January 23, 2018

Economic Sanctions and Anti-Money Laundering Developments: 2017 Year in Review

Table of Contents

Executive Summary

Economic sanctions and anti-money laundering ("AML") remain at the forefront of U.S. regulatory priorities. Indeed, in 2017, federal and state agencies imposed over $2.5 billion in penalties for sanctions/AML violations. And, despite its generally deregulatory agenda, the Trump administration has taken a rigorous approach in this area, particularly with respect to sanctions. At the state level, the New York Department of Financial Services ("DFS") continues to take aggressive action on both the regulatory and enforcement fronts. This memorandum surveys major developments and trends in 2017 and provides an outlook for the year ahead. We also provide some practical advice for U.S. and non-U.S. companies seeking to strengthen compliance and mitigate risk in this challenging environment.

Last year witnessed a number of dramatic changes to the economic sanctions landscape. President Trump has continued the recent trend of using economic sanctions as a powerful national security and foreign policy tool, and Treasury Secretary Mnuchin estimates that he spends "probably over 50 percent" of his time on national security and sanctions issues.[1] In addition, the U.S. Congress asserted its authority on sanctions by passing the Countering America's Adversaries Through Sanctions Act ("CAATSA"), which

President Trump signed into law on August 2, 2017.[2] The administration's and Congress's actions have reshaped President Obama's sanctions policies, significantly expanded the threat of secondary sanctions, and created new uncertainty and risks for U.S. and non-U.S. companies across industries.

The Trump administration has taken an aggressive stance towards North Korea, broadly threatening the imposition of secondary sanctions against non-U.S. persons conducting business involving North Korea. With respect to Iran, President Trump refused to certify that the suspension of sanctions under the Iran deal was in the U.S.'s national interest, and has threatened to reinstitute the sanctions relief granted pursuant to the deal. And, while the president this month extended waivers allowing the nuclear deal to remain intact, he threatened that this was for the "last time." The Trump administration also imposed a new and novel sanctions program in response to events in Venezuela, implemented new Global Magnitsky Act sanctions targeting human rights abuses and government corruption, and re-imposed certain Cuba-related restrictions that had been relaxed under the Obama administration. Finally, 2017 saw the revocation of the longstanding U.S. trade embargo against Sudan. On the enforcement side, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") has continued to push the boundaries of its jurisdiction and intensified its focus on non-financial entities, as demonstrated by its largest ever settlement with Chinese Zhongxing Telecommunications Equipment Corporation ("ZTE").

Enforcement of the Bank Secrecy Act/anti-money laundering ("BSA/AML") laws—and their state analogues—remains a high priority for federal prosecutors and regulatory agencies, as well as the DFS. Prosecutors and regulators remain willing to impose substantial penalties, as when the Department of Justice ("DOJ") and Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") reached a $586 million resolution with Western Union, and DFS issued major consent orders against non-U.S. banks. FinCEN also used its USA PATRIOT Act Section 311 authority to designate Bank of Dandong an institution of "primary money laundering concern" based on its alleged processing of North Korean transactions, thus cutting the institution off from the U.S. financial system. The Securities and Exchange Commission ("SEC") also took several enforcement actions against broker/dealers that demonstrate its continued focus on AML enforcement.

On the policy side, last year FinCEN issued significant guidance, and DFS's groundbreaking Part 504 regulation on sanctions/AML requirements went into effect. Congress has also focused on AML issues with the introduction of multiple bills designed to modernize and enhance the Bank Secrecy Act.[3] Finally, last year's revelations of the Paradise Papers and the new revelations related to the "Russian Laundromat" money laundering scheme—like the release of the Panama Papers the year before—suggest that non-governmental actors, including investigative journalists and hackers, will continue to be an important force in spurring regulatory inquiries and prompting in-house reviews.

Recent Developments and Trends in Economic Sanctions and Anti-Money Laundering

Treasury's Office of Foreign Assets Control

Last year saw sweeping changes to various sanctions programs administered by OFAC, particularly the North Korea, Iran, Russia/Ukraine, Cuba, Venezuela, and Sudan programs. These changes were effectuated through CAATSA, executive orders, regulatory amendments, and guidance documents. On the enforcement front, OFAC levied $120 million in civil penalties (including settlements) in 2017, up from $21 million in 2016, but down from the record-setting $1.2 billion levied in 2014. Notably, there was no blockbuster OFAC case against a major financial institution in 2017; instead, OFAC took eighteen enforcement actions against companies in a large range of industries, including the agency's largest ever enforcement action against a non-financial institution—an approximately $100 million settlement with Chinese telecommunications giant ZTE.

As detailed in our prior memorandum,[4] CAATSA makes significant changes to the Russia/Ukraine, North Korea, and Iran-related sanctions programs. Controversially, the law also restricts President Trump's ability to lift certain sanctions unilaterally, by including a congressional review mechanism that will allow Congress to potentially block the president from relaxing measures targeting Russia. While a number of the sanctions included in CAATSA are referred to as "mandatory," it remains to be seen how certain provisions will be enforced by the Trump administration. As an initial matter, many of these provisions require the president to sanction individuals or entities only after he determines that they have engaged in certain activities, thus allowing the president to theoretically refrain from enforcing these sanctions by withholding certain determinations. Additionally, in signing CAATSA, President Trump released two signing statements, in which he noted his "concerns to Congress about the many ways [the bill] improperly encroaches on Executive power, disadvantages American companies, and hurts the interests of our European allies," and his view that the "bill remains seriously flawed" because it "encroaches on the executive branch's authority to negotiate" and because "the Congress included a number of clearly unconstitutional provisions." President Trump stated that he would implement CAATSA's restrictions "in a manner consistent with the president's constitutional authority to conduct foreign relations."[5]

OFAC continues to be led by Director John Smith, who was made Acting Director under the Obama administration. President Trump's choice to be Treasury's Under Secretary for Terrorism and Financial Intelligence, Sigal Mandelker, was confirmed in June 2017 and oversees both OFAC and FinCEN.

Changes in OFAC Sanctions Programs

North Korea. Primarily in response to North Korea's ballistic missile testing and nuclear proliferation activities, a number of new North Korean sanctions measures were imposed in 2017. The sanctions program now prohibits virtually all dealings with North Korea that involve a U.S. nexus, and includes secondary sanctions authorities that threaten sanctions against non-U.S. entities engaged in North Korea-

related trade that lacks a U.S. nexus. Due to the mounting tensions with North Korea, these sanctions continue to be a high priority for both Congress and the Trump administration.

CAATSA significantly expanded the scope of North Korea-related sanctions, including both the mandatory and discretionary sanctions that were put in place by the 2016 North Korea Sanctions Policy Enhancement Act ("NKSPEA"). And, on September 20, 2017, President Trump signed into law E.O. 13810,[6] which broadly expanded the authorization of secondary sanctions first enacted in CAATSA.[7] The secondary sanctions authorities now in place authorize the Secretary of the Treasury to sanction any non-U.S. entity determined to be engaged in prohibited conduct, which includes, among other things, knowingly conducting or facilitating any significant transaction in connection with trade with North Korea.[8] For example, E.O. 13810 authorizes sanctions against non-U.S. financial institutions that knowingly conduct or facilitate any significant transaction on behalf of a North Korean Specially Designated National ("SDN") or in connection with trade with North Korea; available sanctions include being prohibited from opening correspondent or payable-through accounts in the United States or strict conditions on the maintenance of such accounts.[9] And such sanctions measures targeting non-U.S. financial institutions could be increased further if legislation currently pending in Congress—the Otto Warmbier Banking Restrictions Involving North Korea ("BRINK")—becomes law.[10] The Trump administration has consistently expressed its intention to aggressively enforce North Korea related sanctions. Indeed, North Korea-related designations increased significantly in 2017, and included actions targeting non-North Korean persons and illicit networks operated through front companies, including companies based in China and Russia.[11]

The sophistication of the North Korean regime in using front companies for its illicit networks poses unique compliance challenges. For financial institutions in particular, undertaking more rigorous due diligence is an increasingly paramount concern. Among other things, the Trump administration has emphasized the need for Chinese banks to bolster their efforts at identifying and shutting down North Korea-related activity.[12] Marshall Billingslea, Treasury's Assistant Secretary for Terrorist Financing, warned in testimony before Congress that "[f]inancial institutions in China, or elsewhere, that continue to process transactions on behalf of North Korea should take heed. [The U.S.] will continue to target North Korea's illicit activity, regardless of location."[13]

Iran. 2017 brought a sea change in the U.S. approach toward sanctions targeting Iran. While the Joint Comprehensive Plan of Action ("JCPOA") remains in place, the Trump administration has taken an increasingly aggressive stance toward Iran sanctions policy, both by casting significant uncertainty on the viability of the JCPOA and by implementing multiple rounds of non-nuclear sanctions designations targeting Iran.

For example, as we have described in a previous memorandum, in October 2017, President Trump refused to certify that the suspension of sanctions under the JCPOA was "appropriate and proportionate" to measures taken by Iran with respect to terminating its illicit nuclear program.[14] Under the terms of the

Iran Nuclear Agreement Review Act ("INARA"), this failure to certify triggered a 60-day period during which Congress was authorized—but not required—to consider the expedited re-imposition, or "snapback," of the sanctions previously lifted by the Obama administration to fulfill the U.S.'s obligations under the JCPOA.

To date, Congress has not seriously considered snapback legislation, and the initial 60-day review period has already expired. However, even if Congress does not pass snapback legislation, the president retains unilateral authority to partially or entirely snap back sanctions in other ways. Indeed, when announcing his refusal to certify, President Trump stated that if Congress does not reimpose sanctions, he himself will act to "terminate the JCPOA." The president could achieve this outcome by simply declining to continue to waive the suspension of certain sanctions, as required by the JCPOA. Although President Trump extended the waivers in January 2018, he noted that it was for the "last time," and that he was doing so "only in order to secure our European allies' agreement to fix the terrible flaws of the [JCPOA]. This is a last chance. In the absence of such an agreement, the United States will not again waive sanctions . . . And if at any time I judge that such an agreement is not within reach, I will withdraw from the deal immediately."[15] The next waiver deadline is in May 2018. The president could also re-designate all or some of the Iranian persons whose sanctioned status was lifted pursuant to the JCPOA, or otherwise broadly re-impose previously lifted nuclear-related sanctions on new, "non-nuclear" grounds. He could also direct OFAC to rescind licenses for certain activities involving Iran (such as commercial aviation-related transactions) issued under the Obama administration.

In addition to the de-certification announcement regarding the JCPOA, the Trump administration has also increased sanctions pressure targeting Iran on the non-nuclear front. As OFAC Director John Smith testified before Congress in late November 2017: "Since this Administration took office, OFAC has issued eight tranches of sanctions, designating 78 targets in Iran, China, Germany, Lebanon, and Ukraine in connection with the IRGC [Islamic Revolutionary Guard Corps] and Iran's ballistic missile program, support for terrorism, human rights abuses, cyber-attacks, transnational criminal activity, and other destabilizing regional activities."[16] The Trump administration has also focused pressure on the IRGC: in October 2017, President Trump announced the Treasury Department's designation of the IRGC in its entirety as a terrorist organization, pursuant to Executive Order 13224,[17] as well as the statutory requirement imposed by CAATSA.[18] The IRGC designation was coupled with warnings from the Treasury Department to avoid dealing with the IRGC, with Director Smith recently testifying: "As we have urged the private sector to recognize that the IRGC permeates much of the Iranian economy, we have emphasized that those who transact with IRGC-controlled entities do so at their own risk."[19]

During this period of increased uncertainty, companies currently conducting Iran-related business—or contemplating new such business—may want to seriously consider the risk that the prior U.S. sanctions will snapback into place. And, even if the JCPOA remains in place, companies involved in Iran-related business should ensure they are conducting enhanced due diligence to avoid transactions with the IRGC

or other designated entities, as OFAC will likely aggressively pursue violations of the current non-nuclear sanctions regime.

Last year also saw increased activity involving state-level sanctions measures. For example, in May 2017, Texas Governor Greg Abbott signed two bills that expand divestiture and contracting sanctions involving Iran, the Terror State Divestiture Act[20] and the Terror State Contracting Act (the latter also added sanctions involving Sudan and Foreign Terrorist Organizations).[21]

Russia/Ukraine Sanctions. Following the election of President Trump, some predicted a rollback of U.S. sanctions targeting Russia. Instead, in August 2017, Congress (through CAATSA) strengthened and expanded sectoral sanctions targeting Russia, and threatened the imposition of new and expanded secondary sanctions. Given the significant changes in this area, we have provided an overview of the current state of Russia/Ukraine sanctions in a recent memorandum.[22]

CAATSA's amendments to the sectoral sanctions program have presented increased compliance challenges for U.S. entities providing financing or goods and services to designated Russian entities, as well as for non-U.S. entities engaging in transactions involving such activity and a U.S. nexus. For example, amended Directives 1 and 2 imposed stricter limitations on the provision of goods and services on credit from U.S. suppliers to designated Russian entities. In addition, effective January 29, 2018, amended Directive 4 will cover deepwater, Artic offshore, and shale projects *worldwide* in which a Sectoral Sanctions Identification ("SSI") entity subject to Directive 4 holds a 33% or greater ownership interest. The amendments to Directive 4 do not change the applicability of OFAC's 50 percent rule in the Directive 4 context (the 50% rule continues to apply when determining SSI ownership of entities, while the 33% rule applies to SSI ownership interest in projects). Nevertheless, the "33-percent rule" will pose additional compliance challenges for companies doing business with Russian entities in support of exploration or production for new deepwater, Arctic offshore, or shale projects worldwide.

CAATSA also includes a series of new and expanded secondary sanctions authorities that seek to discourage non-U.S. persons (including entities and individuals that are based outside of Russia) from knowingly engaging in certain Russia-related conduct, including certain transactions involving: Russian deepwater, artic offshore or shale oil projects; privatization of Russian state-owned assets; and Russia's intelligence and defense sectors, among others. While the conventional wisdom is that President Trump will likely not be energetic in implementing these provisions, pressure from Congress and/or developments in geopolitics or domestic politics may lead the Trump administration to take tougher measures towards Russia. As a result, non-U.S. companies should meaningfully consider the risk of secondary sanctions in evaluating their ongoing and future business dealings in Russia.

Cuba. On June 16, 2017, President Trump announced that "effective immediately, I am canceling the last administration's completely one-sided deal with Cuba."[23] That same day, the president issued a National Security Presidential Memorandum entitled "Strengthening the Policy of the United States Toward Cuba."

As part of this directive, the administration barred transactions connected with Cuban military, intelligence, and security agencies and personnel. In addition, the directive aimed to reduce financial support for Cuba's tourism sector by limiting the circumstances in which Americans can travel to Cuba and spend money in the country while visiting.[24] The Treasury, Commerce, and State Departments published new regulations (effective November 9, 2017) to implement the changes President Trump announced in his June memorandum.[25] In particular, the State Department published an updated list of entities subject to prohibitions on direct financial transactions.[26] Additionally, OFAC made conforming edits to its regulations to restrict transactions involving the entities on the updated State Department list.[27]

Despite these changes, most of the Obama administration's actions to ease Cuban sanctions and export controls remain intact. For example, the authorization for the processing of "U-turn" payments through the U.S. financial system and the ability of certain Cuban nationals to maintain U.S. bank accounts remain unchanged.[28]

Venezuela. In response to ongoing human rights abuses in Venezuela in connection with its crackdown on anti-government protestors, the Trump administration has significantly increased sanctions pressure targeting the Venezuelan government. In 2017, the Trump administration designated more than 40 Venezuelan parties for, among other reasons, "undermining democratic processes, engaging in media censorship, or otherwise supporting [Venezuelan President Nicolas] Maduro's dictatorial regime."[29] Most prominently, in July 2017, the Trump administration designated President Nicolas Maduro and officials linked to his regime.[30] Also designated in July were current and former officials of Venezuelan state-owned oil company Petroleos de Venezuela, S.A. ("PdVSA"), which has been repeatedly linked to Venezuelan government corruption.

In August 2017, President Trump issued a new Venezuela-related executive order that introduced novel and complex sanctions measures.[31] The new round of sanctions prohibit U.S. persons from dealing in bonds previously issued by the government of Venezuela and in new Venezuelan debt with a maturity of more than 30 days, or 90 days where PdVSA is the debtor.[32] And, in November 2017, following October elections that OFAC characterized as a "sham" and "neither free nor fair,"[33] OFAC designated an additional ten current and former government officials "associated with undermining electoral processes, media censorship, or corruption in government-administered food programs in Venezuela."[34]

OFAC has also targeted senior Venezuelan officials using its counter-narcotics authorities. In February 2017, OFAC designated Venezuelan Vice President Tareck Zaidan El Aissami Maddah for drug trafficking and also designated or identified as blocked the property of 13 companies involved in El Aissami's global narcotics network, including companies in Venezuela, the British Virgin Islands, Panama, the United Kingdom, and the United States. Given El Aissami's status as Vice President, OFAC issued guidance regarding business with the Government of Venezuela, stating that while the "designation of an official of the Government of Venezuela does not mean that the government itself is also blocked . . . U.S. persons

should be cautious in dealings with the government to ensure that they are not engaged in transactions or dealings, directly or indirectly, with an SDN."[35]

Sudan. In January 2017, the Obama administration announced the revocation of the bulk of the Sudanese Sanctions Regulations ("SSR"), subject to a six-month review period.[36] After briefly extending the review period (through October 2017),[37] President Trump finalized the revocation on October 12, 2017.[38] Accordingly, U.S. persons are no longer prohibited from engaging in transactions previously prohibited by the SSR. An OFAC license is still necessary, however, for certain exports and reexports of agricultural commodities, medicine, and medical devices to Sudan. In addition, the Department of Commerce still requires licenses to export or reexport commodities, software, and technology on the Commerce Control List ("CCL").[39] Finally, the revocation does not affect OFAC designations of any Sudanese persons pursuant to other authorities still in place.

Global Magnitsky Sanctions. On December 20, 2017, President Trump issued an executive order implementing the Global Magnitsky Human Rights Accountability Act, which authorized the imposition of sanctions against human rights abusers and those who facilitate government corruption.[40] OFAC simultaneously added 52 entities and individuals to the SDN list pursuant to the new executive order. These designations include individuals who have been connected to DOJ and SEC Foreign Corrupt Practices Act enforcement actions. The new sanctions regime is remarkably broad and allows for the designation of any person determined to be: (1) responsible for or complicit in serious human rights abuses; (2) a current or former government official (or a person acting for or on behalf of such an official) responsible for or complicit in, corruption or bribery; (3) a current or former government official (or a person acting for or on behalf of such an official) who is responsible for or complicit in the facilitation of the transfer of the proceeds of corruption; or (4) those who have attempted to engage in such activities or materially assisted, sponsored, or provided support for such individuals, entities, or activities. The executive order does not define key terms, such as "corruption." While the effect of the new executive order will depend in large part on its implementation, it has the potential to serve as a powerful new tool in combating foreign corruption and human rights violations.

OFAC Enforcement Actions

OFAC's 2017 enforcement actions highlight the agency's expanded jurisdictional reach as well as an increased focus on non-financial companies. OFAC also continued to make use of Findings of Violation, public enforcement actions that involve no assessment of a monetary penalty. We outline below some of the more significant enforcement actions of 2017.

Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd. ("ZTE"). On March 7, 2017, Chinese telecommunications company ZTE reached a global $1.192 billion resolution with OFAC, DOJ, and the Department of Commerce that included a guilty plea to criminal sanctions and export control violations. ZTE's approximately $100

million settlement with OFAC represents OFAC's largest settlement to date with a non-financial entity.[41] From 2010 to 2016, ZTE knowingly engaged in the systemic practice of utilizing third-party companies to obtain U.S.-origin goods, including controlled goods appearing on the CCL,[42] which it then supplied to Iran.

The total value of ZTE's transactions related to these 251 violations was approximately $39 million. The fact that the conduct at issue involved a "company-wide scheme" that was "developed and approved at the highest levels of management" contributed to the significant penalty. Furthermore, after learning of the U.S. regulatory investigations, ZTE deleted or attempted to delete references to Iran in internal documents and provided incomplete or altered information to its own forensic auditors. OFAC determined that these false submissions were designed to mislead U.S. regulators. This case is also notable for the significant cooperation across government agencies—it was the Commerce Department's addition of ZTE to its entity list that forced the company to cooperate with U.S. authorities in order to maintain its access to U.S. exports.

CSE Global Limited and CSE TransTel Pte. Ltd. As described in our prior memorandum,[43] on July 27, 2017, Singapore based CSE TransTel Pte. Ltd., and its Singaporean parent company CSE Global Limited (collectively, "TransTel"), reached an approximately $12 million settlement with OFAC. According to the settlement agreement, TransTel entered contracts to install telecommunications equipment for Iranian energy projects between August 2010 and November 2011. In furtherance of the contracts, TransTel used U.S. dollar accounts it maintained at a Singapore-based bank to make millions of dollars of payments to third party vendors—including Iranian companies—for goods and services connected to the contracts. Notably, TransTel had signed a letter of undertaking to the Singapore-based bank agreeing not to use its U.S. dollar account for Iran-related transactions. TransTel's failure to comply with this undertaking resulted in the processing of 104 Iran-related wire transfers totaling more than $11 million dollars through the U.S. financial system, causing several financial institutions to engage in the prohibited exportation of financial services from the United States to Iran.[44] This action appears to be the first time that OFAC penalized a non-U.S., non-financial company for violating the International Emergency Economic Powers Act ("IEEPA") by "causing" sanctions violations through the use of U.S. dollar payments involving a sanctioned country.[45]

American International Group ("AIG"). On June 26, 2017, AIG reached a settlement with OFAC for $148,698. OFAC alleged that between approximately November 20, 2008 and September 3, 2012, AIG participated in 555 transactions that totaled $396,530 in premiums and insurance claims related to the maritime shipments of goods and materials to or through Iran, Sudan, and/or a blocked person. OFAC also identified inadequacies in AIG's compliance program related to exclusion clauses in insurance contracts that implicated U.S. sanctions. According to OFAC, AIG's policies and insurance contracts "conferred economic benefit to sanctioned countries or persons and undermined the policy objectives of several U.S. economic sanctions programs."[46]

COSL Singapore Ltd ("COSL"). On August 24, 2017, Singapore oilfield services company COSL agreed to a $415,350 settlement with OFAC for 55 apparent violations of the Iranian Transactions and Sanctions Regulations.[47] COSL, a subsidiary of China Oilfield Service Limited, entered into agreements with third-party drilling companies to allow them to use COSL's oil rigs. Under these arrangements, COSL was responsible for procuring equipment and spare parts for oil rig operations. Between 2011 and 2013, COSL purchased at least 55 orders of supplies (worth $524,664) from U.S.-based vendors on behalf of, and that were specifically intended for, re-export to four COSL oil rigs operating in Iranian territorial waters.

B Whale Corporation. On February 3, 2017, OFAC issued a finding of violation to B Whale, a Taipei based shipping company, for violations of the Iranian Transactions and Sanctions Regulations that occurred when the company's vessel conducted a ship-to-ship oil transfer with an Iranian vessel on OFAC's SDN list.[48] Notably, OFAC's jurisdiction was based on the fact that B Whale had entered into bankruptcy proceedings in the United States at the time of the transfer and that the vessel itself was "subject to U.S. sanctions regulations because it was property under the jurisdiction of a U.S. bankruptcy court." As a result, the oil transferred to B Whale's vessel was considered an "importation" from Iran to the United States.

ExxonMobil Corp., ExxonMobil Development Company, and ExxonMobil Oil Corp. ("ExxonMobil"). On July 20, 2017, OFAC assessed a $2 million civil penalty against ExxonMobil Corp. and two of its U.S. subsidiaries for violating OFAC's Russia/Ukraine-related sanctions by executing eight legal documents with Russian oil company Rosneft OAO.[49] Importantly, the legal documents were countersigned by Rosneft's president, Igor Sechin, an SDN.[50] OFAC took the position that by signing legal documents with Sechin, the companies dealt in the services of a blocked person. Rosneft itself is not an SDN and is not subject to blocking sanctions. ExxonMobil is challenging the penalty in federal court, arguing that U.S. sanctions applied to Sechin only in his "personal" capacity, and not in his "professional" capacity as president of Rosneft.[51] OFAC maintains that there is no such "personal" versus "professional" distinction.[52]

Richemont North America, Inc., doing business as Cartier ("Cartier"). On September 26, 2017, Cartier agreed to a $334,800 settlement for four apparent violations of the Foreign Narcotics Kingpin Sanctions Regulations.[53] Cartier exported four shipments of jewelry to Shuen Wai Holding Limited ("Shuen Wai"), an SDN. This appears to be OFAC's first public enforcement action focused on retail sales. On four separate occasions, an individual purchased jewelry from Cartier boutiques and provided Shuen Wai's name and mailing address as the "ship-to" party. OFAC found that Cartier failed to exercise a minimal degree of caution when it failed to identify any sanctions-related issues with the transactions prior to shipping the goods, despite the fact that the information and documentation provided to Cartier contained the same name, address, and country location for Shuen Wai as it appears on the SDN List. This enforcement action highlights the risks for companies with retail operations that

engage in international transactions, specifically including businesses that ship their products directly to customers located outside of the U.S. In announcing the Cartier settlement, OFAC stated that it encourages the development, implementation, and maintenance of risk-based compliance programs and suggested that companies consider, *inter alia*, their "products and services, frequency and volume of international transactions and shipments, client base, and size and geographic location(s)."[54]

IPSA International Services, Inc. ("IPSA") and BD White Birch Investment LLC ("White Birch"). On August 10, 2017, IPSA, an Arizona-based due-diligence firm, agreed to a $259,200 settlement with OFAC. IPSA and its Canadian subsidiary hired subcontractors to perform due diligence on Iranian nationals in Iran as part of its work related to citizenship by investment programs. OFAC alleged that, as part of its contracts with the subcontractors, IPSA "reviewed, approved, and initiated the foreign subsidiaries' payments to providers of the Iranian-origin services" on 28 occasions.[55] IPSA also allegedly imported Iranian-origin services into the United States on 44 occasions.

On October 5, 2017, White Birch, based in Greenwich, Connecticut, reached a settlement agreement with OFAC for $372,465. According to OFAC, White Birch USA facilitated the sale and shipment of 543,952 metric tons of paper from Canada to Sudan worth $354,602.26 in April and December 2013. White Birch USA employees were actively involved in the exportation of the paper as well as the negotiations that preceded the shipments.[56]

These cases serve as a reminder of the facilitation risks associated with U.S. person involvement—including back office support—in transactions subject to U.S. sanctions. Companies with U.S. offices or U.S. person employees can violate U.S. sanctions by facilitating activity by their non-U.S. counterparts as to which U.S. persons are prohibited from engaging.

Dominica Maritime Registry, Inc. ("DMRI"). On November 28, 2017, OFAC issued a finding of violation to DMRI for violating the Iranian Transactions and Sanctions Regulations. The violation resulted from DMRI's July 4, 2015 execution of a binding Memorandum of Understanding with an Iranian SDN, which OFAC determined was a contingent contract and therefore property in which the SDN had an interest.[57] This case is an important reminder of OFAC's broad definition of "property" and "property interests" to include "services of any nature whatsoever, contracts of any nature whatsoever, and any other property, real, personal, or mixed, tangible or intangible, or interest or interests therein, present, future, or contingent."[58]

Treasury's Financial Crimes Enforcement Network

FinCEN saw a change in leadership in 2017, with Kenneth Blanco, a longtime DOJ prosecutor, taking over for veteran acting director Jamal El-Hindi. FinCEN issued $323 million in penalties in 2017 (compared to $20 million in 2016) and used its USA PATRIOT Act Section 311 authority to cut off a Chinese bank

from the U.S. financial system. The agency was also active in issuing guidance on North Korea, Venezuela, and the risks associated with real estate transactions.

FinCEN Policy and Guidance

North Korea Advisory. In coordination with OFAC's aggressive steps on North Korea sanctions, on November 2, 2017, FinCEN issued an advisory identifying a number of specific red flags that might be indicative of illicit North Korea-related financial activity.[59] The advisory explained that North Korea relies heavily on front companies and trade-based payments in order to access the U.S. financial system. It specifically highlighted China's Liaoning Province and Hong Kong as common areas of operation for North Korean front companies, and Liaoning-based correspondent accounts as a common feature of these transactions. The advisory suggested that financial institutions search for patterns across customers in which one company regularly making payments goes dormant at the same time that another company initiates the same pattern of activity. Other front company red flags included shared addresses, financial activity unrelated to a stated area of business, and the lack of an internet presence.

The advisory underscores the fact that the U.S. Government expects compliance departments to keep pace with increasingly sophisticated criminal strategies. The sophistication of North Korean financing may mean that a one-size-fits-all approach is particularly inapposite in this context, which may require more extensive and unique countermeasures on the part of financial institutions.[60]

Venezuela Advisory. On September 20, 2017, FinCEN issued an advisory regarding pervasive public corruption in Venezuela.[61] FinCEN's then-Acting Director explained that, "particularly now, during a period of turmoil in [Venezuela], financial institutions need to continue their vigilance to help identify and stop the flow of corrupt proceeds and guard against money laundering and other illicit financial activity."[62] The advisory alerted financial institutions to methods that senior Venezuelan officials may use to conceal the proceeds of corruption and move such funds through the U.S. financial system. The advisory includes a list of red flags to help financial institutions detect and report suspicious activity, including transactions related to Venezuelan government contracts that: (1) are directed to companies in an unrelated line of business or to personal accounts; or (2) are corroborated by documentation showing charges substantially higher than market rates or by overly simplified documentation. Another cited red flag is real estate purchases–especially in South Florida and Houston–involving government officials or their family members and associates that are not consistent with the individuals' official salaries.

Given the specifics in the advisory, financial institutions with Venezuelan partners or customers could be subject to additional scrutiny from regulators regarding their practices for onboarding customers, updating KYC, and monitoring transactions. Such institutions should ensure that their risk assessment, due diligence, and transaction monitoring processes account for corruption and money laundering-related risk linked to Venezuela transactions and that they file suspicious activity reports ("SARs") when warranted.

Geographic Targeting Orders ("GTOs") Expansion. In February 2017 and August 2017, FinCEN reissued Geographic Targeting Orders ("GTOs") (first issued in January 2016), which require U.S. title insurance companies to report beneficial information ownership on legal entities involved in certain high-end real estate purchases. The revised GTOs capture a broader range of transactions (including transactions involving wire transfers) and now include transactions conducted in all boroughs of New York City, certain counties in the Miami metropolitan area, five counties in California (including Los Angeles, San Francisco, and San Diego), the Texas county that includes San Antonio, and the City and County of Honolulu, Hawaii. In addition to expanding the scope of the GTOs, FinCEN also published an advisory to provide financial institutions and the real estate industry with information on the money laundering risks associated with real estate transactions, including those involving luxury property purchased through shell companies, particularly when conducted without traditional financing.[63] The advisory provides information on how to detect and report these transactions to FinCEN.

Final Rule on Customer Due Diligence and Beneficial Ownership. As discussed in a previous Paul, Weiss memorandum, FinCEN issued its final rule ("CDD Rule") on May 11, 2016.[64] The rule codifies new and existing customer due diligence ("CDD") requirements under the BSA for covered financial institutions, namely, banks, broker-dealers, mutual funds, and futures commission merchants and introducing brokers in commodities. The rule has two components. First, subject to exceptions, covered institutions are required to identify the beneficial owners of their legal entity customers—including corporations, limited liability companies, partnerships, and similar entities—that open new accounts. Specifically, covered institutions must identify and verify (1) one or more natural persons, if any, who directly or indirectly own 25 percent or more of a legal entity customer, and (2) a natural person who "controls" the entity. Second, the rule supplements the traditional "four pillars" of an effective AML program by adding as a fifth pillar what FinCEN describes as "preexisting" CDD expectations necessary to comply with suspicious activity reporting requirements. Pursuant to this fifth pillar, covered institutions are required to develop customer risk profiles and to conduct ongoing monitoring to identify suspicious activity and, on a risk basis, to maintain and update customer information (including beneficial ownership information).

Banks and other covered financial institutions are already in the process of implementing this rule, and compliance is required by May 11, 2018.

FinCEN Enforcement Actions

Western Union Financial Services, Inc. ("Western Union"). On January 19, 2017, Western Union, a global money services business ("MSB"), agreed to a forfeiture of $586 million to resolve AML and fraud investigations by DOJ, FinCEN, and the Federal Trade Commission ("FTC").[65] DOJ resolution included a deferred prosecution agreement ("DPA") in which Western Union admitted to failing to implement and maintain an effective AML program and aiding and abetting wire fraud. FinCEN assessed a $184 million civil money penalty against Western Union, which was deemed satisfied by the forfeiture.

FinCEN determined that, prior to 2012, Western Union willfully violated the BSA by failing to implement and maintain an effective, risk-based AML program and by failing to file timely SARs. Western Union also failed to conduct adequate due diligence (such as background checks and on-site reviews) on a number of its foreign agents and failed to conduct enhanced due diligence on certain Latin America-based agent locations. As a result of these violations, certain agent locations and outlets that Western Union suspected were involved in fraud and money laundering were able to continue to use Western Union's money transfer system to facilitate illicit activity. Additionally, in many cases, Western Union either failed to file SARs when warranted, or filed such SARs with delays of more than 90 days.

In addition to a penalty, Western Union also agreed to a number of remedial undertakings, including increased scrutiny and periodic reporting regarding agent SAR reporting and disclosure of corrective actions taken against agents.

Merchants Bank of California, N.A. ("Merchants"). On February 27, 2017, FinCEN announced a $7 million civil money penalty against Merchants for BSA/AML violations. FinCEN found that Merchants failed to (1) establish and implement an adequate AML program, (2) conduct required due diligence on its foreign correspondent accounts, and (3) detect and report suspicious activity. Notably, Merchants allegedly failed to effectively monitor and detect suspicious activity for transactions involving billions of dollars on behalf of MSBs and encouraged staff to process these transactions without question or face potential dismissal or retaliation. FinCEN also faulted the bank for failing to identify that several of its foreign correspondent customers were located in high-risk jurisdictions, noting that $192 million in wire transfers were processed through high-risk accounts during a three-month sample period.

Thomas E. Haider. On May 4, 2017, DOJ and FinCEN settled their long-running effort to impose a $1 million penalty against Thomas E. Haider—MoneyGram International, Inc.'s former chief compliance officer—for BSA/AML violations. The civil penalty proceedings against Mr. Haider commenced in December 2014, two years after MoneyGram, a global MSB, entered into a DPA with DOJ and agreed to forfeit $100 million. Pursuant to the settlement, Mr. Haider agreed to pay a $250 million penalty, as well as to a three-year prohibition barring him from performing a compliance function for any money transmitter. In addition, Mr. Haider admitted and accepted responsibility for (among other things): (1) failing to terminate specific MoneyGram outlets after being presented with information that strongly indicated that the outlets were complicit in consumer fraud schemes; and (2) failing to implement a policy for terminating outlets that posed a high risk of fraud.[66]

As discussed in a prior publication,[67] the *Haider* case exemplifies the increasing focus on individual liability in the AML arena. Federal and state regulators continue to emphasize the need to hold individuals, including executives and compliance officers, accountable for AML violations.

BTC-E a/k/a Canton Business Corporation and Alexander Vinnik. On July 26, 2017, in coordination with the U.S. Attorney's Office for the Northern District of California, FinCEN announced a

$110 million civil money penalty against BTC-e, an internet-based, non-U.S.-based money transmitter that exchanged fiat currency as well as convertible virtual currencies (including Bitcoin). FinCEN stated that BTC-E did business "substantially in part" in the United States by conducting "at least 21,000 bitcoin transactions worth over $296,000,000 and tens of thousands of transactions in other convertible virtual currencies" with U.S. customers and recipients and utilizing U.S. servers. FinCEN also assessed a $12 million penalty against Russian national Alexander Vinnik, one of the operators of BTC-e.

FinCEN found that BTC-e lacked basic AML controls and had facilitated transactions involving ransomware, computer hacking, identity theft, tax refund fraud schemes, public corruption, and drug trafficking. Among other things, FinCEN asserted that BTC-E failed to obtain required information from customers beyond a username, a password, and an e-mail address. Users had openly and explicitly discussed criminal activity on BTC-e's user chat, and BTC-e's customer service representatives offered advice on how to process and access money obtained from illegal drug sales on dark net markets like Silk Road, Hansa Market, and AlphaBay. FinCEN also found that BTC-e had processed transactions involving funds stolen between 2011 and 2014 from one of the world's largest bitcoin exchanges, Mt. Gox. Lastly, FinCEN found that BTC-e had failed to file a single SAR, and had also failed to register as an MSB with FinCEN as required by law.

Bank of Dandong (Section 311 Action). On June 29, 2017, FinCEN found that Chinese-based Bank of Dandong was a financial institution of "primary money laundering concern" under Section 311 of the USA PATRIOT Act, and initiated rulemaking to cut off the Bank of Dandong's correspondent banking relationships with the United States.[68] On November 2, 2017, FinCEN finalized this rulemaking by imposing a prohibition on U.S. financial institutions from opening or maintaining correspondent accounts for, or on behalf of, Bank of Dandong.[69]

The Bank of Dandong was allegedly involved in laundering money on behalf of North Korea and the Chinese trading firm Dandong Hongxiang Industrial Development ("DHID").[70] DHID and four of its employees were previously indicted by DOJ on charges of conspiring to use front companies to facilitate U.S. dollar transactions in violation of U.S. sanctions.[71]

The 311 action against Bank of Dandong can be viewed as a warning to larger Chinese financial institutions.[72] At a September 12, 2017 hearing before the House Foreign Affairs Committee, Assistant Secretary of the Treasury for Terrorist Financing Marshall S. Billingslea testified that it "was the Treasury Department's first action in over a decade that targeted a non-North Korean bank for facilitating North Korean financial activity . . . . Financial institutions in China, or elsewhere, that continue to process transactions on behalf of North Korea should take heed."[73]

Department of Justice

2017 marked leadership and policy announcements that may have a significant impact on future DOJ prosecutions. On the sanctions side, the most significant criminal corporate action of 2017 was the ZTE case described above. Apart from the Western Union matter described above and the Banamex USA matter described below, both involving MSBs, there were no significant DOJ enforcement actions involving AML violations. DOJ continued to focus on individual prosecutions in 2017, and sanctions and AML matters were no exception to this theme.

On June 5, 2017, President Trump announced his intent to nominate Brian A. Benczkowski to be the Assistant Attorney General of DOJ's Criminal Division, who oversees, among other sections, the Money Laundering and Asset Recovery Section (previously known as the Asset Forfeiture & Money Laundering Section). This section leads DOJ's AML enforcement efforts and has been involved in DOJ's most significant recent AML and sanctions enforcement actions against financial institutions. Mr. Benczkowski's nomination has not yet been confirmed by the Senate.

Review of DOJ Policies. Corporate enforcement and the policies governing such enforcement remain a priority for DOJ. In October 2017, Deputy Attorney General Rosenstein announced that his office would be conducting a review and incorporation into the U.S. Attorney's Manual, where appropriate, of informal DOJ guidance. Any changes will reflect several common themes, specifically: (1) DOJ's "resolve to hold individuals accountable for corporate wrongdoing"; (2) that "the government should not use criminal authority unfairly to extract civil payments"; (3) that "any changes will make the policy more clear and concise" and (4) that any changes will "reflect input form stakeholders inside and outside the Department of Justice."[74] Rosenstein also stated that "[c]orporate enforcement is an important focus" for DOJ and specifically referenced DOJ actions involving violations of AML and export control restrictions.[75] This review is significant because it is not yet known which DOJ enforcement policies will ultimately be included in the U.S. Attorney's Manual, or whether they will be substantially altered.

Banamex USA. On May 22, 2017, DOJ announced its first resolution of a BSA/AML matter under the Trump administration, an agreement concerning Citigroup Inc. ("Citigroup") and one of its subsidiaries, Banamex USA ("BUSA").[76] Pursuant to this resolution, BUSA entered into a non-prosecution agreement ("NPA") for a one-year period and agreed to forfeit $97.4 million. BUSA admitted that, from approximately 2007 to 2012, it willfully failed to maintain an effective AML program and file SARs relating to remittances it processed to Mexico in partnership with MSBs.[77] Compared to past DOJ BSA/AML resolutions with other financial institutions, this resolution is notable for the relatively smaller size of the penalty,[78] the use of an NPA (rather than a DPA or a guilty plea), and a global release for all conduct investigated by DOJ. DOJ gave BUSA and Citigroup credit, among other things, for devoting significant resources to remediating compliance violations, terminating participation in the high-risk business line at issue, and ultimately shuttering BUSA.

Sanctions Prosecution of Kassim Tajideen. On March 24, 2017, the U.S. Attorney's Office for the District of Columbia announced the unsealing of an 11-count indictment against Kassim Tajideen of Lebanon.[79] Tajideen and co-defendant Imad Hassoun were charged with, among other things, conspiracy to violate IEEPA and the Global Terrorism Sanctions Regulations ("GTSR"), conspiracy to commit money laundering, and conspiracy to defraud the U.S. Government.[80] Due to his support for Hizballah, OFAC added Tajideen to the SDN List in 2009, effectively prohibiting U.S. persons from engaging in commercial transactions with Tajideen. Tajideen allegedly engaged in a complex evasive scheme—including by restructuring his business operations, creating new trade names, and misrepresenting his ownership interest in certain entities—to continue to purchase goods from U.S. companies and to use the U.S. financial and freight transportation systems while concealing his involvement in those transactions.

Sanctions Prosecution of Kenneth Zong. In December 2016, the U.S. Attorney's Office for the District of Alaska charged Kenneth Zong and his co-conspirators with conspiracy to violate IEEPA and the ITSR, conspiracy to commit money laundering, and money laundering. Zong, a U.S. citizen, allegedly engaged in false and fictitious transactions in South Korea designed to unlawfully convert Iranian owned funds into 1 billion U.S. dollars in the span of six months.[81] According to the indictment, Zong and his co-conspirators used an intermediary trading scheme by which Zong's Korean shell company feigned selling construction supplies to a shell company in Iran. The Korean shell company then fictitiously purchased similar supplies from an Iranian-controlled shell company located in Dubai, which fictitiously shipped the supplies to a shell company in Iran. By fabricating bills of lading and invoices, Zong allegedly demonstrated to Korean banking regulators that Iranian funds held in restricted accounts in Korea could be released.[82] Zong allegedly transferred the Iranian funds to his Korean shell company account, and then transferred the funds to entities and individuals throughout the world, including in Alaska and other U.S. states.

Sanctions Prosecution of Hakan Atilla and Reza Zarrab. On January 3, 2018, Mehmet Hakan Atilla, a Turkish citizen and the former Deputy General Manager of Halkbank, was convicted by a jury in the Southern District of New York on five counts relating to a scheme to violate U.S. sanctions targeting Iran.[83] Atilla was convicted of a substantive count of bank fraud, as well as conspiracy to defraud the United States, to violate the IEEPA, to commit bank fraud, and to commit money laundering. He was found not guilty on a substantive count of money laundering.

The verdict came after an October 2017 guilty plea by Turkish-Iranian dual national Reza Zarrab relating to similar charges.[84] Zarrab agreed to cooperate against Atilla, testifying in detail at trial how Atilla, Zarrab, and others used deceptive measures to provide the Government of Iran with access to the U.S. and international financial system. Among other schemes, using Halkbank, they took steps to conceal Zarrab's supply of currency and gold to the Government of Iran, Iranian entities, and other SDNs. They also used a web of Turkish and other companies to make U.S. dollar payments in Iran-related transactions and used fraudulent documents to disguise prohibited transactions for Iran as transactions falling within

humanitarian exceptions to the sanctions regime, and thereby induced U.S. banks to unknowingly process transactions in violations of the IEEPA.

Zarrab's testimony implicated Turkish President Recep Tayyip Erdogan in the scheme, and DOJ pursued the case over the strenuous protest of the Turkish government. Following the verdict, Acting U.S. Attorney Joon Kim stated: "Foreign banks and bankers have a choice: you can choose willfully to help Iran and other sanctioned nations evade U.S. law, or you can choose to be part of the international banking community transacting in U.S. dollars. But you can't do both."[85]

Compliance Monitor Reports. As discussed in a prior Paul, Weiss memorandum,[86] on July 12, 2017, the U.S. Court of Appeals for the Second Circuit ruled that a compliance monitor's report, prepared pursuant to a 2012 DPA entered into between HSBC and DOJ and filed with the district court, could not be unsealed and made public by the district court. The Second Circuit rejected the district court's ruling that the report was a "judicial" document subject to public disclosure and held that the district court erred in invoking its supervisory authority over the DPA in the absence of a showing of impropriety. Judge Rosemary Pooler's concurring opinion expressed concern that the current use of DPAs allows prosecutors to "adjudicat[e] guilt and impos[e] sentences with no meaningful oversight from the courts," and she urged Congress to consider legislation on this topic.[87] The Second Circuit's decision significantly limits district courts' authority to review the substance of a DPA or to monitor its execution and implementation.[88]

Federal Banking Agencies

Sanctions/AML compliance continues to be an area of important focus by the federal banking agencies. For example, in its most recent Semiannual Risk Perspective, the Office of the Comptroller of the Currency ("OCC") noted that compliance risk remains "elevated" as banks continue to manage money laundering risks.[89] The OCC added that "bank offerings using new or evolving delivery channels may increase customer convenience and access to financial products and services, but banks need to maintain a focus on refining or updating BSA compliance programs to address any vulnerabilities created by these new offerings, which criminals can exploit."[90]

The direction of federal banking agency enforcement efforts will be influenced by President Trump's recent nominations and appointments. President Trump has nominated Jerome Powell to replace Janet Yellen as Chairman of the Federal Reserve Board of Governors,[91] and his appointee, Randall Quarles, has been confirmed as the Federal Reserve Board's Vice Chair for Supervision.[92] President Trump's nominee Joseph Otting, former CEO of OneWest Bank, has been confirmed as head of the OCC,[93] and the president has announced that he intends to nominate Jelena McWilliams, currently the chief legal officer for Fifth Third, to be chairman of the FDIC.[94] While it is not clear how these appointees view enforcement in the sanctions/AML space, there appears to be considerable institutional momentum and staff commitment at each banking agency to maintain strong enforcement.[95]

Federal Banking Agency Enforcement Actions

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

Deutsche Bank. On May 26, 2017, the Federal Reserve levied a $41 million civil monetary penalty against Deutsche Bank AG and its U.S. operations ("Deutsche Bank") for BSA/AML deficiencies. In the consent order, the Federal Reserve stated that its recent examination had identified "significant deficiencies" that resulted in Deutsche Bank's failure to maintain an effective AML program, and that these deficiencies had "prevented [Deutsche Bank] from properly assessing BSA/AML risk for billions of dollars in potentially suspicious transactions processed between 2011 and 2015 for certain [Deutsche Bank] affiliates in Europe for which the affiliates failed to provide sufficiently accurate and complete information."[96] The conduct at issue appears to relate to the so-called Russian "mirror trading scheme" centered in Deutsche Bank's Moscow branch, which was the subject of a DFS penalty described below.[97] In addition to the penalty, the Federal Reserve required Deutsche Bank to engage a consultant to review its BSA/AML compliance and to conduct a transaction review of its foreign correspondent bank activity.[98]

Citibank, N.A. On Jan. 4, 2018, the OCC issued a consent order against Citibank imposing a $70 million penalty based on the bank's alleged failure to make the BSA/AML compliance reforms required in an OCC consent order from 2012.[99]

Mega Bank. On January 17, 2018, the Federal Reserve and Illinois Department of Financial and Professional Regulation announced a $29 million penalty against Taiwan's Mega International Commercial Bank and certain of its U.S. operations ("Mega Bank") for BSA/AML violations, as well as violations of Illinois law.[100] The consent order includes a number of requirements, including the submission of plans to create a consolidated framework for BSA/AML and OFAC compliance across the bank's U.S. operations (including the bank's New York, Chicago, and Silicon Valley branches) and to enhance oversight by U.S. senior management and the bank's board of directors. Mega Bank and its New York branch are also required to engage an independent third party to conduct a lookback review of U.S. dollar clearing transaction activity for a six-month period to determine whether suspicious activity involving high risk customers or transactions was properly identified and reported. While the consent order does not detail specific findings, Mega Bank paid a $180 million penalty to the NY DFS in August 2016 based on a number of alleged AML deficiencies, including the failure to identify and report suspicious transactions with its Panama branches.

Resolutions Without Penalties. As in prior years, the federal banking agencies also issued BSA/AML-related consent orders or written agreements that lacked financial penalties. For example, BB&T Bank entered into a consent order with the Federal Reserve, which noted "significant deficiencies" in the bank's firm-wide compliance program with respect to BSA/AML requirements.[101] Similarly, the OCC entered into a written agreement with UBS AG New York for BSA/AML deficiencies.[102] Both

resolutions required the respective financial institutions to develop and implement plans for strengthening BSA/AML compliance; neither required a transactional lookback.

Securities and Exchange Commission

President Trump's choice for SEC chairman, Jay Clayton, was sworn in on May 4, 2017. Under Chairman Clayton's leadership, the SEC took several BSA/AML enforcement actions against broker-dealers last year.

Merrill Lynch, Pierce, Fenner & Smith Incorporated ("Merrill Lynch"). On December 21, 2017, the SEC announced a $13 million settlement with Merrill Lynch for failing, during the 2011-2015 period, to file SARs on certain suspicious movements of funds through its customers' accounts.[103] The SEC alleged that this failure resulted from Merrill Lynch's lack of AML policies and procedures that were reasonably designed to account for the additional risk associated with the money transfer services it offered to customers with brokerage accounts, including ATM cash deposits, wires, journal-entry transfers, check writing, ATM withdrawals, cash advances, and ACH transfers.[104] As the SEC noted, these services presented money laundering risks that included "structuring currency deposits and withdrawals to avoid cash transaction reporting obligations and other risks associated with cash-intensive activities, such as laundering the proceeds of illegal activity."

In addition, the SEC alleged that from 2006 to May 2015, Merrill Lynch did not apply its automated transaction monitoring system to about 4.2 million retirement accounts, 228,000 retail brokerage accounts, and 421,000 security-based loan accounts. Although the company applied other AML detection systems to these accounts, the SEC believed they were not sufficient for the volume of transactions occurring in certain accounts. The SEC also identified other alleged deficiencies, including with respect to scoring and investigating hits produced by the transaction monitoring system.

Wells Fargo Advisors, LLC ("Wells Fargo"). On November 13, 2017, the SEC and Wells Fargo reached a settlement of $3.5 million for failure to file or timely file at least fifty SARs from approximately March 2012 through June 2013.[105] According to the SEC, the majority of these failures involved the failure to file SARs on ongoing suspicious activity that continued after the initial filing of a SAR on related suspicious activity. The SEC found that, in 2012, new managers with responsibility over the Surveillance and Investigations group, which was responsible for investigating suspicious activity, created "confusion" by communicating to the group: that they were filing "too many SARs"; that continuing activity SARs were not a regulatory requirement; that they were to take steps to eliminate further continuing activity reviews; and that filing a SAR required "proof" of illegal activity. Among other things, the new AML management also instructed the investigators not to document any disagreements with management's decisions not to file SARs in the company's internal case management system, but instead to use the system to record only facts and management's final decision. Following an employee complaint and an

internal investigation, the company retained a compliance firm to re-review cases, which ultimately led to new SAR filings.[106]

Alpine Securities Corporation ("Alpine"). In a federal lawsuit filed on June 5, 2017, the SEC charged that Alpine, a Utah-based broker-dealer, systematically failed to file SARs when required, despite having flagged transactions as suspicious.[107] According to the SEC's complaint, since 2001, Alpine has cleared thousands of deposits of microcap securities, most of them involving Scottsdale Capital Advisors as the introducing broker (which is owned by Alpine's owner), and many of which were used as "part of various stock manipulation and other schemes." The SEC also charged that the SARs that Alpine did file omitted material indications of suspicious activity of which Alpine was aware in nearly 2,000 instances. The complaint notes that regulators have repeatedly cited Alpine for SAR failures. The SEC enforcement action remains pending in federal court.

Financial Industry Regulatory Authority

In its 2018 Regulatory and Examination Priorities Letter,[108] FINRA stated that it intends to continue to address shortcomings in broker-dealers' AML programs, including "concerns related to, for example, the adequacy of (1) firms' policies and procedures to detect and report suspicious transactions; (2) resources for AML monitoring; and (3) independent testing required under FINRA Rule 3310(c)." FINRA also highlighted that firms "should be attentive to the potential use of their foreign affiliates to conduct high-risk transactions through accounts at member firms, including in microcap and dual-currency securities. FINRA has observed situations where firms do not monitor, or may monitor less closely, accounts opened for an affiliate." Finally, firms should also confirm that their "AML surveillance programs cover accounts used in connection with securities-backed lines of credit (SBLOCs) and aggregate activity across accounts when they use multiple accounts to receive and disburse funds in connection with an SBLOC."

Merrill Lynch, Pierce, Fenner & Smith Incorporated ("Merrill Lynch"). On December 21, 2017, Merrill Lynch entered into a $13 million settlement with FINRA for "numerous deficiencies" in its AML controls applicable to retail brokerage accounts.[109] FINRA essentially penalized the company for the same failures noted in the SEC enforcement action described above, but the FINRA settlement includes greater detail on suspicious account activity at Merrill Lynch's branches in McAllen, San Diego, and New York. These accounts were used to transfer funds to and from high risk jurisdictions such as Russia, Zambia, Mexico, China, Lebanon, Panama, Venezuela, the Philippines, Syria, Egypt, Peru, Haiti, and Ecuador. One of the recurring issues was Merrill Lynch's failure to link related accounts for purposes of transaction monitoring.

New York Department of Financial Services

DFS continued its aggressive regulatory and enforcement activity in the sanctions/AML arena in 2017, issuing major consent orders against Deutsche Bank and Habib Bank and putting in place its new Part

504 regulation, which prescribes requirements for DFS-licensed institutions' transaction monitoring and sanctions screening programs and mandates annual senior-level certifications.

Part 504 Regulation. As detailed in our prior memorandum, on June 30, 2016, DFS adopted Part 504, a wide-reaching set of requirements for the AML and sanctions compliance programs of DFS-regulated banks and branches.[110] The regulation became effective January 1, 2017, and affected institutions have expended considerable resources and time over the past year in formulating their approaches to Part 504 compliance; conducting gap analyses; designing and, where possible, implementing remediation; and constructing their frameworks for annual senior-level certification, with the first certification due on April 15, 2018.

Institutions have been wrangling with a number of questions under the regulation, including how to certify compliance despite the presence of open compliance issues. On October 26, 2017, DFS published long-awaited guidance on Part 504.[111] However, the guidance consisted of only five "frequently asked questions"; by contrast, DFS issued twenty-six FAQs on its Part 500 regulation concerning cybersecurity.[112] The Part 504 FAQs still leave affected institutions with uncertainty on important issues.

Deutsche Bank. On January 30, 2017, DFS issued a consent order against Deutsche Bank AG and its New York branch ("Deutsche Bank"), assessing a $425 million penalty and installing an independent monitor for a two-year term to review the bank's AML programs on a global basis, insofar as they affect the New York offices.[113] As noted above, the Federal Reserve also assessed a $41 million penalty against Deutsche Bank for BSA/AML deficiencies.[114] The DFS order involved an alleged "Russian mirror-trading scheme," in which traders based mainly in the bank's Moscow branch purportedly arranged matching securities trades, which were executed closely in time and between closely related entities and that, according to DFS, "had no economic purpose other than disguising what the client was doing."[115] The transactions are alleged to have also involved the bank's London and New York offices, with more than $10 billion allegedly flowing through the latter. According to DFS, the bank missed several "clear" opportunities to identify this scheme from 2011 until early 2015. Notably, the consent order largely focuses on asserted AML deficiencies at the bank's Moscow branch; there is little focus on actions or inactions at the bank's New York offices. The deficiencies alleged include: flaws in KYC policies and procedures at the Moscow branch, including with respect to onboarding new customers and periodically reviewing them; the lack of a "central repository" at the bank for KYC information; and failure to accurately rate AML country and client risks.

DFS's consent order appears to go further than previous actions in penalizing a bank for alleged AML failures that were predominantly centered outside of New York. The order suggests a DFS expectation that non-U.S. banks impose U.S.-style, "[c]entralized" AML frameworks across their global operations. The U.K. Financial Conduct Authority concurrently issued a consent order against the bank imposing a penalty of £163 million.

Habib Bank. As discussed in a previous memorandum, on September 7, 2017, DFS issued a consent order against Habib Bank Limited ("Habib") and its New York branch that imposed a $225 million penalty for alleged persistent BSA/AML and sanctions compliance failures.[116] In the consent order, Habib stipulated to: failing to maintain an effective AML and OFAC compliance program; failing to maintain true and accurate books and records; operating in an unsafe and unsound manner; and violating provisions of a prior written agreement and consent order. The consent order came approximately 10 days after DFS had issued a rare "Notice of Hearing and Statement of Charges," which sought to impose a nearly $630 million civil penalty against Habib for a laundry list of violations. Habib had indicated that it planned to contest any DFS penalty and surrender its DFS banking license, thus eliminating its only U.S. branch.[117]

Ultimately, Habib—the largest bank in Pakistan—will surrender its license to operate its New York Branch upon the fulfillment of conditions outlined in a separate Surrender Order issued by DFS.[118] And, Habib is required to complete an expanded transactional lookback conducted by an independent consultant, which was already underway under the terms of a prior order.[119]

This enforcement action illustrates that a DFS-regulated institution's failure to show steady progress in remedying identified concerns can have significant and franchise-threatening consequences. The action also emphasizes that DFS will pursue enforcement against a bank even if it voluntarily decides to give up its license and exit the New York market. When issuing the consent order, Superintendent Vullo stated that DFS will not allow a bank to "sneak out of the United States without holding it accountable for putting the integrity of the financial services industry and the safety of our nation at risk."[120]

NongHyup Bank. On December 21, 2017, DFS issued a consent order against a major Korean bank, NongHyup Bank, and its New York branch, assessing an $11 million penalty for the Bank's alleged failure to maintain an adequate AML program. The order details a number of AML deficiencies identified at the Bank's New York branch over the course of three examinations. The order focuses in particular on deficiencies in the branch's transaction monitoring system, including failure to establish adequate rules, failure to review alerts for potentially suspicious activity in a timely manner, and manipulation of rule thresholds to reduce the branch's workload. The order also describes the branch's failures in conducting due diligence on the Bank's Head Office, including the failure to monitor the Bank's Head Office account in terms of expected account activity and the purpose of the account, the failure to screen the account against lists of prohibited persons and entities, and the failure to determine whether members of Head Office executive management were politically exposed persons (PEPs). The order also cites deficiencies in compliance personnel expertise. DFS stated that while a bank's examination ratings should improve over time, "the opposite occurred at NongHyup—each successive examination uncovered an increasing number of deficiencies in connection with the New York Branch."[121]

This consent order is particularly notable for the relatively modest size of the penalty imposed—$11 million—compared to other AML/sanctions penalties DFS levied during Superintendent Vullo's tenure.

The order also does not impose a monitor or independent consultant and does not require that NongHyup perform a transactional lookback. Finally, DFS's order expressly "recognizes and credits the manner in which [the Bank] has cooperated with the Department in its investigation of this matter," and the remedies imposed reflect the DFS's "positive consideration" of that cooperation.[122]

Western Union. On January 4, 2018, DFS issued a consent order against Western Union that imposed a $60 million penalty for allegedly failing to maintain an effective AML program and failing to exercise reasonable supervision over its agents.[123] This order follows a resolution from January 2017, discussed earlier in this memorandum, among Western Union and DOJ, FinCEN, and the FTC. In the order, DFS alleged that several Western Union "executives and managers" willfully ignored suspicious transactions undertaken by Western Union agents, or intervened on their behalf when faced with potential disciplinary action, and that none of this misconduct was timely disclosed to DFS.[124] In a press release, Superintendent Vullo stated: "Western Union executives put profits ahead of the company's responsibilities to detect and prevent money laundering and fraud, by choosing to maintain relationships with and failing to discipline obviously suspect, but highly profitable, agents."[125]

In addition to the $60 million penalty, DFS required Western Union to submit a written plan designed to ensure the adequacy of its AML programs.[126] Notably, this plan would, among other things, require all Western Union agents "around the world, regardless of their location," to adhere to U.S. regulatory and AML standards, "unless in direct conflict with local law."[127] It would also require Western Union to file SARs for any suspicious activity in customer-to-customer transfers of over $2,000.[128] The order does not, however, impose a monitor or independent consultant or require a lookback.

Licensing Conversion. In November 2017, media outlets reported on the Bank of Tokyo Mitsubishi UFJ's (BTMU's) decision to convert its U.S. branches and agencies—which were licensed and supervised by different state banking regulators in New York, California, Illinois, and Texas—to federal licenses granted by the OCC. BTMU sought to obtain a unified supervisory framework for its operations in the United States, and its California-based subsidiary was already OCC-supervised. Following an order issued by DFS in the aftermath of BTMU NY's license conversion, the bank filed suit against DFS based on federal preemption. The litigation is ongoing.

Additional Developments

The Paradise Papers. As something of a sequel to the 2016 release of the "Panama Papers" purloined from the Panamanian law firm Mossack Fonseca, in November 2017 newspapers began running stories concerning the so-called "Paradise Papers."[129] The Paradise Papers consist of a trove of approximately 13.4 million documents stolen from the files of Bermuda-based law firm Appleby, as well as the Singapore-based trust and corporate services company Asiaciti. The stolen documents have already been connected to more than 100 prominent politicians and political leaders—including Britain's Queen Elizabeth and Prince Charles, Colombia's Juan Manuel Santos, and Secretary of Commerce Wilbur Ross.

The Paradise Papers have also shed light on the tax planning structures of more than 31,000 individuals and companies. In significant contrast to the public outcry following publication of the Panama Papers, the release of the Paradise Papers has generated a more muted reaction, perhaps because the conduct described in the documents is, at least in part, lawful tax planning. Nevertheless, as of this writing, a number of countries, including Canada and Australia, have initiated investigations based on the documents.

Regardless of any illicit activity, the Paradise Papers present a potential opportunity for financial institutions and other companies to gain additional intelligence on the beneficial ownership structures of, and relationships between, new or existing clients. The International Consortium of Investigative Journalists maintains a database made up of structured datasets detailing networks and interrelationships between companies and people (officers, owners, directors) and providing jurisdiction and location information. The database comprises information from four major leaks—the Offshore Leaks, the Bahamas Leaks, the Panama Papers, and the Paradise Papers—and includes information on more than 680,000 offshore companies, funds, and trusts, including more than 600,000 names of people and entities behind them. Financial institutions may want to consider whether this information could be appropriately utilized to improve KYC and suspicious activity monitoring efforts.

The Russian Laundromat. In 2014, the Organized Crime and Corruption Reporting Project ("OCCPRP") unveiled the "Russian Laundromat," an alleged criminal scheme designed to move vast sums of illegal funds out of Russia. In March 2017, the OCCPRP revealed, for the first time, details regarding how the scheme was allegedly structured.[130]

Between 2011 and 2014, at least $20.8 billion was allegedly laundered through 19 Russian banks. The funds allegedly went to 5,140 companies with accounts at 732 banks, including global financial institutions, in 96 countries. Typically, one offshore shell company (the "loaning company") would pretend to loan a large sum of money to another overseas shell company (the "receiving company"). Most of the loaning and receiving companies were located in the United Kingdom. Russian businesses, fronted by Moldovans, would then guarantee these "loans." The receiving companies would fail to return the "money." Moldovan judges (complicit in the alleged scheme) would then authenticate the "debt," allowing the Russian companies to transfer real money to Moldindconbank in Moldova. From there it was transferred to a Latvian bank, Trasta Komercbanka. Moldovan prosecutors have reportedly launched criminal cases against 14 judges as well as 10 senior bank managers, 10 senior central bank officials, and four bailiffs in relation to the scheme.

The OCCPRP website lists the thousands of shell companies allegedly involved in the scheme, as well as the volumes of dollars allegedly processed through major global financial institutions. Financial institutions may want to consider whether and how to use this information to evaluate their own transactions.

AML/CFT Modernization Legislative Proposals. Both the Senate and House of Representatives are discussing measures to modernize the U.S. AML/counter-financing of terrorism ("CFT") regime.

There appears to be growing support across the banking industry, law enforcement, and legislators in favor of addressing the use of shell companies with anonymous ownership. One draft bill under consideration, the Counter Terrorism and Illicit Finance Act, would be sponsored by Congressmen Steve Pearce (R-NM) and Blaine Luetkemeyer (R-MO) and would require new and existing corporations to report beneficial ownership information to FinCEN.[131] Such a measure could remove some burden from financial institutions in complying with FinCEN's 2016 regulation on customer due diligence and beneficial ownership. The draft House bill also includes provisions requiring the Secretary of the Treasury to: facilitate information sharing between government and financial institutions; encourage the use of technological innovation in AML programs; and establish and publicize priorities for AML/CFT laws. Another House bill, the Anti-Money Laundering and Counter-Terrorism Financing Modernization Act introduced by Congressmen Ed Royce (R-CA) and Vicente Gonzalez (D-TX), would similarly promote greater information sharing and require the Treasury Department to explore the potential role of technology in money laundering and terrorist financing detection efforts.[132]

Another theme in AML/CFT regime modernization discussions is addressing the use of cryptocurrencies for illicit activities. A bill considered in November 2017 by the Senate Committee on the Judiciary—the Combating Money Laundering, Terrorist Financing, and Counterfeiting Act—is sponsored by Senator Chuck Grassley (R-IA) with bipartisan co-sponsorship and would amend the definition of "financial institutions" to which U.S. AML laws apply to include issuers of digital currencies and digital currency exchangers and tumblers. The Senate bill would also make it a crime to lie to a financial institution about the beneficial ownership or control of an account or assets in an account at the financial institution.[133]

On January 9, 2018, the Senate Committee on Banking, Housing, and Urban Affairs held a hearing on modernizing U.S. AML/CFT laws. The witnesses from industry and AML/CFT groups testified that amendments to the current regime should require entities incorporated in the United States to report their ownership information and should address the use of cryptocurrencies. There was also general agreement that the incorporation of innovative technologies and artificial intelligence could improve the efficiency of financial institutions' transaction monitoring. One area of disagreement in the hearing was whether monetary thresholds that trigger currency transaction reports should be increased, as contemplated in the aforementioned House proposals.

Suggestions for Strengthening Sanctions/AML Compliance

In light of the developments described above, senior management, general counsel, and compliance officers should consider strengthening their institutions' sanctions/AML posture along the following lines:

1. **Take proactive steps to analyze data and identify risky parties**. As illicit actors develop increasingly sophisticated schemes to evade sanctions and AML controls, regulators are expecting companies—and financial institutions in particular—to develop more sophisticated compliance solutions. While it is not possible (or reasonable, in a risk-based compliance environment) to detect every illicit transaction, there are steps that companies can take to stay ahead of the curve. These steps include leveraging public information and internal reporting to identify entities and individuals with potential ties to sanctioned parties and sanctioned countries, searching for any such identified entities or individuals within customer accounts/transactions, and conducting "micro" lookbacks to identify parties associated with problematic transactions. Such efforts should make use of the guidance issued by FinCEN on detecting North Korean front activity and corrupt activity related to Venezuela, and should also utilize sources as diverse as C4ADS (a nonprofit that maps elicit North Korean networks), U.N. sanctions reports, and data from the Paradise Papers, the Russian Laundromat, and similar phenomena.

2. **Bolster customer due diligence, customer screening, and transaction monitoring**. A main theme of enforcement continues to be the failure to identify the prohibited status of certain customers, often despite the fact that such information was within an institution's possession or readily accessible. The reasons for these problems include weak procedures, inadequate information sharing across an institution's branches and units, and systems misconfigurations. Financial institutions should continue to bolster their KYC and CDD efforts, as well as strengthen their daily screening of customers. And as evidenced by DFS's consent order against Deutsche Bank, the more difficult but necessary task is ensuring that strong and relatively consistent procedures are in place across the institution's locations worldwide, given that deficiencies at non-U.S. branches can expose the U.S. locations to sanctions/AML risk.

   FinCEN's action against BTC-e highlights the increased AML-related risks associated with certain FinTech companies. Although the FinTech regulatory environment is relatively nascent, the BTC-e action demonstrates the U.S. Government's ability to employ existing MSB-related AML regulations as an enforcement tool. Additionally, financial institutions and companies with FinTech companies as customers or partners should consider adopting appropriate KYC and CDD mechanisms to mitigate against these enhanced risks.

   Non-financial companies should also implement risk-based due diligence and screening procedures, commensurate with their business operations and risk profiles. For example, OFAC's settlement with Cartier highlights the sanctions risks for retail companies that engage in international transactions and drives home the need for all U.S. entities to develop, implement, and maintain risk-based compliance programs based upon the scope and nature of their operations. Depending on a company's international business profile, a risk-based approach may counsel in favor of incorporating

OFAC prohibited-party screening, in addition to country/region-based screening, into the company's procedures for processing customer transactions.

3. **Strengthen due diligence on foreign correspondent banks, including affiliates**. Regulators have increasingly emphasized the importance of conducting risk-based due diligence on foreign correspondent banking clients, which generally present heightened risks. One of these risks includes "nested" activity, in which a correspondent banking client is serving as an intermediary for an upstream and potentially unknown bank. For example, the DFS consent order against Habib Bank noted that the bank had not conducted sufficient due diligence on a correspondent banking client, Al Rajhi Bank, a Saudi entity with alleged links to Al Qaeda. The Al Rajhi account allegedly engaged in correspondent clearing activities for several of Al Rajhi's own affiliates, including Al Rajhi branches in Malaysia and Jordan. According to the DFS consent order, this nested account activity was entirely unknown to New York branch management, as it was not captured in the relevant customer file or correspondence and was not accounted for by Habib's transaction monitoring system.

   Since at least HSBC's December 2012 DPA, regulators expect banks to conduct due diligence on their non-U.S. branches and other affiliates as though they were unaffiliated banks. As a practical matter, regulators' diligence expectations are sometimes even higher with respect to affiliates, as there is a general assumption that a U.S. branch can obtain greater access to its affiliates' information, despite non-U.S. banking and privacy laws that might pose significant obstacles. Although it is sometimes institutionally difficult for a U.S. branch to conduct this sort of diligence on its affiliates (much less its head office), regulators will generally expect to see thorough diligence, including a well-documented review of the non-U.S. affiliate's compliance systems, products, customer types, and other risk factors. For instance, the DFS consent order against NongHyup faulted the New York branch for conducting inadequate diligence on the NongHyup Head Office and its executive management.

4. Consider implementing or updating standards for wire messages. Given the regulatory focus on wire transfers, financial institutions should consider establishing or updating policies governing the minimum information required to be included in wire messages. DFS, in particular, has signaled the importance of including sufficient information in wire messages to promote sanctions screening and AML transaction monitoring. For example, in its consent order against Habib Bank, DFS faulted the bank for processing wires that omitted "essential information" from SWIFT payment messages, "such as the identities of the ultimate originator and beneficiary of each transaction."[134] Another relevant precedent is DFS's 2014 consent order against Standard Chartered Bank ("SCB"), which required, among other remedial measures, that SCB's New York branch require that SCB affiliates include originator name and address (including country) information and any beneficiary identification information received in wire messages sent to the New York branch.[135] DFS further obligated SCB's New York branch to obtain any missing originator address information and to "undertake good faith efforts" to do the same for missing beneficiary address information. Processing payments without

this identifying information could expose financial institutions to sanctions and AML risk. Similarly, given the increasing regulatory focus on data integrity, policies on wire messages can prescribe the number of characters in input fields and other controls to help ensure that wire information is not inadvertently truncated or deleted as it travels through the banks' systems and is converted to the SWIFT format.

5. **Consider risks posed by Russia-related secondary sanctions**. The secondary sanctions provisions enacted in the CAATSA legislation create new risks for non-U.S. and U.S. entities alike, even as there remains uncertainty as to whether or how the Trump administration would implement these "mandatory" and "discretionary" provisions. It is particularly important for non-U.S. entities to conduct enhanced due diligence, if they wish to participate in: transactions targeted by secondary sanctions, including the privatization of Russia's state-owned assets; investment in, or the provision of significant goods or services to, Russian energy export pipeline projects (a potentially broad category that will likely be the subject of negotiations between the United States and EU countries); or significant transactions with the Russian defense and intelligence sectors. Non-U.S. entities also face the risk of sanctions for knowingly facilitating significant transactions, including deceptive or structured transactions, for or on behalf of any Russian related parties on the SDN list or SSI list—regardless of whether the transactions have a U.S. nexus.

   Meanwhile, U.S. entities may want to consider the commercial and reputational concerns associated with entering into business relationships with non-U.S. entities facing a significant risk of secondary sanctions. For example, U.S. defense companies may want to consider the risk of secondary sanctions in deciding whether to form new business relationships with (currently non-designated) entities that are potential targets of future sanctions, and financial institutions may want to screen for such transactions.

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

* * *

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

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

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

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

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

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

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

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

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

Associates Kamil Ammari, Matthew J. Carhart, Joseph Delich, Evan J. Meyerson, Jeffrey Newton, Matthew J. Rosenbaum, Mary Anne Schlapprizzi, Jacobus J. Schutte, Oleg M. Shik, James R. Simmons, Jr., Anand Sithian, Stephen Speirs, Katherine S. Stewart, and Kaveri Vaid contributed to this Client Memorandum.

1 Angela Greiling Keane, *Pro Policy Summit: Live Updates and highlights*, Politico (Sept. 14, 2017), *available* here.

2 *See* our prior Paul, Weiss memorandum, *President Trump Signs Sanctions Legislation Targeting Russia, North Korea and Iran, Creating New Compliance Risks for U.S. and Non-U.S. Companies* (Aug. 3, 2017), *available* here.

3 *See, e.g.*, H.R. 4373, 115th Cong. (1st Sess. 2017), *available* here; S. 1241, 115th Cong. (1st Sess. 2017), *available* here.

4 *See* Paul, Weiss memorandum, *supra* n. 2.

5 Statement by President Donald J. Trump on the Signing of H.R. 3364; Statement by President Donald J. Trump on Signing the "Countering America's Adversaries Through Sanctions Act" (Aug. 2, 2017), *available* here and here.

6 Executive Order 13810, *Imposing Additional Sanctions with Respect to North Korea* (Sept. 20, 2017), *available* here.

7 On October 20, 2017, President Trump announced the designation of North Korea as a state sponsor of terrorism, triggering additional sanctions authorities. From a compliance perspective, this designation was largely symbolic, as it is mostly duplicative of other sanctions authorities already in place. *See* Jeff Mason, *Trump Declares North Korea State Sponsor of Terrorism, Triggers Sanctions*, Reuters (Nov. 20, 2017), *available* here.

8 E.O. 13810, *supra* n. 6.

9 *Id.*

10 On November 7, 2017, the Senate Banking Committee unanimously approved the BRINK Act of 2017, which would enact mandatory secondary sanctions against non-U.S. financial institutions that provide financial services to designated persons. The BRINK Act is expressly modeled on the Iran secondary sanctions with the intention of specifically targeting non-U.S. financial institutions, and it is currently pending before the full Senate. *See* Patricia Zengerle, *U.S. Senate Panel Targets Chinese Banks with North Korea Sanctions*, Reuters (Nov. 7, 2017), *available* here; S. 1591, *To Impose Sanctions with respect to the Democratic People's Republic of Korea, and for other purposes (July 19, 2017), available* here; Sens. Chris Van Hollen & Pat Toomey, CNN, *The Act that Gets Tough on North Korea* (Nov. 7, 2017), *available* here.

11 Testimony of Anthony Ruggiero to Senate Committee on Banking, Housing, and Urban Affairs at *6 (Sept. 7, 2017), *available* here; *see, e.g.*, Treasury, *Treasury Sanctions Trading, Labor, and Shipping Companies and Vessels to Further Isolate North Korea* (Nov. 21, 2017), *available* here; Treasury, *Treasury Targets Chinese and Russian Entities and Individuals Supporting the North Korean Regime* (Aug. 22, 2017), *available* here.

12 *See* Remarks by President Trump and Prime Minister Abe of Japan Before Bilateral Meeting (Sep. 21, 2017), *available* here; @realDonaldTrump, Twitter (Dec. 28, 2017), *available* here; Statement by White House Press Secretary (Jan. 12, 2018), *available* here.

13 U.S. Dep't of Treasury, Press Release, *Testimony of Assistant Sec'y Marshall S. Billingslea before House Foreign Affairs Comm. On Threat Posed by North Korea* (Sept. 12, 2017), *available* here.

14 The president's decertification announcement came two days before a periodic deadline under INARA to certify Iran's compliance with the JCPOA. Among other requirements, INARA requires the president to certify every 90 days that four conditions have been met: (1) Iran "is transparently, verifiably, and fully implementing the agreement"; (2) Iran "has not committed a material breach with respect to the agreement or, if Iran has committed a material breach, Iran has cured the

material breach"; (3) Iran "has not taken any action, including covert activities, that could significantly advance its nuclear weapons program"; and (4) "suspension of sanctions related to Iran pursuant to the agreement is (I) appropriate and proportionate to measures taken by Iran with respect to terminating its illicit nuclear program and (II) vital to the national security interests of the United States." *See* Paul, Weiss memorandum, *President Trump Announces Intent to "De-Certify" Iran's Compliance with the Joint Comprehensive Plan of Action* (Oct. 13, 2017), *available* here.

15 The White House, Press Release, *Statement by the President on the Iran Nuclear Deal* (Jan. 12, 2018), *available* here.

16 U.S. Dep't of Treasury, Press Release, *Testimony of John E. Smith Before the House Committee on Financial Services Subcommittee on Monetary Policy and Trade Thursday, November 30, 2017* (Nov. 30, 2017), *available* here.

17 Executive Order 13224 prohibits transactions with (and blocks the assets of) persons who commit or threaten to commit international terrorism.

18 We describe CAATSA's Iran-related provisions in a previous Paul, Weiss memorandum, *available* here. While CAATSA directed the president to designate the IRGC as a terrorist organization by October 30, 2017, it also included waiver authority allowing the president to refuse to do so. From a compliance perspective, most of CAATSA's Iran-related provisions are not new, but rather codify certain authorities already used in some form by the Treasury Department to target Iran outside the scope of the JCPOA.

19 *See* Testimony of John E. Smith, *supra* n. 15.

20 *Available* here.

21 *Available* here.

22 For additional information on Russia/Ukraine sanctions, please refer to our December 20, 2017 memorandum, *available* here.

23 *See* The White House, Press Release, *Remarks by President Trump on the Policy of the United States Towards Cuba* (June 16, 2017), *available* here.

24 *See* The White House, Press Release, *National Security Memorandum on Strengthening the Policy of the United States Toward Cuba* (June 16, 2017), *available* here.

25 *See* U.S. Department of Treasury, Press Release, *Treasury, Commerce, and State Implement Changes to the Cuba Sanctions Rules, Amendments Implement President Trump's June 2017 National Security Presidential Memorandum (NSPM) Strengthening the Policy of the United States Toward Cuba* (Nov. 9, 2017), *available* here.

26 *See* U.S. Department of State, List of Restricted Entities and Subentities Associated with Cuba as of November 9, 2017 (Nov. 8, 2017), *available* here.

27 *See* 31 CFR § 515.209.

28 *See* 31 CFR §§ 515.209, 515.505(a), 515.571, 515.584(d).

29 See *Testimony of John E. Smith*, *supra* n. 16.

30 *See* U.S. Dep't of the Treasury, *Treasury Sanctions 13 Current and Former Senior Officials of the Government of Venezuela* (July 26, 2017), *available* here; U.S. Dep't of the Treasury, Press Release, *Treasury Sanctions the President of Venezuela* (July 31, 2017), *available* here.

[31] *See* Executive Order 13808, 82 Fed. Reg. 41,155, *Imposing Additional Sanctions with Respect to the Situation in Venezuela* (Aug. 29, 2017), *available* here.

[32] OFAC also published four Venezuela-related general licenses to, among other things, allow companies to wind down existing contracts impacted by the executive order and to allow certain humanitarian imports.

[33] U.S. Dep't of the Treasury, Press Release, *Testimony of John E. Smith Director of the Office of Foreign Assets Control U.S. Dep't of the Treasury House Committee on Financial Services Subcommittee on Monetary Policy and Trade Thursday, November 30, 2017* (Nov. 30, 2017), *available* here.

[34] U.S. Dep't of the Treasury, Press Release, *Treasury Sanctions Ten Venezuelan Government Officials* (Nov. 9, 2017), *available* here.

[35] *See* U.S. Dep't of the Treasury, *Office of Foreign Assets Control, FAQs: Other Sanctions Programs, Question 505* (Feb. 13, 2017), *available* here.

[36] *See* Executive Order No. 13761, *Recognizing Positive Actions by the Government of Sudan and Providing for the Revocation of Certain Sudan-Related Sanctions* (Jan. 13, 2017) , *available* here.

[37] *See* Executive Order No. 13804, *Allowing Additional Time for Recognizing Positive Actions by the Government of Sudan Amending Executive Order 13761* (July 11, 2017) , *available* here.

[38] *See* U.S. Dep't of the Treasury, Resource Center, Sudan and Darfur Sanctions, *available* here.

[39] *See* U.S. Department of the Treasury, Sudan, Darfur, and South Sudan-related Sanctions, Revocation of Certain Sanctions with Respect to Sudan and the Government of Sudan on October 12, 2017, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#sudan_whole.

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

[41] OFAC's March 7, 2017 settlement agreement with ZTE is *available* here.

[42] The March 7, 2017 OFAC enforcement information is *available* here.

[43] Paul, Weiss memorandum, *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.

[44] The July 27, 2017 OFAC enforcement information is available here.

[45] *See* 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.

[46] The June 26, 2017 OFAC enforcement information is *available* here.

[47] The August 24, 2017 OFAC enforcement information is *available* here.

[48] *See* U.S. Dep't of the Treasury Office of Foreign Assets Control, *Enforcement Information for Feb. 3, 2017, available* here.

[49] *See* U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Enforcement Information for July 20, 2017, available* here. Rosneft is on the SSI List as subject to Directives 2 and 4 under Executive Order 13662 of March 20, 2014, "Blocking Property

of Additional Persons Contributing to the Situation in Ukraine," but those authorities are not implicated in the enforcement action. Rosneft is not subject to blocking sanctions.

50 *Id*.

51 *See ExxonMobil Corp*. v. *Mnuchin*, Civ. No. 3:17-cv-1930 (N.D. Tex. Jul, 7, 2017).

52 *See* U.S. Dep't of the Treasury, Office of Foreign Assets Control, *The U.S. Department of the Treasury's Office of Foreign Assets Control Assesses a Civil Monetary Penalty Against ExxonMobil Corporation* (Jul. 20, 2017), available here.

53 The September 26, 2017 OFAC enforcement information is *available* here.

54 *Id*.

55 The August 10, 2017 OFAC enforcement information is *available* here.

56 The October 5, 2017 OFAC enforcement information is *available* here.

57 The November 28, 2017 OFAC enforcement information is *available* here.

58 *See* Section 560.325 of the Iranian Transactions and Sanctions Regulations.

59 FinCEN Advisory FIN-2017-A008, Advisory on North Korea's Use of the International Financial System, dated Nov. 2, 2017, *available* here.

60 Striking a similar note in 2016, Juan Zarate, former Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes, described the future of BSA/AML compliance as follows: "Higher-quality data and greater information sharing would be essential for this model, using big data capabilities, biometrics and identity verification, and network and behavioral analysis." *See* Juan Zarate & Chip Poncy, *Designing a New AML System* (2016), *available* here. This trend is already emerging more broadly in the form of in-house Financial Intelligence Units (FIUs) dedicated to investigations beyond day-to-day monitoring and the more frequent deployment of sophisticated analytics software.

61 U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, *Advisory on Widespread Public Corruption in Venezuela* (Sept. 20, 2017), *available* here.

62 U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, *FinCEN Warns Financial Institutions to Guard Against Corrupt Venezuelan Money Flowing to U.S.* (Sept. 20, 2017), *available* here.

63 U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, *FinCEN Advisory to Financial Institutions and Real Estate Firms and Professionals* (Aug. 22, 2017), *available* here.

64 *See* Paul, Weiss, *FinCEN Issues Sweeping Requirements on the Collection of Beneficial Ownership Information and Customer Due Diligence* (May 10, 2016), *available* here; *see also* Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29397 (May 11, 2016).

65 *See United States* v. *The Western Union Company*, No. 1:17-cr-00011 (M.D. Pa. Jan. 19, 2017).

66 U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, *FinCEN and Manhattan U.S. Attorney Announce Settlement with Former MoneyGram Executive Thomas E. Haider* (May 4, 2017), *available* here.

67 The National Law Journal, R. Gonzalez and J. Carey, *The Government's Making AML Enforcement Personal* (Feb. 22, 2016).

[68] U.S. Dep't of the Treasury, *Treasury Acts to Increase Economic Pressure on North Korea and Protect the U.S. Financial System* (June 29, 2017), *available* here.

[69] Final Rule, Imposition of Special Measure Against Bank of Dandong as a Financial Institution of Primary Money Laundering Concern, Nov. 8, 2017, *available* here.

[70] *Id*.

[71] U.S. Dept. of Justice, *Four Chinese Nationals and China-Based Company Charged with Using Front Companies to Evade U.S. Sanctions Targeting North Korea's Nuclear Weapons and Ballistic Missile Programs* (Sep. 26, 2016), *available* here.

[72] Ian Talley, WSJ, *U.S. to Sanction Chinese Bank Over North Korea Financing* (June 29, 2017), *available* here.

[73] Testimony of Assistant Secretary Billingslea to House Foreign Affairs Committee (Sept. 12, 2017), *available* here.

[74] *Id*.

[75] *Id*.

[76] U.S. Dept. of Justice, *Banamex USA Agrees to Forfeit $97 Million in Connection with Bank Secrecy Act Violations* (May 22, 2016), *available* here. Paul, Weiss represented Citigroup and BUSA in this matter.

[77] According to the Statement of Facts, from 2007 to 2012 BUSA "processed over 30 million remittance transactions to Mexico with a total value of more than $8.8 billion with virtually no investigation for suspicious activity."

[78] DOJ recognized BUSA's prior payment of $140 million in penalties to the Federal Deposit Insurance Company and the California Department of Business Oversight to resolve related BSA/AML investigations.

[79] U.S. Dept. of Justice, *Lebanese Businessman Tied to Hizballah Arrested For Violating IEEPA and Defrauding the U.S. Government* (Mar. 24, 2017), *available* here.

[80] Indictment, *United States* v. *Tajideen*, 1:17-cr-00046-RBW, (D.D.C. Mar. 7, 2017); U.S. Dept. of Justice, *Lebanese Businessman Tied to Hizballah Arrested For Violating IEEPA and Defrauding the U.S. Government* (Mar. 24, 2017), *available* here.

[81] Indictment, *United States* v. Zong, 3:16-cr-00142-SLG-DMS (D. Alaska Dec. 14, 2016), ECF No. 1.

[82] *Id*.

[83] U.S. Dep't of Justice, *Turkish Banker Convicted of Conspiring to Evade U.S. Sanctions Against Iran and Other Offenses* (Jan. 3, 2018), *available* here.

[84] Sealed Superseding Information, *United States* v. *Zarrab*, 1:15-cr-00867-RMB (S.D.N.Y. Oct. 16, 2017), ECF No. 364.

[85] *Id*.

[86] Paul, Weiss, *Second Circuit Rules that Compliance Monitor's Report is not a Judicial Document, Rejecting District Court's Supervisory Power Over Deferred Prosecution Agreement* (Jan. 18, 2017), *available* here.

[87] *U.S.* v. *HSBC Bank, N.A.*, 16-308(L), slip op. at 3 (2d Cir. July 12, 2017) (Pooler, J., concurring).

[88] In December of 2017, DOJ submitted to the district court a motion to dismiss the criminal information DOJ filed against HSBC five years earlier. Under the DPA, DOJ agreed that it would move to dismiss the information against HSBC within 30 days following the expiration of the DPA's five-year term, provided that HSBC fully complied with its obligations under the DPA.

DOJ informed the district court that it had determined that HSBC complied with its DPA obligations, and, accordingly, dismissal of the information with prejudice was appropriate. That same day, the district court granted the government's motion and dismissed the information against HSBC with prejudice. Motion to Dismiss Information at 2, *United States* v. *HSBC Bank, USA, N.A., et al.*, No. 12 CR 763 (AMD), (E.D.N.Y. Dec. 12, 2017) ("*HSBC*"), ECF No. 96.

89 Office of the Comptroller of the Currency, *OCC Report Discusses Key Risks for Federal Banking System* (Jan. 18, 2018), *available* here.

90 *Id*.

91 Jeff Cox, *Trump Picks Jerome Powell to Succeed Yellen as Fed Chair*, CNBC.com (Nov. 2, 2017), *available* here.

92 Jesse Hamilton, *Senate Confirms Ex-Carlyle Executive Randall Quarles as Fed Vice Chairman*, Bloomberg (Oct. 5, 2017), *available* here.

93 Pete Schroeder & Patrick Rucker, *Ex-banker Otting Confirmed as U.S. Comptroller of the Currency*, Reuters (Nov. 17, 2017), *available* here.

94 Pete Schroeder, *Trump Taps Fifth Third Lawyer McWilliams to Lead FDIC*, Reuters (Dec. 1, 2017), *available* here.

95 Brett Wolf, Exclusive: Trump Unlikely to Curb AML rules; new, 'fairly loose' cyber standards seen–Guiliani, Reuters (Mar. 11, 2017), *available* here.

96 *See* Bd. Of Governors of the Fed. Reserve System, Cease and Desist Order Issued Upon Consent Pursuant to the Federal Deposit Insurance Act, as amended, In the Matter of Deutsche Bank AG, et al. (May 26, 2017), at pg. 2–3.

97 Financial Conduct Authority, *FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings* (Jan. 31, 2017), *available* here.

98 *See id*.

99 Office of the Comptroller of the Currency, *OCC Assesses $70 Million Civil Money Penalty Against Citibank* (Jan. 4, 2018), *available* here.

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

101 *See* Bd. Of Governors of the Fed. Reserve System, Cease and Desist Order Issued Upon Consent Pursuant to the Federal Deposit Insurance Act, as amended, In the Matter of BB&T Corporation (Jan. 25, 2017).

102 *See* U.S. Dep't of the Treasury, Comptroller of the Currency, Agreement by and between UBS AG New York, New York, and The Office of the Comptroller of the Currency (March 24, 2017).

103 *See* Securities and Exchange Commission, Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, and Section 203(e) of the Investment Advisers Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order, In the Matter of Merrill Lynch, Pierce, Fenner & Smith Incorporated (Dec. 21, 2016).

104 *Id*.

[105] *See* Securities and Exchange Commission, Order Instituting Administrative and Cease-and-Desist Proceedings Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order, In the Matter of Wells Fargo Advisors, LLC (Nov. 13, 2017).

[106] *Id.*

[107] *See* Complaint, *U.S. Sec. & Exch. Comm'n* v. *Alpine Securities Corporation* (S.D.N.Y. June 5, 2017), *available* here.

[108] FINRA's 2018 Annual Regulatory and Examinations Priorities Letter, *available* here.

[109] *See* Merrill Lynch, Financial Industry Regulatory Authority Letter Of Acceptance, Waiver And Consent (Dec. 23, 2016), *available* here.

[110] *See* our prior Paul, Weiss memorandum, *New York DFS Finalizes Stringent Anti-Money Laundering and Sanctions Regulation* (Jul. 1, 2016), *available* here.

[111] N.Y. Dep't of Fin. Servs., *Frequently Asked Questions Regarding 3 NYCRR 504* (Oct. 26, 2017), *available* here.

[112] N.Y. Dep't of Fin. Servs., *Frequently Asked Questions Regarding 23 NYCRR 500* (Mar. 1, 2017), *available* here.

[113] N.Y. Dep't of Fin. Servs., Consent Order Under New York Banking Law §§ 39, 44 and 44-a in the Matter of Deutsche Bank AG and Deutsche Bank AG New York Branch (Jan. 30, 2017) , *available* here.

[114] Federal Reserve, Order to Cease and Desist and Order of Assessment of a Civil Money Penalty Issued Upon Consent, Pursuant to the Federal Deposit Insurance Act, as Amended (May 26, 2017), *available* here.

[115] N.Y. Dep't of Fin. Servs., *DFS Fines Deutsche Bank $425 Million for Russian Mirror-Trading Scheme* (Jan.30, 2017), *available* here.

[116] The consent order can be found here. For a more detailed analysis of the Habib case, see a prior Paul, Weiss memorandum *available* here.

[117] The August 24, 2017 notice of hearing and statement of charges by DFS is available here. While the document is dated August 24, 2017, DFS did not publish it until August 28, 2017.

[118] The order regarding the surrender of the Branch's banking license can be found here.

[119] The order regarding the expanded transactional lookback can be found here. DFS's December 15, 2015 consent order against Habib is available here. The Federal Reserve's December 11, 2015 consent order against the Habib is available here. As noted by DFS, Habib had recognized compliance issues dating back more than a decade, as evidenced by a December 2006 agreement among Habib, the Federal Reserve, and the New York State Banking Department, which is available here.

[120] N.Y. Dep't of Fin. Servs., *DFS Fines Habib Bank and its New York Branch $225 Million for Failure to Comply with Laws and Regulations Designed to Combat Money Laundering, Terrorist Financing, and Other Illicit Financial Transactions* (Sep. 7, 2017), *available* here.

[121] N.Y. Dep't of Fin. Servs., Consent Order Under New York Banking Law §§ 39 and 44 in the Matter of NongHyup Bank and NongHyup Bank, New York Branch (Dec. 21, 2017), *available* here.

[122] *Id.*

[123] The consent order can be found here.

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

[125] N.Y. Dep't of Fin. Servs., *DFS Fines Western Union $60 Million for Violations of New York's Anti-Money Laundering Laws and for Ignoring Suspicious Transactions to Locations in China* (Jan. 4, 2018), *available* here.

[126] Consent Order ¶ 69.

[127] *Id*. at ¶ 69(b).

[128] *Id*. at ¶ 69(g)(i).

[129] As with the Panama Papers, the Paradise Papers were leaked to reporters affiliated with the German newspaper *Suddutsche Zeitung* and then shared with the International Consortium of Investigative Journalists ("ICIJ"), a network of more than 380 journalists from journalistic institutions around the world.

[130] OCCRP, The Russian Laundromat Exposed, *available* here.

[131] The draft bill, as published by the House Financial Services Committee, is *available* here.

[132] H.R. 4373, 115th Cong. (1st Sess. 2017), *available* here.

[133] S. 1241, 115th Cong. (1st Sess. 2017), *available* here.

[134] N.Y. Dep't of Fin. Servs., Consent Order Under New York Banking Law §§ 39, 44 and 605 in the Matter of Habib Bank Limited and Habib Bank Limited, New York Branch (Aug. 24, 2017), at 8.