally consisted of personnel who were not sanctions specialists. In issuing a finding of violation instead of a civil monetary penalty, OFAC considered several factors, including that no SSBT managers appeared to have been aware of the conduct leading to the violations, and that SSBT took remedial actions in response to the violations and enhanced its escalation procedures for sanction-related alerts.

Apple, Inc. On November 25, 2019, Apple, Inc. ("Apple") agreed to pay OFAC $466,912 to settle apparent violations of the Foreign Narcotics Kingpin Sanctions Regulations ("FNKSR").[74] According to OFAC, Apple dealt in the property interests of SIS, d.o.o. ("SIS"), a Slovenian software company designated by OFAC as a significant foreign narcotics trafficker. Specifically, OFAC found that from approximately February 2015 to May 2017, Apple appears to have violated the FNKSR when it "hosted, sold, and facilitated the transfer" of SIS's software application and associated content. Apple initially entered into an app development agreement with SIS in 2008. When OFAC added SIS and its director and majority owner, Savo Stjepanovic, to the SDN list on February 24, 2015, Apple failed to identify SIS as an SDN, because its sanctions screening tool failed to match the upper case name "SIS DOO" in Apple's system with the lower case name "SIS d.o.o." as it appears on the SDN List, even though the address for SIS in Apple's records matched the SIS address reflected on the SDN List. Further, Apple only screened individuals listed as "developers" in its system, and therefore missed Stjepanovic, who was listed as an "account administrator" in SIS's App Store developer account. On or about April 17, 2017—approximately two months after the designations—Apple facilitated the transfer of a portion of SIS's apps to a second software company, which had been incorporated several days after the designations. And in September 2015, SIS entered into an agreement with a third software company, which obtained SIS's remained apps and took over SIS's App Store account and replaced SIS's banking information with its own. OFAC noted that "these actions were all conducted without personnel oversight or additional screening by Apple."

After enhancing its sanctions screening tool and related processes, Apple identified SIS as a potential SDN in February 2017 and, while Apple immediately suspended further payments associated with the SIS account (administered by the third company), Apple continued to make payments to the second software company that had acquired a portion of SIS's apps, which remained blocked. OFAC noted that Apple made 47 payments associated with the blocked apps and that, over 54 months, Apple collected $1,152,868 from customers who downloaded SIS apps. OFAC determined that the statutory maximum penalty was $74,331,860, but found that Apple voluntarily disclosed the apparent violations and that the apparent violations constituted a non-egregious case. OFAC noted that this enforcement action highlights the benefit of "comprehensive SDN List screening that utilizes all of the information on the SDN List," and stated that companies should consider OFAC screening that makes uses of "names, addresses, and other identifying information on the SDN List." OFAC also noted that companies should consider preventive measures to alert themselves and react to "sanctions evasion warning signs," an apparent reference to SIS's transfer of its apps and administration of its accounts to other companies.

Other Sanctions Diligence Issues

e.l.f. Cosmetics, Inc. As discussed in our prior memorandum,[75] on January 31, 2019, U.S.-based e.l.f. Cosmetics, Inc. ("ELF") agreed to pay OFAC $996,080 to settle apparent violations of North Korea sanctions.[76] 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. 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 a prior advisory regarding risks associated with North Korea supply chain links, 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."

Apollo Aviation Group, LLC. As discussed in our prior memorandum,[77] on November 7, 2019, U.S.-based Apollo Aviation Group, LLC ("Apollo Aviation") agreed to pay OFAC $210,600 to settle apparent violations of the Sudan Sanctions Regulations ("SSR").[78] According to OFAC, Apollo Aviation leased three aircraft engines to a UAE company that subleased the engines to an airline in Ukraine that, in turn, installed the engines on an aircraft that was wet leased to an SDN, Sudan Airways. Under U.S. law, U.S. companies can be held liable for the subleasing or other temporary transfers of items they own to sanctioned countries or persons. Although Apollo Aviation's lease agreements with the UAE company included U.S. sanctions commitments, OFAC faulted Apollo Aviation for failing to take steps during the terms of the leases to monitor whether the aircraft engines were being used in a sanctions-compliant manner. OFAC pointed to its July 2019 advisory to the civil aviation industry regarding Iran's deceptive practices with respect to aviation products and services, and noted that "participants in the civil aviation industry should be aware that other jurisdictions subject to OFAC sanctions may engage in similar deceptive practices." OFAC stated that the action highlights, among other things, "the importance of companies operating internationally to implement Know Your Customer screening procedures and implement compliance measures that extend beyond the point-of-sale and function throughout the entire business or lease period."[79] OFAC's action is a reminder that sanctions contractual provisions will not, by themselves, shield a company from liability, and that OFAC will expect companies to take additional measures to monitor and minimize sanctions risk.

Sectoral Sanctions

Haverly Systems, Inc. On April 25, 2019, Haverly Systems, Inc. ("Haverly"), a U.S.-based software company, agreed to pay $75,375 to settle apparent Russia/Ukraine sectoral sanctions violations.[80] According to OFAC, Haverly transacted with JSC Rosneft ("Rosneft"), an entity listed by OFAC on the Sectoral Sanctions Identification List (the "SSI List"). Under Directive 2, Haverly was not permitted to provide new debt greater than 90 days maturity to Rosneft, and OFAC defines "debt" broadly to include delayed payment terms. Here, Haverly issued two separate invoices to Rosneft with payment due dates of 30 and 70 days from the date of issuance. Rosneft, however, did not pay the first invoice until May 2016,

approximately nine months after issuance. Following that payment and until approximately October 27, 2016, Rosneft made four attempts to pay the second invoice, but each was rejected by financial institutions after determining the transactions would violate OFAC's sectoral sanctions Directive 2. According to OFAC, at the suggestion of Rosneft, Haverly re-issued and re-dated the second invoice, and Haverly received payment on the second invoice on January 11, 2017. OFAC determined that Haverly did not voluntarily self-disclose the apparent violations to OFAC, and that the apparent violations constitute a non-egregious case. As a mitigating factor, OFAC noted that it would "have likely authorized the transactions had Haverly requested a license to receive the payments." This is OFAC's first enforcement action under Russia/Ukraine sectoral sanctions. It is also notable that this first sectoral sanctions enforcement action involves delayed payment, which OFAC views as constituting debt that can violate the sectoral sanctions directives' applicable thresholds—a continuing pain point for U.S. companies that do business with SSI entities. In connection with this action, OFAC encouraged companies to "exercise enhanced due diligence" in business relationships with SSI entities and to "avoid the use of unorthodox business practices—such as the amendment or alteration of trade documents, or resubmission of payment information without a sanctions-related term, phrase, or location."

Inadequate Response to OFAC Subpoena

Southern Cross Aviation, LLC. On August 8, 2019, OFAC issued a Finding of Violation to U.S.-based Southern Cross Aviation, LLC ("Southern Cross") for violations of § 501.602 of the OFAC's RPPR.[81] According to OFAC, Southern Cross failed to provide complete information in response to OFAC's June 27, 2016 Administrative Subpoena. That subpoena and an accompanying letter stated OFAC had reason to believe that Southern Cross was recently involved in the potential sale of several helicopters destined for Iran via an Iranian businessman based in Ecuador (the "Iranian Businessman"). After Southern Cross responded without providing documentation for a potential sale of helicopters to an Iranian group for operation in Ecuador, OFAC issued a second subpoena on October 6, 2016 that repeated similar information and document requests from the initial subpoena and specifically requested documentation related to the potential sale. When Southern Cross again failed to provide the requested information, OFAC issued a Finding of Violation. OFAC specifically noted that "This enforcement action highlights the compliance obligation of persons subject to the RPPR, and the importance for all subject persons to cooperate with OFAC investigations." While Southern Cross avoided monetary penalties, likely due to OFAC's determination that the "potential sale in question does not appear to have occurred," this Finding of Violation makes it more likely that OFAC will penalize Southern Cross more severely in the event of another violation by the Company in the next five years.

Additional Enforcement Actions

Zag IP. On February 21, 2019, a ZAG IP, LLC ("ZAG") a U.S.-based cement producer agreed to pay $506,250 to settle potential civil liability for violations of Iranian sanctions.[82] OFAC reported that between July 2014 and January 2015, ZAG purchased over 200,000 tons of Iranian-origin cement clinker, valued at $14,495,961 from a company located in the United Arab Emirates, with knowledge that the cement clinker was sourced from Iran, and then resold and transported to a company in Tanzania. [83] According to OFAC,

ZAG relied on the supplier's misrepresentation that the clinker was not subject to U.S. economic sanctions on Iran. OFAC pointed to several aggravating factors including that ZAG is a "commercially sophisticated company operating globally with experience and expertise in international transactions" and that ZAG did not have an effective OFAC compliance program in place at the time of the transactions. OFAC concluded that the apparent violations constituted a non-egregious case. OFAC explained that this case demonstrates the importance for companies that operate in high-risk industries such as international trading to implement risk-based compliance measures, particularly when engaging in transactions involving exposure to jurisdictions or persons subject to U.S. sanctions and evaluating relevant commercial documents for potential transshipment or other sanctions-related risks.

MID-SHIP Group LLC. On May 2, 2019, MID-SHIP Group LLC ("MID-SHIP"), a U.S.-based shipbroker, agreed to pay $871,837 to settle five apparent violations of the Weapons of Mass Destruction sanctions.[84] According to OFAC, between February 2011 and November 2011, MID-SHIP processed five electronic funds transfers that pertained to payments associated with blocked vessels identified on OFAC's SDN List. OFAC determined that MID-SHIP did not voluntarily self-disclose the apparent violations to OFAC, and that the apparent violations constitute an egregious case. OFAC found that the company's "culture of compliance appears to have been deficient," noting senior management's awareness of financial institutions holding or rejecting payments for compliance reasons. OFAC stated the company operates in a high-risk industry ("international shipping and logistics") and observed that the case illustrates the benefits of "maintaining a culture of compliance where senior" management sets a positive example of compliance and encouraging staff to comply with the law," as well as the benefits of responding accordingly to "sanctions-related warning signs," such as payments that are blocked or rejected by financial institutions for compliance or sanctions reasons.[85]

Treasury's Financial Crimes Enforcement Network

Last year, FinCEN announced the launch of a new Global Investigations Division, responsible for targeted investigations to combat illicit finance threats and related crimes. It also continued to focus on AML risk related to virtual currency businesses and transactions, issuing further guidance and advisories. On the enforcement front, following three enforcement actions in late 2018, FinCEN enforcement was relatively quiet in 2019, with only one enforcement action against an individual.

FinCEN Organizational Developments

New Global Investigations Division. On August 28, 2019, FinCEN announced the launch of a new Global Investigations Division ("GID"), responsible for implementing "targeted investigation strategies" to combat illicit finance threats and related crimes, both domestically and internationally.[86] Matthew Stiglitz, a former Principal Deputy Chief in the Department of Justice's Criminal Division, was appointed to lead the GID. The division expects to make particular use of two authorities: Section 311 of the USA PATRIOT Act and Geographic Targeting Orders ("GTOs").[87] Under Section 311, if FinCEN finds that a foreign jurisdiction, financial institution, or class of transactions qualifies as a "primary money laundering concern," it may initiate rulemaking that would impose one or more of five different "special

measures." FinCEN has used this authority to designate non-U.S. banks that are found to have deficient AML controls and to prohibit those banks from opening or maintaining U.S. correspondent bank accounts used for clearing U.S. dollar payments. This broad prohibition would constitute a significant impediment to conducting business for any financial institution. FinCEN also has the authority to issue GTOs that require all identified businesses within a geographic area to report on specified transactions. There are civil and criminal penalties for failing to comply with a GTO's requirements. In recent years, specific money laundering concerns have motivated FinCEN to issue GTOs in several areas.

FinCEN Guidance

Guidance on Applicability of FinCEN Regulations to Certain Business Models Involving Convertible Virtual Currencies. On May 9, 2019, FinCEN issued interpretive guidance stating that preexisting BSA regulations applied to several common business models involving Convertible Virtual Currencies ("CVCs").[88] Covered business models include:

- *Peer-to-Peer Exchangers*: Natural persons who engage in transfers between different types of CVCs, as well as exchanges of CVC for other types of value;
- *CVC Wallets and Kiosks*: Interfaces for storing and transferring CVCs that vary based on the technology used, where and how the value is stored, and who controls access to the value;
- *Decentralized (distributed) Applications ("DApps")*: Software programs that operate a blockchain platform, and provide a wide range of functions, with fees charged in CVC to users in order to run the software;
- *Anonymity-Enhanced CVC Transactions*: Transactions structured to conceal information otherwise generally available through the distributed public ledger;
- *Payment Processing Services*: Intermediaries that enable traditional merchants to accept CVC from customers; and
- *Internet Casinos*: Virtual platforms creating for betting which include predictive, information, and decision markets, as well as idea futures and event derivatives.[89]

Guidance on Red Flags and Typologies for Suspicious Convertible Virtual Currencies Activity. Also on May 9, 2019, FinCEN issued an advisory regarding the use of virtual currency to support illegal activity, money laundering, and other behavior endangering U.S. national security.[90] The advisory highlights the capability of virtual currency to be used as an alternative to traditional payment transmission systems, and tracks the rising exploitation of virtual currency in criminal enterprises. The advisory describes multiple virtual currency abuse typologies, including those involving darknet marketplaces, unregistered peer-to-peer exchangers, unregistered foreign-located MSBs, and CVC kiosks, and provides

case studies of each. In addition, the advisory discusses several red flags to assist financial institutions in identifying unregistered MSB activity and suspicious virtual currency purchases, transfers, and transactions. The red flags include any connections between a customer's CVC addresses or IP addresses to darknet or Tor activity; receipt of multiple cash deposits or wires prior to purchasing virtual currency; transmission or receipt of funds or CVCs to or from foreign exchanges or jurisdictions with reputations for being tax havens; operation of CVC kiosks in locations with high incidences of criminal activity; and structuring of transactions just below reporting thresholds or CVC kiosk daily limit to the same wallet address.[91]

Updated Advisory on Widespread Public Corruption in Venezuela. On May 3, 2019, FinCEN issued an updated advisory to alert financial institutions of widespread corruption in Venezuela.[92] The advisory reports FinCEN's assessment that there is a "high risk of corruption involving senior political figures of the illegitimate Maduro regime and employees at all levels, including those managing or working at Venezuelan [state-owned enterprises]."[93] Among other things, the advisory alleges that the Maduro regime is using Venezuela's government-sponsored food distribution program as a "political weapon" to subsidize food for supporters, deny food from other Venezuelan citizens, and enrich insiders through "embezzlement, price manipulation, and trade-based money laundering schemes using front and shell companies."[94] The advisory also noted that the regime has experimented with the use of digital currency to circumvent sanctions and generate revenue, by developing a digital currency called "petro."[95] FinCEN stated that financial institutions should take risk-based steps to identify and limit exposure to funds and assets associated with the Maduro regime's corruption, while also noting that transactions with "normal" businesses or with Venezuelan nationals "do not necessarily represent the same high risk."[96]

FinCEN Enforcement Actions

Eric Powers (MSB). On April 18, 2019, FinCEN announced the imposition (upon consent) of a civil monetary penalty of $35,350 against an individual, Eric Powers.[97] Mr. Powers also consented to an industry bar against provision of money transmission services. From December 6 through September 24, 2014, Mr. Powers acted as a "peer-to-peer exchanger" of the virtual currency bitcoin by purchasing and selling bitcoin on behalf of others, and advertising his services on multiple internet message boards. FinCEN determined that, in doing so, Mr. Powers willfully violated the BSA's registration, program, and reporting requirements by failing to (1) register as a MSB with FinCEN, (2) establish and implement an effective written AML program, (3) detect and adequately report numerous suspicious transactions (such as transactions related to the illicit darknet marketplace "Silk Road"), and (4) file Currency Transaction Reports (CTRs), despite conducting numerous in-person transactions involving more than $10,000 in currency.[98] FinCEN noted that this was its first enforcement action against a peer-to-peer virtual currency exchanger, as well as the first instance in which it had penalized an exchanger for failure to file CTRs.

Department of Justice

Last year, DOJ announced two large-bank criminal sanctions resolutions (UniCredit and Standard Chartered), initiated a major sanctions criminal prosecution against another non-U.S. bank (Halkbank), and continued its prosecution of Huawei. DOJ also announced a revised corporate criminal enforcement policy for export control and sanctions violations, as well as other criminal enforcement guidance that could impact sanctions/AML prosecutions. Unlike in 2018, which saw significant resolutions against Rabobank and U.S. Bancorp, in 2019 DOJ had no major AML-related resolutions.

DOJ Criminal Enforcement Policies

Revised DOJ Export Control and Sanctions Enforcement Policy. As discussed in our prior memorandum,[99] on December 13, 2019, DOJ's National Security Division ("NSD") announced a revised export control and sanctions enforcement policy designed to encourage companies to make voluntary self-disclosures to DOJ in connection with potentially willful export control and sanctions violations. The policy revises a 2016 DOJ policy on the same topic. As the revised policy notes, in the export control and sanctions context, criminal violations require proof of "willfulness," defined as knowledge that the conduct violated the law.

Under the revised policy, when a company (1) voluntarily self-discloses export control or sanctions violations to DOJ's NSD's Counterintelligence and Export Control Section, (2) fully cooperates, and (3) timely and appropriately remediates, there is a presumption that the company will receive a non-prosecution agreement and will not pay a fine, absent "aggravating factors." The policy goes on to define what counts as voluntary self-disclosure, full cooperation, and timely and appropriate remediation. Aggravating factors include, but are not limited to, knowing involvement by upper management in the potentially unlawful conduct, repeated violations, and export of military items to a hostile power. Notably, even if aggravating factors are present and the resolution is a deferred prosecution agreement or a guilty plea, the policy provides benefits in the form of a reduced recommended fine and the avoidance of a corporate monitor if the elements of the policy have been satisfied. The policy applies to financial institutions that had been excluded from the 2016 version of the policy.

Other DOJ Enforcement Guidance. Although not specific to the sanctions/AML areas, DOJ issued additional, broadly applicable guidance in 2019 relating to its evaluation of corporate compliance programs, as well as its evaluation of "inability-to-pay" claims.

On April 30, 2019, DOJ's Criminal Division released updated guidance on how prosecutors should evaluate the effectiveness of corporate compliance programs; the guidance expanded upon guidance issued in 2017. As discussed in our prior memorandum,[100] the updated guidance contains 12 topics and nearly 150 sample questions that are structured around three "fundamental questions" concerning a compliance program's design, implementation, and function: (1) Is the corporation's compliance program well designed? (2) Is

the program being applied earnestly and in good faith? (In other words, is the program being implemented effectively?) and (3) Does the corporation's compliance program work in practice? These three fundamental questions provide a useful framework for companies to design, implement, and test their corporate compliance programs (in addition to other applicable guidance, such as by OFAC or FinCEN).

Additionally, as discussed in our prior memorandum,[101] on October 8, 2019, DOJ's Criminal Division released guidance on how federal prosecutors should evaluate "inability-to-pay" claims (*i.e.*, claims that companies are unable to pay a proposed fine or monetary penalty). The guidance sets forth a detailed framework for prosecutors to assess a company's "inability-to-pay" and requires a company making such a claim to submit to DOJ a completed questionnaire regarding the company's financial condition, projections, and other financial materials. Due to this guidance, companies now have additional insight into how DOJ assesses corporate fine or penalty reductions based on an inability to pay.

DOJ Enforcement Actions

UniCredit Group. As described in more detail above, on April 15, 2019, UniCredit Bank AG, headquartered in Munich, Germany, UniCredit Bank Austria AG, headquartered in Vienna, Austria, and their corporate parent, UniCredit S.p.A., an Italian global banking and financial services company (collectively the "UniCredit Group"), resolved alleged sanctions violations with federal and state agencies for a combined $1.3 billion payment and the imposition of a monitor.[102] As part of the resolution, UCB AG pled guilty to federal criminal sanctions charges, with the DOJ plea agreement requiring a forfeiture of $316.5 million and a fine of approximately $464.4 million. Bank Austria entered into a non-prosecution agreement with DOJ, which required a forfeiture of $20 million. Unicredit S.p.A. separately agreed to ensure that UCB AG and Bank Austria's obligations to DOJ are fulfilled.

Standard Chartered Bank. As described in more detail above, on April 9, 2019, SCB entered into a $1.1 billion resolution with federal and state agencies (and the UK Financial Conduct Authority) to resolve alleged sanctions violations. As part of the resolution, DOJ extended its deferred prosecution agreement with SCB by two years, required a $240 million forfeiture, and a fine of $480 million (which, after crediting other payments, was reduced to approximately $52 million). In connection with this matter, a former employee of SCB's Dubai branch pled guilty in the District Court for the District of Columbia to conspiring to defraud the United States and sanctions violations.[103] Also, a criminal indictment was unsealed against a customer of the SCB Dubai branch (an Iranian national) alleged to have participated in the conspiracy.[104]

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").[105] 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. 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. 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. 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."[106] 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. In addition, Huawei allegedly obstructed the grand jury investigation by moving witnesses with knowledge of Huawei's Iran-related business to China and by allegedly destroying and concealing evidence relating to that business. The case is pending in the U.S. District Court for the Eastern District of New York. On December 3, 2019, the court accepted federal prosecutors' motion to disqualify James Cole as one of Huawei's defense attorneys given his prior role as Deputy Attorney General. Meanwhile, efforts to challenge Meng's extradition from Canada to the United States are ongoing.

Halkbank. On October 15, 2019, DOJ announced a six count indictment against Türkiye Halk Bankasi, A.S. ("Halkbank"), a major Turkish bank that is partially owned by the Turkish government.[107] The indictment alleges that Halkbank violated U.S. sanctions targeting Iran and committed bank fraud when it facilitated the use of money services businesses and front companies in Iran, Turkey, and the United Arab Emirates to allow sanctioned entities in Iran to gain access to billions of dollars' worth of funds denominated in U.S. dollars. According to the indictment, proceeds of Iran's oil sales were deposited in accounts at Halkbank in the names of the Central Bank of Iran and the National Iranian Oil Company (both of which are SDNs), and Halkbank allegedly then allowed these Iranian entities to buy gold for the benefit of the Government of Iran (which is also the target of U.S. sanctions). The indictment also alleges that Halkbank also allowed these entities to transfer funds to other accounts at Halkbank in the name of front companies and other entities in order to conceal the relationship of the funds to Iran and sanctioned Iranian entities. According to the indictment, Halkbank worked with these front companies to make their purchases appear to be of food and medicine destined for Iran so that the purchases would appear to be authorized by OFAC's food and medicine general license. As a result of these inaccurate payment descriptions, the indictment alleges that Iran was able to make over $20 billion of U.S. dollar-denominated transactions via its accounts at Halkbank and that the U.S. correspondent banks through which these payments passed were unaware that such payments were not in fact related to food or medicine purchases. The indictment also alleges that members of Halkbank's senior management took actions to conceal the true nature of these transactions from OFAC to avoid the secondary sanctions risk that Halkbank could itself be sanctioned for providing banking services to sanctioned Iranian entities. The case is pending in the U.S. District Court for the Southern District of New York.

Dandong Hongxiang Industrial Development Co. Ltd. Indictment. On July 23, 2019, DOJ announced the indictment of four Chinese nationals and a Chinese company, Dandong Hongxiang Industrial Development Co. Ltd. ("DHID").[108] The indictment alleges that DHID violated U.S. sanctions targeting North Korea and weapons of mass destruction proliferators when over the course of years it conducted U.S. dollar transactions on behalf of a number of North Korea entities, including several designated as SDNs pursuant to the Weapons of Mass Destruction sanctions program. DHID and the indicted individuals allegedly used more than 20 front companies to process these transactions through U.S. banks and took steps conceal the relation of the payments to North Korea. The front companies were allegedly located in jurisdictions that included the British Virgin Islands, the Seychelles, Hong Kong, Wales, England, and Anguilla, and the conspirators allegedly established bank accounts in the names of these front companies at Chinese banks that maintained U.S. correspondent banking relationships. The indictment also charges conspiracy to defraud the United States (*i.e.*, OFAC) and money laundering. OFAC had already designated DHID and the four indicted individuals in September 2016 due to this same alleged conduct.

DOJ Subpoena/Civil Contempt Litigation Regarding Three Chinese Banks. As discussed in our prior memorandum,[109] on July 30, 2019, the U.S. Court of Appeals for the District of Columbia affirmed civil contempt orders by the D.C. District Court against three Chinese banks for their failure to produce documents in response to U.S. government subpoenas relating to an investigation of North Korea's financing of its nuclear weapons program. For the two banks that had U.S. branches, DOJ served *Bank of Nova Scotia* subpoenas on the branches. For the bank that had no U.S. presence, DOJ had issued a subpoena pursuant to 31 U.S.C. 5318(k)(3)(A), a USA Patriot Act provision. The D.C. Circuit concluded that there was personal jurisdiction over all three banks because two of the banks consented to jurisdiction when they opened branches in the United States and the third bank's choice to maintain correspondent accounts in the United States was sufficient to sustain jurisdiction. The court further concluded that comity principles did not require that the subpoenas be quashed because the district court exercised appropriate discretion in finding that the comity concerns identified by the banks—including that compliance with the subpoenas would put the banks in breach of Chinese law—were outweighed by the national security interests of the United States. The D.C. Circuit decision likely will embolden DOJ to make further use of these authorities to obtain bank records located in China and other countries. Among other things, the court endorsed DOJ's expansive reading of the scope of the subpoena authority pursuant to 31 U.S.C. § 5318(k) as covering in some circumstances overseas records related to funds transfers that did not pass through a U.S. correspondent account

Sanctions Prosecution of Mahin Mojtahedzadeh. On July 19, 2019, DOJ announced that Mahin Mojtahedzadeh ("Mahin"), a citizen of Iran, pleaded guilty to conspiring to export gas turbine parts from the United States to Iran in violation of U.S. sanctions.[110] According to DOJ, Mahin was the President and Managing Dierector of a UAE-based export company, ETCO-FZC, which acted as a supplier for power generation companies in the Middle East, including Iran. Mahin admitted that from 2013 to 2017 she conspired to evade U.S. sanctions by working with companies in Canada and Germany, which acquired

approximately $3 million worth of gas turbines from a U.S. company and then re-exported them to Mahin for ultimate use in Iran. DOJ noted that two co-conspirators associated with the Germany company also pleaded guilty to sanctions conspiracy charges.

Sanctions Prosecution of Peyman Amiri Larijani. On June 4, 2019, DOJ announced a 34-count indictment against Peyman Amiri Larijani ("Larijani"), a citizen of Iran.[111] The indictment alleges that Larijani violated U.S. sanctions and export controls when he and a Turkish-based company for which he worked, Kral Aviation (which was also indicted) acquired U.S. origin aviation parts with the intention of reexporting those parts to Iranian aviation companies, including to Mahan Air, an SDN also listed on the BIS Denied Parties List. According to the indictment, the payments made by Larijani to purchase these U.S. origin items were denominated in U.S. dollars and processed by U.S. banks that were unaware of the connection to Iran. The indictment further alleges that Larijani and his co-conspirators attempted to conceal from the U.S. companies selling the parts that the ultimate end use and users of the aviation parts being sourced were in Iran. Similar to OFAC's Apollo Aviation enforcement action, this case shows the significant diversion risk with regard to U.S. origin aviation parts. The case is pending in the U.S. District Court for the District of Columbia.

Danske Bank Investigations. Following a 2014 whistleblower report regarding inadequate AML controls in the Tallinn, Estonia branch of Danske Bank ("Danske")—the largest bank in Denmark—Danske conducted an internal investigation, which expanded through 2018. In September 2018, Bruun & Hjele, a law firm hired by Danske to conduct an investigation into the branch's non-resident portfolio of foreign customers who were not residing in or conducting business from Estonia.[112] The law firm ultimately released a report detailing the various management failures, process deficiencies, and insufficient controls at the branch.[113] Between 2007 and 2015, approximately 9.5 million suspicious transactions totaling approximately $236 billion flowed through the branch.[114] Since the September 2018 report, Danske has been cooperating with investigating authorities in Estonia, Denmark, France, and the United States.[115] Several other banks are alleged to have been involved in the money laundering scheme as well.

In the United States, news reports indicate that DOJ had been conducting a criminal investigation into the alleged money-laundering scheme at Danske, which has focused in part on whether banks helped transfer money from the Danske Tallinn branch to the United States.[116] DOJ is also reportedly investigating whether financial institutions failed to timely report information related to certain suspicious transactions.[117] The SEC and the Treasury Department reportedly have similarly launched investigations.[118]

Federal Banking Agencies

Sanctions/AML compliance continues to be an area of important focus by the federal banking agencies.

Federal Banking Agency Enforcement Actions

UniCredit Group and Standard Chartered. As discussed above, the Federal Reserve was part of the multi-agency sanctions resolutions with UniCredit Group and Standard Chartered. For example, the Federal Reserve's cease and desist order against UniCredit Group imposed a $158 million penalty for its "unsafe and unsound practices relating to inadequate sanctions controls and supervision of its subsidiary banks." The Federal Reserve required UniCredit Group to submit an enhanced global compliance program for the Federal Reserve's review, which would include an annual global sanctions risk assessment, enhanced policies and procedures, a worldwide reporting hotline, and an annual compliance review.[119]

Daniel Weiss, former General Counsel of Rabobank, N.A. On July 23, 2019, the OCC announced the issuance of a consent order of prohibition and a $50,000 civil money penalty against Daniel Weiss, the former General Counsel of Rabobank, N.A. ("Rabobank"), a California-based subsidiary of the Dutch financial services company, for allegedly participating in the concealment of a third-party report assessing Rabobank's BSA/AML compliance program in violation of 12 U.S.C. § 481 and making false statements to the OCC in violation of 18 U.S.C. § 1001.[120] Mr. Weiss's penalty follows a February 2018 enforcement action by the OCC and DOJ against Rabobank,[121] in which Rabobank plead guilty to one count of conspiracy to obstruct the OCC's attempts to identify deficiencies in Rabobank's BSA/AML compliance program involving branch activity along the U.S.-Mexico border. Rabobank paid $368.7 million in penalties to DOJ and a $50 million fine to the OCC. The guilty plea related to the OCC's request that Rabobank turn over reports drafted by consultants retained to evaluate the bank's BSA/AML compliance program—reports which were highly critical of the program.

The OCC's notice of charges against Mr. Weiss alleged that he received a third-party audit report assessing Rabobank's BSA/AML controls and distributed it to bank executives in March 2013.[122] Mr. Weiss subsequently submitted a response to the OCC on behalf of Rabobank that failed to disclose the consultant's report. The OCC alleges that Weiss subsequently "knowingly and willfully participated in the making of materially false statements regarding the Bank's possession of the [audit firm] Report to the OCC continuously and repeatedly throughout March of 2013 until April 18, 2013." In addition to assessing a $50,000 penalty, the consent order prohibits Mr. Weiss from participating in the affairs of any federally insured depository institution. The penalty is in line with the OCC's recent trend of assessing AML-related penalties against individuals for knowing and willful conduct.

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, Sumitomo Mitsui Banking Corporation entered into a written agreement

with the Federal Reserve to address deficiencies in the New York Branch's BSA/AML compliance program.[123] Although it did not involve penalties, the financial institution was required to develop and implement plans for strengthening BSA/AML compliance and to conduct a lookback.

Securities and Exchange Commission and Financial Industry Regulatory Authority

The SEC and FINRA have continued to pursue AML-related enforcement actions, which have recently focused on AML program deficiencies and the failure to file SARs relating to low-priced securities transactions.

Quad/Graphics, Inc. On September 26, 2019, the SEC announced a nearly $10 million dollar cease and desist order against Quad/Graphics Inc., a U.S. digital and print marketing provider, for Foreign Corrupt Practices Act ("FCPA") violations.[124] In addition to bribery allegations, the SEC determined that Quad/Graphics' Peruvian subsidiary violated the FCPA's books and records provisions by creating false records to conceal transactions with a state-controlled Cuban telecommunications company which violated U.S. sanctions and export controls laws. This appears to be the first time that the SEC has made use of the books and records provisions of the FCPA in connection with U.S. sanctions violations. This matter may signal that the SEC intends to play a more active role in sanctions enforcement in the future.

SEC* v. *Alpine. As described in last year's annual review and our separate memorandum, on December 11, 2018, the SEC prevailed in its enforcement action against Alpine Securities Corporation, a clearing broker that allegedly failed to file SARs relating to certain microcap securities transactions.[125] 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.[126] 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.

On September 26, 2019, Judge Cote imposed a $12 million penalty and a permanent injunction against further violations. The court considered a number of factors in reaching this outcome, including: (i) the breadth and regularity of Alpine's violations; (ii) Alpine's awareness of the nature and extent of its SAR violations; (iii) the increased risk to investors caused by these violations; (iv) the recurrent nature of the violations; and (v) Alpine's failure to admit wrongdoing and its lack of cooperation with authorities.[127] On October 10, 2019, Alpine filed a notice of appeal with the Second Circuit.[128]

BNP Paribas. On October 23, 2019, FINRA fined BNP Paribas Securities Corp. and BNP Paribas Prime Brokerage, Inc. ("BNP") $15 million for AML program and supervisory failures involving low-priced security deposits and resales and certain wire transfers over a four-year period. BNP neither admitted nor denied the charges, but consented to the entry of FINRA's findings.[129]

FINRA found that, from February 2013 to March 2017, BNP failed to implement a written AML program that could monitor potentially suspicious transactions related to low-priced securities activity. Specifically, FINRA alleged that until 2016, BNP's AML program did not conduct any surveillance targeting transactions in low-priced securities or securities trading outside of the traditional exchanges, and focused solely on wire transfers conducted in U.S. dollars.[130] FINRA found that BNP did not review foreign currency wires to determine whether they involved high-risk entities or jurisdictions, and that its AML program was not reasonably designed to identify wire transfers (or a pattern of wire transfers) conducted in amounts that would avoid attention or review.[131] FINRA also characterized BNP's AML program as understaffed.[132] FINRA further observed that BNP identified many of these deficiencies as early as January 2014, but did not fully revise its AML program until March 2017. As a result, BNP allegedly did not identify red flags indicative of, or review, potentially suspicious activity involving the deposit and sales of low-priced securities or foreign wire transfers that may have required a filing of a SAR.[133]

New York Department of Financial Services

It remains to be seen how the DFS's new leadership intends to approach sanctions and AML matters, including the application and potential enforcement of Part 504, DFS's regulation that imposes various sanctions/AML program requirements on DFS-regulated entities. Other than the UniCredit and Standard Chartered actions described above—which were substantially complete prior to Superintendent Lacewell's appointment—DFS was relatively quiet on the sanctions/AML front in 2019.

DFS Organizational Developments

Lacewell Appointment. In late December 2018, former Superintendent Maria Vullo announced that she would be leaving DFS, effective February 1, 2019. On January 4, 2019, Governor Cuomo announced the appointment of Linda A. Lacewell as the new acting Superintendent.[134] She assumed office on February 11, 2019, and was confirmed on June 21, 2019.[135] Lacewell previously served as Cuomo's Chief of Staff and, before that, as a federal prosecutor in the U.S. Attorney's Office for the Eastern District of New York.[136]

New Consumer Protection and Financial Enforcement Division. On April 29, 2019, Superintendent Lacewell announced the combination of DFS's previously separate Enforcement Division and Financial Frauds and Consumer Protection Division into a newly created Consumer Protection and Financial Enforcement Division.[137] The new division is headed by Executive Deputy Superintendent Katherine A. Lemire, a former partner at a compliance consulting firm and a former federal and city prosecutor. The reorganization appears to have been motivated, at least in part, by DFS's perception of a "troublesome policy shift away from consumer protection" at the federal Consumer Financial Protection Bureau (CFPB), which motivated DFS to "take action to fill the increasing number of regulatory voids created by the federal government."[138]

New Cybersecurity Division. On May 22, 2019, DFS announced the creation of a new Cybersecurity Division.[139] The new division will "enforce [DFS's] cybersecurity regulations, advise on cybersecurity examinations, issue guidance on DFS's cybersecurity regulations, and conduct cyber-related investigations[.]" The division will also disseminate information on trends and threats concerning cyber-attacks. The Cybersecurity Division is headed by Justin Herring, who had been Chief of the Cyber Crimes Unit in the United States Attorney's Office for the District of New Jersey. The creation of the new Cybersecurity Division suggests that DFS intends to vigorously enforce and examine compliance with its groundbreaking cybersecurity regulations, which went into effect in phases during a two-year transitional period ending March 1, 2019.[140]

Additional Developments

Designation of Chinese Companies Under U.S. Export Controls

In 2019, the U.S. Commerce Department's Bureau of Industry and Security ("BIS") made two waves of additions of Chinese companies to the Entity List. In May 2019, BIS designated Huawei Technologies Co. Ltd. and 69 of its non-U.S. affiliates located worldwide to the Entity List (BIS subsequently added another 46 affiliates of Huawei to the Entity List in August 2019 (all such listed entities, collectively "Huawei")). In October 2019, BIS designated 8 Chinese technology and video companies, as well as 20 regional Chinese government entities, to the Entity List. Designating major companies located in a non-sanctioned country to the Entity List is a novel use of U.S. export controls and contributed to the increase of tensions between the United States and China in 2019. The Entity List designation of a company as pervasive as Huawei led U.S. and non-U.S. companies alike scrambling and has brought renewed attention to U.S. export control regulations and compliance measures. As a field adjacent to sanctions, we briefly highlight last year's significant export control developments below.

Huawei. On May 16, 2019, BIS announced the designation of Huawei and 69 of its non-U.S. affiliates to the Entity List and the designations became effective on May 21, 2019.[141] The announcement in the Federal Register noted that the designation of Huawei was at least partially related to its indictment in U.S. federal court on 13 counts (see description above in the DOJ section), which included alleged violations of U.S. sanctions. Designation to the Entity List has the effect of broadly prohibiting the listed entities from receiving any item subject to the U.S. Export Administration Regulations ("EAR"), no matter where the item was manufactured or located or the nationality of the individual or entity in possession of the item, unless authorized by BIS (and BIS' licensing policy with regard to persons on the Entity List is generally a presumption of denial).

On May 20, 2019, BIS issued a temporary general license permitting certain activities related to Huawei for 90 days (*i.e.*, until August 19, 2019), although this temporary general license has since been extended two times, and it now expires on February 16, 2020 (but may be subsequently renewed for another 90 days).[142] Although, Huawei's placement on the Entity List broadly prohibits companies from providing Huawei with

any goods that are subject to the EAR, the general license from BIS temporarily permits four types of activities related to Huawei, including: (i) continued operation of existing networks and equipment; (ii) support for existing handsets; (iii) cybersecurity research and vulnerability defense; and (iv) engagement as necessary for the development of 5G standards by a "duly recognized" standards body. The use of the temporary general license is subject to certain certification and recordkeeping requirements.

As a result of the Huawei designation, exports to Huawei by U.S. manufacturers and of items manufactured in the United States were essentially prohibited absent a license from BIS. Meanwhile, many non-U.S. companies that provided products to Huawei have had to examine whether their products, even if manufactured outside of the United States, contained a sufficient amount of controlled U.S. content to qualify the products as subject to the EAR. Additionally, in obtaining products from Huawei, companies have had to be mindful that they have not been knowingly receiving U.S.-origin items from Huawei that may have been obtained by Huawei in violation of U.S. export controls. Given Huawei's vast global presence and the wide diversity of its product portfolio, confirming these points can be burdensome, particularly for companies located outside of the United States.

Hikvision, *et al*. On October 7, 2019, BIS added 28 entities to the Entity List. These additions comprised 20 regional Chinese government entities including and related to the Xinjiang Uighur Autonomous Region ("XUAR") People's Government Public Security Bureau and 8 companies: Dahua Technology; Hikvision; IFLYTEK; Megvii Technology; Sense Time, Xiamen Meiya Pico Information Co. Ltd.; Yitu Technologies; and Yixin Science and Technology Co. Ltd.[143] No subsidiaries or affiliates of these 28 designated entities were added to the Entity List at the time of this designation. The designations' effective date was October 9, 2019.

BIS stated that these designations had been made because "these entities have been implicated in human rights violations and abuses in the implementation of China's campaign of repression, mass arbitrary detention, and high-technology surveillance against Uighurs, Kazakhs, and other members of Muslim minority groups in the XUAR."[144] These sorts of human rights concerns are a novel basis for Entity List designations and demonstrate the current Administration's increased willingness to use the Entity List as a foreign policy tool, particularly with regard to Chinese companies. Unlike the designation of Huawei, however, no corresponding temporary general license was issued along with these designations, meaning that the export, reexport, or transfer of any item subject to the EAR to these designated entities now requires a license from BIS (and, as discussed above, such licenses are generally subject to a presumption of denial).

Virtual Currency

The continued proliferation of virtual currencies presents a number of challenges related to BSA/AML and sanctions compliance.

As discussed above, FinCEN has continued to take strides in its interpretation and regulation of virtual currencies. On April 18, 2019, FinCEN announced its first enforcement action against an individual peer-to-peer virtual currency exchanger, as well as the first instance in which it had penalized an exchanger for failure to file CTRs. On May 9, 2019, FinCEN issued interpretive guidance regarding the application of FinCEN regulations to business models involving the transmission of CVCs. That same day, FinCEN issued an advisory regarding the use of virtual currency to support illegal activity, money laundering, and other behavior endangering U.S. national security.

On October 11, 2019, the CFTC, FinCEN, and SEC issued a joint statement on activities involving digital assets.[145] In this statement, the agencies discuss the AML/CFT obligations that apply to entities that the BSA defines as "financial institutions," as well as the factors involved in determining whether and how a person or entity must register with one or more of the different agencies. Each agency also separately provided additional commentary regarding the application of BSA regulations to their specific agencies.

At the state level, the New York DFS continues to be a leader in addressing virtual currency through the continued issuance and denial of virtual currency licenses, also known as BitLicenses. On March 27, 2019, DFS issued a BitLicense and a money transmission license for Tagomi Trading, LLC, an aggregation platform for trading virtual currencies across multiple platforms that hails itself as "New York's first brokerage for virtual currencies."[146] On April 9, 2019, DFS issued a BitLicense to Bitstamp USA, Inc., a U.S.-based subsidiary of Luxembourg-based cryptocurrency exchange Bitstamp Ltd.[147] On April 10, 2019, DFS denied the application of Bittrex, Inc. for a BitLicense and a money transmitter license.[148] In its press release, DFS explained that Bittrex's applications were being denied "primarily due to deficiencies in Bittrex's BSA/AML/OFAC compliance program; deficiency in meeting the Department's capital requirement; and deficient due diligence and control over Bittrex's token and product launches."[149] After denying DFS's applications, DFS required Bittrex to cease operating in New York State and wind down its New York business within 60 days. On December 11, 2019, DFS announced that, in order to enhance efficiency and enable virtual currency licensees to offer and use new coins in a timely fashion, DFS is seeking comments regarding coin adoption or listing options that DFS wishes to make available to virtual currency licensees.[150]

At the international level, on June 21, 2019, the Financial Action Task Force ("FATF") published updated guidance detailing a risk-based approach to regulating virtual assets and virtual asset service providers.[151] FATF's updated guidance discusses (1) AML/terrorist financing risks associated with virtual asset activities, and best practices for taking appropriate mitigating measures; (2) activities and entities that fall within FATF's definitions of virtual asset activities and virtual asset service providers; (3) the application of FATF's recommendations to countries and regulatory authorities, virtual asset service providers, and other entities that engage in virtual asset activity, including banks and securities broker-dealers; (4) obligations applicable to virtual assets and virtual asset service providers under the FATF recommendations; (5) virtual asset service provider registration or licensing requirements, including in which jurisdictions service

providers are required to register; (6) the need for independent (as opposed to self-regulatory) risk-based supervisory or monitoring bodies for virtual asset service providers; (7) the application of preventative measures previously described in FATF's recommendations to virtual assets and virtual asset service providers; and (8) examples of different jurisdictional approaches to regulating, supervising, and enforcing virtual asset activities for AML and counter-terrorist financing purposes.

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. **Review and Respond to OFAC's Guidance on Sanctions Compliance Programs**. Although OFAC's regulations do not themselves require the implementation of a compliance program, OFAC's May 2019 compliance guidance, and the related "compliance commitments" in recent OFAC settlements, represent a new effort by OFAC to more clearly and comprehensively communicate its expectations about appropriate sanctions compliance practices. The Framework describes numerous sanctions compliance best practices and largely aligns with the compliance expectations of the federal banking regulators. Accordingly, many banks operating in the United States—and many large, sophisticated companies outside the financial sector—likely already incorporate the sanctions compliance elements described in the guidance.

   For the large majority of U.S. and non-U.S. companies that engage in international trade, however, there may be gaps between their current practices and the elements described in the guidance. It is important for such companies to study the guidance in light of their own sanctions risk profiles (including factors such as the company's size and sophistication, products and services offered, customers and counterparties, and geographic locations) to determine whether updating or enhancing their programs would be appropriate. In many ways, the guidance can be viewed as the "gold standard" for compliance, and companies with lower risk profiles may be able to implement lesser measures. Nonetheless, as demonstrated by recent enforcement trends, the failure to have in place an effective, appropriately tailored, compliance program, may be viewed by OFAC as an aggravating factor in the event of an enforcement action.

2. **Strengthen Sanctions Diligence and Compliance Pre- and Post-Acquisition**. Several OFAC enforcement actions in 2019 imposed liability on U.S.-based acquiring entities for the apparent sanctions violations of their newly acquired non-U.S. subsidiaries. Sanctions-related reviews of acquisition targets to identify and assess risk remain a key part of pre-acquisition compliance diligence and OFAC has continued to stress the importance of this diligence. In addition, implementing and following through on post-acquisition sanctions enhancements (particularly in the case of the acquisition of non-U.S. entities) remains a key theme of recent OFAC enforcement actions. As shown in the *Kollmorgen* and *Stanley Black & Decker* enforcement actions, OFAC will hold U.S. parents liable

for the apparent sanctions violations of their acquired non-U.S. subsidiaries, but the penalty amounts can vary significantly based upon the level of pre-acquisition diligence and post-acquisition compliance integration and monitoring efforts.

3. **Enhance Sanctions Components of Supply-Chain Diligence.** As highlighted by OFAC's settlement with ELF, sanctions-related risks can arise not only with regard to a company's customers, but also its suppliers and even the jurisdictions from which its suppliers source. OFAC has noted that companies that do not conduct "full-spectrum supply chain due diligence" when sourcing products from outside of the United States face increased sanctions-related risks. This is particularly true when, as was the case in the *ELF* enforcement action, products are sourced from areas that border comprehensively sanctioned countries. Additionally, non-U.S. companies that export to the United States could also face OFAC liability if they knowingly export products to the United States that were sourced in a comprehensively sanctioned country or incorporate materials or components sourced from a comprehensively sanctioned country.

4. **Tailor and Regularly Update Sanctions Compliance Procedures**. OFAC's 2019 guidance regarding sanctions compliance programs explicitly conveys OFAC's expectation that U.S. and non-U.S. companies doing U.S.-related business will "develop, implement, and routinely update" risk-based sanctions compliance programs *tailored to their particular business operations*. OFAC recommends that companies conduct risk assessments to determine the particular risks posed by its clients, customers, and other counterparties, products, supply chain, and geographic locations. OFAC has repeatedly demonstrated its willingness to pursue enforcement actions where this expectation is not met. For example, in the context of the Apple settlement, OFAC noted, with respect to Apple's transfer of ownership of blocked property to two different software companies that "compliance measures should. . . anticipate potential vulnerabilities in a company's compliance program that could allow sanctions evasion and circumvention, and should include preventative measures that alert and react to sanctions evasion warning signs." As part of this effort, companies would be well-served to ensure that their compliance programs are capable of detecting and rejecting "second attempt" transactions where a counterparty or non-U.S. subsidiary restructures a transaction initially rejected for compliance reasons in an attempt to consummate the violative transaction (see *PACCAR*) and of flagging "unorthodox business practices" (see *Haverty*).

5. **Strengthen Sanctions Monitoring Mechanisms During the Life of a Contractual Relationship**. As shown in the *Apollo Aviation* enforcement action, OFAC has stated that sanctions compliance provisions in contractual agreements alone are not sufficient to shield U.S. companies from liability should their non-U.S. counterparty sublease U.S.-origin goods to a comprehensively sanctioned country or otherwise in violation of U.S. sanctions. Depending on the circumstances and the level of sanctions risk involved (which is determined by the industry, counterparties, geographies, and other factors), companies may need to take additional measures after the point of initial transfer

to monitor whether their counterparties are complying with U.S. sanctions restrictions. Although there are no one-size-fits-all solutions, OFAC has made clear that sanctions contractual provisions will not, by themselves, be a shield to liability and that OFAC often expects companies to take additional measures (such as export control compliance provisions and monitoring of available shipping or location data) to monitor and minimize sanctions risk.

6. **Continued Caution Around U.S. Dollar Transactions**. In its landmark 2017 settlement with CSE Global and CSE TransTel, two Singapore-based companies, OFAC found that they violated U.S. sanctions by sending U.S. dollar payments involving Iran, where the payments cleared through U.S. financial institutions and thereby "caused" them to violate sanctions by exporting financial services to a comprehensively sanctioned country.[152] For some non-U.S. companies, conducting business involving sanctioned jurisdictions or parties in U.S. dollars—even without any other U.S. touchpoints—remains a major area of sanctions-related risk.

   There also remains uncertainty over what uses of U.S. dollars in connection with sanctioned jurisdictions or parties (such as utilizing non-U.S. clearing mechanisms) would be viewed by OFAC or DOJ as compliant with applicable sanctions. In 2019, OFAC signaled a potentially expansive view regarding U.S. dollar payments in the *British Arab Commercial Bank* enforcement action, in which OFAC determined that bulk U.S. dollar payments processed by BACB through U.S. financial institutions were apparent violations of OFAC's Sudan regulations because they were used to fund a U.S. dollar account at a non-U.S. financial institution, which was in turn used to process payments for sanctioned parties with accounts at the same bank. With regard to U.S. dollars, it remains unclear what level of attenuation between U.S. financial institutions and sanctioned jurisdictions will remove the risk of liability. Finally, the *Huawei* and *Halkbank* cases show that DOJ can prosecute the use of U.S. dollar payments not just by using sanctions, but also by charging bank fraud, which, unlike sanctions charges, has a ten-year statute of limitations. As a result, non-U.S. companies should remain highly cautious about any use of U.S. dollars in connection with U.S. sanctioned jurisdictions or parties.

7. **Increase Focus on Venezuela-related Risks**. Venezuela sanctions continued to expand in 2019 and now encompass the Government of Venezuela as well as a number of prominent state-owned entities, including PDVSA. Although the sanctions targeting Venezuela are not a comprehensive embargo, given the prominence of the Government of Venezuela (including state-owned entities) in the Venezuelan economy, some compliance departments are considering whether to treat Venezuela as though it were subject to comprehensive U.S. sanctions. Additionally, under several of the executive orders imposing sanctions on the Venezuelan Government and state-owned entities, there is a risk that non-U.S. companies could themselves be the target of U.S. sanctions if they provide material assistance to the Maduro regime.

8. **Renew Focus on the Shipping and Aviation Industries**. In 2019, OFAC issued two advisories to the global shipping industry and one to the aviation industry regarding deceptive practices by Iran

as well as attempts to conceal shipments of petroleum to Syria. As shown in the *Apollo Aviation* enforcement action, OFAC clearly expects participants in these industries to be aware of the sanctions risks in such industries regardless of sanctions program (the *Apollo Aviation* enforcement action referenced the Iran aviation advisory, but involved apparent violations of the Sudanese sanctions). Companies that operate in or facilitate (such as by providing financial services or insurance) international shipping and aviation activities should be mindful of OFAC's renewed focus on these areas and OFAC's recommended risk-mitigation measures. For example, in the shipping context, OFAC emphasized that, given the ability of illicit actors to change the name of vessels, "it is essential to research a vessel not only by name, but also by its International Maritime Organization (IMO) number."[153]

9. **Strengthen BSA/AML Controls Related to Low-Priced Securities Trading**. The SEC and FINRA continue to focus on broker-dealer BSA/AML controls, with a particular emphasis on low-priced securities trading. Financial institutions should ensure appropriate assessment of BSA/AML risk associated with securities trading and confirm that activity is monitored commensurate with identified risk. Broker-dealers should confirm that SAR-filing procedures adequately respond to regulator expectations for identifying suspicious activity associated with securities trading.

10. **Enhance Compliance Procedures for Virtual Currency Businesses and Clients**. In 2019, regulators continued to emphasize the potential risks posed by virtual currency transactions and businesses. Regulatory expectations of appropriate monitoring of virtual currency BSA/AML and sanctions risk are increasing as further guidance and advisories related to virtual currency are issued. Among other things, financial institutions should ensure that all procedures are updated to consider the unique risks of virtual currencies, including virtual currency exchangers. When evaluating potentially suspicious activity, FinCEN advises that red flags relevant to identifying efforts to circumvent AML and Sanctions controls include (1) if a customer transfers or receives funds to or from an unregistered foreign virtual currency exchange, or other MSB with no relation to where the customer lives or conducts business; (2) if a customer conducts transactions with virtual currency addresses that have been linked to extortion, ransomware, sanctioned addresses, or other illicit activity; and (3) if a customer's transactions are initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious.

11. **Consider BSA/AML Risk of Correspondent Banking Relationships with Higher-Risk Financial Institutions**. As the expanding Danske Bank inquiry has demonstrated, financial institutions should consider the regulatory risk and compliance costs associated with maintaining correspondent banking relationships with financial institutions with high-risk customers or located in higher-risk jurisdictions. U.S. dollar clearing services pose unique risks as financial institutions have more limited information about underlying transaction activity. U.S. regulators expect that banks that

provide services to higher risk financial institutions will appropriately monitor for and report suspicious activity flowing through correspondent banking channels.

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	Christopher D. Frey +81-3-3597-6309 cfrey@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 Robyn Bernstein, Theo Galanakis, Udi Karklinsky, Sofia Martos, Mariah Rivera, James R. Simmons, Jr., Jacobus "Janus" Schutte, Katherine S. Stewart, Sylvia Sui, Joshua R. Thompson, Apeksha Vora, Bailey Williams, and Law Clerk Jacob A. Braly contributed to this Client Memorandum.

---

1 *See* U.S. Dep't of the Treasury, Press Release, *Treasury Targets Assets of Russian Financier who Attempted to Influence 2018 U.S. Elections* (Sept. 30, 2019), *available* here; U.S. Dep't of the Treasury, Press Release, *Treasury Announces Sanctions under the Chemical and Biological Weapons Control and Warfare Elimination Act* (Aug. 3, 2019), *available* here.

2 U.S. Dep't of the Treasury, Press Release, *Treasury Designates Turkish Ministries and Senior Officials in Response to Military Action in Syria* (Oct. 14, 2019), *available* here.

3 U.S. Dep't of the Treasury, Press Release, *Treasury Removes Sanctions Imposed on Turkish Ministries and Senior Officials Following Pause of Turkish Operations in Northeast Syria* (Oct. 23, 2019), *available* here.

4 Dylan Tokar, *Treasury Department Changes Approach to Fines in Sanctions Cases*, THE WALL STREET JOURNAL (June 14, 2019), available here. Director Gacki cited OFAC's settlements with Standard Chartered Bank and UniCredit Group SpA as examples of OFAC's new approach.

5 Alan Rappeport, *Trump's Top Sanctions Official Will Depart*, THE NEW YORK TIMES (Oct. 2, 2019), available here.

6 White House, Press Release, *President Donald J. Trump Announces Intent to Nominate and Appoint Individuals to Key Administration Posts* (Dec. 10, 2019), *available* here.

7 *See* Paul, Weiss, *OFAC Issues Guidance on Sanctions Compliance Programs and Flags "Root Causes" Underlying Prior Enforcement Actions* (May 14, 2019), *available* here.

8 U.S. Dep't of the Treasury, Office of Foreign Assets Control, *A Framework for OFAC Compliance Commitments*, (May 2, 2019), *available* here.

9 *Id.*

10 *Id.*

11 *See* 31 C.F.R. Part 501, App. A, *Economic Sanctions Enforcement Guidelines*, *available* here.

12 White House, Press Release, *Statement from the Press Secretary on Cooperation between the United States, Saudi Arabia, and the United Arab Emirates on Energy and Iran Policies* (Apr. 22, 2019), *available* here.

13 Executive Order 13871, *Imposing Sanctions with Respect to the Iron, Steel, Aluminum, and Copper Sectors of Iran* (May 8, 2019), *available* here.

14 Executive Order 13876, *Imposing Sanctions with Respect to Iran* (June 24, 2019), *available* here.

15 *See* U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Frequently Asked Questions Regarding Executive Order (E.O.) "Imposing Sanctions with Respect to the Iron, Steel, Aluminum, and Copper Sectors of Iran" of May 8, 2019, Question 810* (Dec. 11, 2019), *available* here.

16 The EU Blocking Regulation, as amended, prohibits any "EU operator" (generally, any person or entity residing or incorporated in the EU) 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. *See* Paul, Weiss, *Economic Sanctions & Anti-Money Laundering Developments: 2018 Year in Review* (Feb. 5, 2019), *available* here.

17 In the first UK decision to interpret the relationship between U.S. sanctions on Iran and the EU Blocking Regulation, *Mamancochet Mining Ltd v Aegis Managing Agency Ltd & Others* [2018] EWHC 2643 (Comm), the High Court included an *obiter* comment that the EU Blocking Regulation would not apply where an insurer's liability is suspended under a sanctions clause, because an insurer in that scenario would not be "complying" with a third country's prohibition, but would instead simply be relying the terms of the policy to resist payment. The High Court held that defendant underwriters were liable for failure to pay an insurance claim under a marine cargo policy, following theft at a port in Iran. The defendants argued that they were not liable because the sanctions clause in the policy provided that they would not have to pay any claim that would "expose" them to sanctions, but the High Court rejected this argument on the basis that (i) the mere risk of sanctions (as opposed to an actual breach of sanctions) was insufficient to create an "exposure" to sanctions under U.S. or EU law, and (ii) there was no "exposure" to sanctions, provided the payment of the insurance claims would be made prior to November 5, 2018 (when the relevant U.S. sanction on Iran would become effective, following the conclusion of the wind-down period). Two 2018 Regional Court decisions in Hamburg involving banking services in Germany that were subject to U.S. sanctions resulted in different outcomes based on the facts at hand, but both decisions included reasoning that suggests that consideration will be

given to the commercial consequences of performing banking services in violation U.S. sanctions, rather than a strict application of the EU Blocking Regulation. In contrast, two recent Italian cases offered a much stricter interpretation of the EU Blocking Regulation: in the first case, the Italian court ordered an injunction preventing an Italian bank from terminating its services to an Italian company controlled by partners in Iran over concerns of U.S. sanctions, because in doing so the bank would breach the EU Blocking Regulation; and in the second case, the Italian court ordered the release of funds frozen by an Italian company's bank upon finding that U.S. sanctions designations do not have effect in the EU. Similarly, a Dutch court recently ordered Dutch software company Exact to restore its contractual services of distributing software to Cuba; Exact had terminated the agreement at issue upon being acquired by KKR, an American investment company, because of exposure to U.S. sanctions risk. The Court held that the termination was not in accordance with standards of reasonableness and fairness, because the sanctions risk was Exact's burden to bear and did not constitute *force majeure*. In addition, this case has led to one of the first reported EU Member State government investigations for violation of the EU Blocking Regulation, which was begun by Dutch Customs at the request of the European Commission.

18 Foreign Ministers of France, Germany and the United Kingdom, Press Release, *E3 foreign ministers' statement on the JCPoA: 14 January 2020* (Jan. 14, 2020), *available* here.

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

20 On February 1, 2019, in relation to this action, OFAC issued two amended FAQs, *available* here and here, and eleven new FAQs, *available* here. *See also* 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.

21 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.

22 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.

23 Executive Order 13857, *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. To mitigate some of the effects of this broad definition, OFAC issued General License 4B, which has since been superseded by General License 4C, *available* here.

24 Executive Order 13884, *Blocking Property of the Government of Venezuela* (Aug. 5, 2019), *available* here.

25 U.S. Dep't of Treasury, Press Release, *Treasury and Commerce Implement Changes to Cuba Sanctions Rules* (June 4, 2019), *available* here.

26 U.S. Dep't of Treasury, Press Release, *Treasury Issues Changes to Strengthen Cuba Sanctions Rules* (Sept. 6, 2019), *available* here.

27 Now defined in the CACR as including any Cuban national who is: "(a) an owner or employee of a small private business or a sole proprietorship, including restaurants (paladares), taxis, and bed-and-breakfasts (casas particulares); (b) an independent contractor or consultant; (c) a small farmer who owns his or her own land; or (d) a small usufruct farmer who cultivates state-owned land to sell products on the open market."

[28] 31 C.F.R. § 515.340.

[29] U.S. Dep't of State, Remarks by Secretary of State Michael R. Pompeo (May 2, 2019), *available* here.

[30] Five of these entities were delisted on December 18, 2019. *See* U.S. Dep't of the Treasury, Press Release, *Global Magnitsky Designation Removal; Issuance of Amended Global Magnitsky General License* (Dec. 18, 2019), *available* here.

[31] U.S. Dep't of the Treasury, Press Release, *Treasury Works with Government of Mexico Against Perpetrators of Corruption and their Networks* (May 17, 2019), *available* here.

[32] U.S. Dep't of the Treasury, Press Release, *Treasury Sanctions Persons Associated with Serious Human Rights Abuse and Corrupt Actors in Iraq* (July 18, 2019), *available* here.

[33] U.S. Dep't of the Treasury, Press Release, *Treasury Sanctions Former Ugandan Inspector General of Police for Role in Serious Human Rights Abuse and Corruption* (Sept. 13, 2019), *available* here.

[34] U.S. Dep't of the Treasury, Press Release, *Treasury Sanctions Members of a Significant Corruption Network in South Africa* (Oct. 10, 2019), *available* here.

[35] *Id.*

[36] U.S. Dep't of the Treasury, Press Release, *Treasury Targets Wide Range of Terrorists and Their Supporters Using Enhanced Counterterrorism Sanctions Authorities* (Sept. 10, 2019), *available* here.

[37] U.S. Dep't of the Treasury, OFAC, *Reporting, Procedures and Penalties Regulations* 84 Fed. Reg. 29,055 (Jun. 21, 2019), *available* here.

[38] OFAC also made a number of technical changes to the RPPR regarding applications for the release of blocked funds and OFAC's electronic license application procedures.

[39] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *OFAC Advisory to the Maritime Petroleum Shipping Community: Sanctions Risks Related to Petroleum Shipments involving Iran and Syria* (Mar. 25, 2019), *available* here.

[40] *Id.*

[41] *Id.*

[42] U.S. Dep't of the Treasury, U.S. Dep't of State, and U.S. Coast Guard, *North Korea Sanctions Advisory: Updated Guidance on Addressing North Korea's Illicit Shipping Practices* (Mar. 21, 2019), *available* here.

[43] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *OFAC Advisory to the Maritime Petroleum Shipping Community: Sanctions Risks Related to Petroleum Shipments involving Iran and Syria* (Sept, 4, 2019), *available* here.

[44] *Id.*

[45] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Iran-Related Civil Aviation Industry Advisory: Deceptive Practices by Iran with respect to the Civil Aviation Industry* (July 23, 2019), *available* here.

[46] Compl., *Intrater* v. *United States*, No. 1:19-cv-06139 (S.D.N.Y. July 1, 2019).

[47] Paul, Weiss, *UniCredit Group Banks Agree to Pay a Combined $1.3 Billion Penalty for Iranian and Other Sanctions Violations; One Bank Pleads Guilty* (May 1, 2019), *available* here.

[48] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *UniCredit Bank AG Settles Potential Civil Liability for Apparent Violations of Multiple Sanctions Programs* (Apr. 15, 2019), *available* here.

[49] Paul, Weiss, *UniCredit Group Banks Agrees to Pay a Combined $1.3 Billion Penalty for Iranian and Other Sanctions Violations; One Bank Pleads Guilty* (May 1, 2019), *available* here.

[50] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Standard Chartered Bank Settles Potential Civil Liability for Apparent Violations of Multiple Sanctions Programs* (Apr. 9, 2019), *available* here.

[51] Paul, Weiss, *OFAC Reaches Settlement Agreement with U.K. Bank for Complex Payment Structures Used to Circumvent U.S. Sanctions* (Sept. 19, 2019), *available* here.

[52] U.S. Dep't of Treasury, OFAC, *British Arab Commercial Bank plc Settles Potential Liability for Apparent Violations of the Sudanese Sanctions Regulations* (Sep. 17, 2019), *available* here.

[53] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *AppliChem GmbH Assessed a Penalty for Violating the Cuban Assets Control Regulations* (Feb. 14, 2019), *available* here.

[54] *Id.*

[55] *Id.*

[56] Paul, Weiss, *In Unprecedented Move, OFAC Takes Enforcement Action Against U.S. Parent Company for Turkish Subsidiary's Iran Sanctions Violations and Simultaneously Sanctions the Subsidiary's Ex-Managing Director* (Feb. 11, 2019), *available* here.

[57] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Kollmorgen Corporation Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations* (Feb. 7, 2019), *available* here.

[58] Paul, Weiss, *OFAC Takes Enforcement Action Against U.S. Parent Company for its Recently Acquired Chinese Subsidiary's Iran Sanctions Violations* (Apr. 1, 2019), *available* here.

[59] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Stanley Black & Decker, Inc. Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations Committed by its Chinese-Based Subsidiary Jiangsu Guoqiang Tools Co. Ltd.* (Mar. 27, 2019), *available* here.

[60] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and PACCAR Inc.* (Aug. 6, 2019), *available* here.

[61] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Acteon Group Ltd., and 2H Offshore Engineering Ltd. Settle Potential Civil Liability for Apparent Violations of the Cuban Assets Control Regulations* (Apr. 11, 2019), *available* here. The OFAC and Acteon, 2H Offshore, and 2H KL Settlement Agreement is available here.

[62] OFAC noted that KKR and its affiliated investment funds did not appear to have been directly involved in the apparent violations involving Iran, and the apparent violations involving Cuba pre-dated the ownership of KKR and its affiliated investment funds in Acteon.

[63] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Separately, Acteon Group Ltd. Settles Potential Civil Liability for Apparent Violations of the Cuban Assets Control Regulations, and KKR & Co. Inc. Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations* (Apr. 11, 2019), *available* here.

[64] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Hotelbeds USA, Inc. Settles Potential Civil Liability for Apparent Violations of the Cuba Assets Control Regulations*, 31 C.F.R. part 515 (June 13, 2019), *available* here.

65 U.S. Dep't of Treasury, Office of Foreign Assets Control, *An Individual and Cubasphere Inc. Settle Potential Civil Liability for Apparent Violations of the Cuban Assets Control Regulations* (June 13, 2019), *available* here.

66 U.S. Dep't of Treasury, Office of Foreign Assets Control, *Chubb Limited (as Successor Legal Entity of the Former ACE Limited) Settles Potential Liability for Apparent Violations of the Cuban Assets Control Regulations* (Dec. 9, 2019), *available* here.

67 *Id.*

68 U.S. Dep't of Treasury, Office of Foreign Assets Control, *Allianz Global Risks US Insurance Company Settles Potential Liability for Apparent Violations of the Cuban Assets Control Regulations* (Dec. 9, 2019), *available* here.

69 *Id.*

70 U.S. Dep't of Treasury, Press Release, *Settlements between the U.S. Department of the Treasury's Office of Foreign Assets Control and Allianz Global Risks U.S. Insurance Company, and, separately, Chubb Limited* (Dec. 9, 2019), *available* here.

71 U.S. Dep't of Treasury, Office of Foreign Assets Control, *Allianz Global Risks US Insurance Company Settles Potential Liability for Apparent Violations of the Cuban Assets Control Regulations* (Dec. 9, 2019), *available* here.

72 *Id.*

73 U.S. Dep't of the Treasury, Office of Foreign Assets Control, *State Street Bank and Trust Co. Receives a Finding of Violation Regarding Violations of the Iranian Transactions and Sanctions Regulations* (May 28, 2019), *available* here.

74 U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Apple, Inc. Settles Potential Civil Liability for Apparent Violations of the Foreign Narcotics Kingpin Sanctions Regulations*, 31 C.F.R. part 598 (Nov. 25, 2019), *available* here.

75 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.

76 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.

77 Paul, Weiss, *OFAC Enforcement Action against U.S. Aviation Company Shows the Importance of Ongoing Monitoring over the Course of a Contractual Relationship* (Dec. 9, 2019), *available* here.

78 U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Apollo Aviation Group, LLC ("Apollo," now d/b/a Carlyle Aviation Partners Ltd.) Settles Potential Civil Liability for Apparent Violations of Sudanese Sanctions Regulations, 31 C.F.R. part 538* (Nov. 7, 2019), *available* here.

79 *Id.*

80 U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Haverly Systems, Inc. Settles Potential Civil Liability for Apparent Violations of the Ukraine Related Sanctions Regulations* (Apr. 25, 2019), *available* here.

81 U.S. Dep't of the Treasury, Office of Foreign Assets Control, *OFAC Issues a Finding of Violation to Southern Cross Aviation, LLC, for a Violation of the Reporting, Procedures and Penalties Regulations* (Aug. 8, 2019), *available* here.

82 U.S. Dep't of the Treasury, Office of Foreign Assets Control, *ZAG IP, LCC Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations* (Feb. 21, 2019), *available* here.

83 *Id.*

84 U.S. Dep't of the Treasury, Office of Foreign Assets Control, *MID-SHIP Group LLC Settles Potential Civil Liability for Apparent Violations of the Weapons of Mass Destruction Proliferators Sanctions Regulations* (May 2, 2019), available here.

85 *Id.*

86 Paul, Weiss, *FinCEN Announces Launch of New Global Investigations Division Focused on Exercising Section 311 and Geographic Targeting Order Authorities* (Aug. 30, 2019), *available* here; U.S. Dep't of the Treasury, Press Release, *New FinCEN Division Focuses on Identifying Primary Foreign Money Laundering Threats,* (August 28, 2019), *available* here.

87 *Id.*

88 U.S. Dep't of the Treasury, Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies,* FIN-2019-G001 (May 9, 2019), *available* here.

89 *Id.*

90 U.S. Dep't of the Treasury, Financial Crimes Enforcement Network, *Advisory on Illicit Activity Involving Convertible Virtual Currency*, FIN-2019-A003 (May 9, 2019), *available* here.

91 *Id.* The advisory lists numerous other red flags including: transactions with CVC addresses linked to illicit activity; transactions being initiated from non-trusted, sanctioned, or suspicious jurisdictions; use of VPN services or Tor to access CVC accounts; multiple rapid trades between multiple virtual currencies (potentially in an attempt to "break the chain of custody" of the blockchains); provision of identification or account credentials shared by another account; multiple transactions or CVC conversions below due diligence, recordkeeping, or reporting thresholds; discrepancies between the customer's profile IP address and the IP address from which transactions are being initiated; large numbers of transactions by a customer significantly older than the average age of platform users (signaling a potential CVC mule or victim of financial exploitation); a customer's limited knowledge of CVCs despite account activity; lack of cooperation in requests for KYC documents or related inquires; large purchases of CVCs despite low available wealth or inconsistency with financial profile; a common wallet address being shared between accounts operated by different customers; significantly higher than usual deposits into accounts or CVC addresses with unknown sources, potentially followed by conversion to fiat currency; multiple changes to contact information for an account or customer; and indications in CVC message fields that transactions are being conducted to support illicit activity.

92 U.S. Dep't of the Treasury, Financial Crimes Enforcement Network, *Updated Advisory on Widespread Public Corruption in Venezuela*, FIN-2019-A002 (May 3, 2019), *available* here.

93 *Id.*

94 U.S. Dep't of the Treasury, Financial Crimes Enforcement Network, Press Release, *Updated FinCEN Advisory Warns Against Continued Corrupt Venezuelan Attempts to Steal, Hide, or Launder Money* (May 3, 2019), *available* here.

95 *Id.*

96 *Id.*

97 U.S. Dep't of the Treasury, Press Release, *FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws* (Apr. 18, 2019), *available* here.

98 *Id.*

[99] Paul, Weiss, *DOJ Announces Revised Export Control and Sanctions Enforcement Policy for Companies, Including Financial Institutions* (Dec. 19, 2019), *available* here.

[100] Paul, Weiss, *DOJ Updated Guidance for Evaluating Corporate Compliance Programs Focuses on Effectiveness* (May 6, 2019), *available* here.

[101] Paul, Weiss, *DOJ Announces Guidance for "Inability-to-Pay" Claims* (Oct. 10, 2019), *available* here.

[102] U.S. Dep't of Justice, Press Release, Standard Chartered Bank Admits to Illegally Processing Transactions in Violation of Iranian Sanctions and Agrees to Pay More Than $1 Billion (Apr. 9, 2019), available here.

[103] U.S. Dep't of Justice, Press Release, *UniCredit Bank AG Agrees to Plead Guilty for Illegally Processing Transactions in Violation of Iranian Sanctions* (Apr. 15, 2019), *available* here.

[104] *Id.*

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

[106] As described in the related indictment, *available* here.

[107] U.S. Dep't of Justice, Press Release, *Turkish Bank Charged in Manhattan Federal Court for Its Participation in a Multibillion-Dollar Iranian Sanctions Evasion Scheme* (Oct. 15, 2019), *available* here.

[108] U.S. Dep't of Justice, Press Release, *Four Chinese Nationals and Chinese Company Indicted for Conspiracy to Defraud the United States and Evade Sanctions* (July 23, 2019), *available* here.

[109] Paul, Weiss, *D.C. Circuit Upholds Decision Requiring Three Chinese Banks to Produce Documents Located in China to the U.S. Government* (Aug. 12, 2019), *available* here.

[110] U.S. Dep't of Justice, Press Release, *Export Company Executive Pleads Guilty to Violating U.S. Sanctions against Iran* (July 19, 2019), *available* here.

[111] U.S. Dep't of Justice, Press Release, *Two Indictments Unsealed Charging Iranian Citizen with Violating U.S. Export Laws and Sanctions against Iran* (June 4, 2019), *available* here.

[112] Danske Bank, *The investigations relating to Danske Bank's Estonian Branch, available* here.

[113] Bruun & Hjeje, *Report on the Non-Resident Portfolio at Danske Bank's Estonian Branch* (Sept. 19, 2018), *available* here; Frances Coppola, *The Tiny Bank At The Heart Of Europe's Largest Money Laundering Scandal,* FORBES (Sept. 26, 2018), *available* here.

[114] *Id.*

[115] *Id.*

[116] Drew Hinshaw, *Danske Bank Under Criminal Investigation by U.S. Justice Department,* THE WALL STREET JOURNAL (Oct. 4, 2018), *available* here; John O'Donnell, Tom Sims, Matt Schuffham, *Exclusive: U.S. digs deeper into Deutsche role in Danske money laundering scandal – sources,* REUTERS (Dec. 2, 2019), *available* here.

[117] Zacks Equity Research, *Deutsche Bank (DB) Under DOJ Probe Over Danske Bank Scandal,* NASDAQ (Dec. 2, 2019), *available* here.

[118] Frances Schwartzkopff, *Danske Investigated by SEC as Money Laundering Case Grows,* BLOOMBERG (Feb. 21, 2019), *available* here; Teis Jensen, Jacob Gronholt-Pedersen, Keith Weir, *U.S. investigators approach Deutsche Bank, BofA, JPM in Danske probe: Bloomberg,* REUTERS (Nov. 16, 2018), *available* here.

[119] The Board of Governors of the Federal Reserve System, *Order to Cease and Desist and Order of Assessment of a Civil Monetary Penalty Issued Upon Consent Pursuant to the Federal Deposit Insurance Act, as Amended* (Apr. 15, 2019), available here.

[120] U.S. Dept of the Treasury, Office of the Comptroller of the Currency, Press Release, *OCC Issues Consent Order of Prohibition and $50,000 Civil Money Penalty Against Former General Counsel of Rabobank N.A.* (July 23, 2019), *available* here.

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

[122] U.S. Dep't of the Treasury, Office of the Comptroller of the Currency, *Notice of Charges for Order of Prohibition and Notice of Assessment of a Civil Money Penalty* in *the Matter of Daniel Weiss,* (Mar. 25, 2019), *available* here.

[123] Written Agreement by and among Sumitomo Mitsui Banking Corporation, Sumitomo Mitsui Banking Corporation New York Branch, and Federal Reserve Bank of New York, (Apr. 23, 2019), *available* here.

[124] U.S. Sec. & Exch. Comm., *Order in the Matter of Quad/Graphics, Inc.* (September 26, 2019), *available* here.

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

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

[127] *U.S. Sec. & Exch. Comm.* v. *Alpine Sec. Corp.*, No. 1:17-cv-04179 (DLC), 2019 WL 4686716, at *8-*13 (S.D.N.Y. Sept. 26, 2019).

[128] Notice of Appeal, *U.S. Sec. & Exch. Comm.* v. *Alpine Sec. Corp.*, No. 1:17-cv-04179 (S.D.N.Y. Oct. 10, 2019).

[129] *See* BNP Paribas Securities Corp., *FINRA Letter of Acceptance, Waiver, and Consent No. 20160511052O1* (Oct. 23, 2019), *available* here.

[130] *Id.* at 4-7.

[131] *Id.*

[132] *Id.* at 7.

[133] *Id.* at 3.

[134] New York State, Press Release, *Governor Cuomo Announces First Round of Term 3 Administration Appointments* (Jan. 4 2019), *available* here; Paul, Weiss, *New York DFS Creates New "Powerhouse" Division Combining the Enforcement Division and Financial Frauds and Consumer Protection Division* (May 3, 2019), *available* here.

[135] *Id.*; N.Y. Dep't of Fin. Servs., Press Release, *Linda A. Lacewell Confirmed by Senate as New York Superintendent of Financial Services* (June 21, 2019), *available* here.

[136] *Id.*

[137] Paul, Weiss, *New York DFS Creates New "Powerhouse" Division Combining the Enforcement Division and Financial Frauds and Consumer Protection Division* (May 3, 2019), *available* here; N.Y. Dep't of Fin. Servs., Press Release, *Acting DFS Superintendent Lacewell Announces Appointment of Katherine Lemire as Executive Deputy Superintendent of Newly Created Consumer Protection & Enforcement Division* (Apr. 29, 2019), *available* here.

[138] N.Y. Dep't of Fin. Servs., *Statement by DFS Superintendent Maria T. Vullo Regarding CFPB's Troublesome Policy Shift Away from Consumer Protection* (Jan. 25, 2018), *available* here.

[139] Paul, Weiss, *New York DFS Creates New Cybersecurity Division* (May 29, 2019), *available* here; N.Y. Dep't of Fin. Servs., Press Release, *Acting Superintendent Linda A. Lacewell Names Justin Herring Executive Deputy Superintendent of Newly Created Cybersecurity Division* (May 22, 2019), *available* here.

[140] *See* 23 NYCRR 500.22.

[141] 84 Fed. Reg. 22961-22968, *Addition of Entities to the Entity List* (May 21, 2019).

[142] *See* BIS, *U.S. Department of Commerce Extends Huawei Temporary General License* (Nov. 18, 2019), *available* here.

[143] 84 Fed. Reg. 54002, *Addition of Certain Entities to the Entity List* (Oct. 9, 2019).

[144] *Id.*

[145] U.S. Sec. & Exch. Comm., *Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets* (Oct. 11, 2019), *available* here; *see also* Paul, Weiss, *Federal Agencies Issue Joint Statement on AML/CFT Obligations, and IRS Updates Guidance, for Digital Assets* (Oct. 15, 2019), *available* here.

[146] N.Y. Dep't of Fin. Servs., Press Release, *DFS Advances New York's Thriving Virtual Currency Market, Grants Virtual Currency and Money Transmitter Licenses to Tagomi Trading, LLC* (Mar. 27, 2019), *available* here.

[147] N.Y. Dep't of Fin. Servs., Press Release, *DFS Grants Virtual Currency License to Bitstamp USA, Inc.* (Apr. 9, 2019), *available* here.

[148] N.Y. Dep't of Fin. Servs., Press Release, *DFS Denies the Applications of Bittrex, Inc. for New York Virtual Currency and Money Transmitter Licenses* (Apr. 10, 2019), *available* here.

[149] *Id.*

[150] N.Y. Dep't of Fin. Servs., *Proposed Guidance Regarding Adoption or Listing of Virtual Currencies* (Dec. 11, 2019), *available* here.

[151] Fin. Action Task Force, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (June 21, 2019), *available* here.

[152] Paul, Weiss, *OFAC Breaks New Ground By Penalizing Non-U.S. Companies for Making U.S. Dollar Payments Involving a Sanctioned Country* (July 28, 2017), *available* here.

[153] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *OFAC Advisory to the Maritime Petroleum Shipping Community: Sanctions Risks Related to Petroleum Shipments involving Iran and Syria* (Mar. 25, 2019), *available* here.