February 22, 2017

The Regulatory and Enforcement Outlook for Financial Institutions in 2017: Trends in Sanctions, Anti-Money Laundering and Cybersecurity

Table of Contents

Executive Summary

Economic sanctions, anti-money laundering and cybersecurity remain at the forefront of U.S. regulatory priorities. This memorandum surveys major developments and trends in these areas in 2016 and early 2017 and provides an outlook for financial institutions in the year ahead. As discussed below, although the new administration brings considerable uncertainty, we believe the strong federal agency focus in these areas is likely to continue. And, at the state level, the New York Department of Financial Services' attention to these areas will continue to be rigorous. Boards of directors, senior management, general counsel and compliance officers of both U.S. and non-U.S. financial institutions would be well advised to continue their vigilance in these areas. We also provide some practical suggestions for continuing to strengthen compliance in this challenging environment.

Sanctions/Anti-money Laundering. Bookended by the implementation of the Iran nuclear deal in January 2016 and the presidential transition in January 2017, the past year saw a number of sea changes in sanctions programs administered by Treasury's Office of Foreign Asset Control ("OFAC"). As summarized below, the Obama Administration eased or rolled back sanctions on Iran, Cuba, Burma and Sudan, and, for the first time, imposed cyber sanctions, designating certain Russian targets for interference with U.S. election processes. OFAC also entered into a number of enforcement settlements showing the agency's increasing concern with financial institutions that fail to identify that their customers were—or later became—sanctioned parties or were linked in some manner to sanctioned parties or countries.

In the Bank Secrecy Act/anti-money laundering ("AML") area, the publication of the Panama Papers in April 2016 brought intense global focus to issues of money laundering and shell companies. A month later, Treasury's Financial Crimes Enforcement Network ("FinCEN") finalized its broad new rule on customer due diligence and beneficial ownership, adding new compliance challenges to banks and other covered institutions. And, although there were no blockbuster enforcement actions last year at the federal level, 2017 began with a half-billion dollar AML resolution by the Department of Justice ("DOJ"), FinCEN and the Federal Trade Commission against a prominent money services business. Last year also saw active AML enforcement from the Financial Industry Regulatory Authority ("FINRA"), which levied several penalties against broker-dealers, including its largest AML penalty to date of $17 million.

At the state level, the New York Department of Financial Services ("DFS") continued its aggressive activity on the regulatory and enforcement fronts. Following Maria Vullo's confirmation as Superintendent, the agency finalized its Part 504 regulation, which prescribes broad requirements for transaction monitoring and sanctions screening programs and mandates annual senior-level compliance certifications. DFS also issued four significant consent orders against non-U.S. banks and their New York branches, each $180 million or higher. Three of these orders demonstrate DFS's increasing willingness to issue sizable penalties based primarily on findings of AML (and, to a lesser extent, sanctions) compliance deficiencies, rather than on specific violative transactions. The fourth order is notable for imposing a large penalty focused on AML deficiencies at a non-U.S. branch, with little attention given to the actions or inactions of the bank's New York offices.

We also provide an update on the latest expansive turn in Anti-Terrorism Act civil litigation, which can follow in the wake of sanctions/AML enforcement actions.

As discussed in more detail on pages 23-26, to strengthen sanctions/AML compliance we would recommend that financial institutions consider the following steps, many of which are abiding themes:

1. Exercise increased caution in light of a changed administration.

2. Bolster tone at the top and the culture of compliance.

3. Focus on data integrity, systems, and programming issues.

4. Further prepare for enforcement focused on compliance deficiencies rather than specific violative transactions.

5. Bolster customer due diligence and daily customer screening across the institution.

6. Strengthen due diligence on non-U.S. branches and other affiliates.

Cybersecurity. In another year marked by high-profile cyberattacks, financial regulators showed an increased focus on promulgating regulations—a harbinger of increased examination attention and, potentially, enforcement actions in the years ahead. The most aggressive step was taken by DFS, which proposed a cybersecurity regulation in September 2016, revised the proposal in December 2016, and issued the final regulation on February 16, 2017. The landmark regulation prescribes an array of cybersecurity program requirements and requires senior-level annual certifications of compliance. Last October, the federal banking agencies issued an advanced notice of proposed rulemaking on enhanced cybersecurity standards for the largest banks and branches. While banks have thus far not experienced sizeable penalties in connection with cyberattacks, under increasingly detailed cybersecurity regulatory requirements they may find themselves the targets of regulatory criticism and enforcement for their failure to avert cybercrime.

Other financial regulatory agencies showed increased activity in cybersecurity last year. For example, the Securities and Exchange Commission ("SEC") imposed a $1 million penalty in connection with the alleged failure of a registered broker-dealer and investment advisor to adopt adequate policies and procedures that would have prevented an employee's theft of customer information. And, the Consumer Financial Protection Bureau ("CFPB") took its first cybersecurity action against a company for purportedly mispresenting the strength of its data protection practices.

As discussed in more detail on pages 29-31, we would suggest consideration of the following steps to strengthen cybersecurity:

1. Prepare for a tougher regulatory approach to cybersecurity, potentially including enforcement actions.

2. Review external policies and statements regarding data security.

3. Emphasize employee training.

4. Clarify roles between U.S. branches and the bank's headquarters.

5. Continue to monitor the private litigation environment and bolster incident response planning.

Implications of the New Trump Administration

With the inauguration of President Trump and the substantial turnover in federal agency leadership, the months and years ahead will see considerable uncertainty across a number of regulatory areas. Nevertheless—and despite President Trump's deregulatory agenda—there is reason to believe that the rigorous level of federal sanctions and AML enforcement will largely remain stable.

As an initial matter, economic sanctions will likely continue to be a favored tool for addressing national security and foreign policy problems, representing an expedient midway point between diplomacy and military force.[1] Indeed, after only two weeks in office, President Trump announced new designations targeting Iran. And, while certain U.S. sanctions programs may expand (*e.g.*, Iran) or contract (*e.g.*, Russia) under President Trump, there is generally bipartisan support for sanctions and AML enforcement, given its groundings in national security and anti-terrorism concerns. The dynamic of multi-agency jurisdiction in this area, combined with a strong staff-level commitment at the banking agencies to avoid "missing" a sanctions/AML problem on their watch, also creates powerful momentum for continued agency focus. While the size of corporate penalties may be impacted under a Trump Administration, we do not foresee a significant shift in terms of overall sanctions/AML enforcement. (For a discussion of recent developments in Foreign Corrupt Practices Act enforcement and the potential impact of the Trump Administration, see the recent Paul, Weiss memorandum on the subject.[2])

The Trump Administration's impact on cybersecurity regulation is less clear. As a candidate, President Trump called the federal government's cyber defenses "obsolete" and promised an immediate review of those capabilities.[3] More recently, President Trump has indicated that he plans to sign a new Executive Order regarding cybersecurity, although to date the final order has not been released.[4] In light of President Trump's generally deregulatory stance, it is uncertain whether he would favor strengthening legislative or regulatory cybersecurity requirements on the private sector. Nevertheless, the financial regulatory agencies seem firmly committed to increased activity in this area given the high stakes. In our view, this commitment seems unlikely to waver under new agency leadership.

With respect to financial institutions also regulated by DFS, no wane in enforcement is in sight. Indeed, Superintendent Vullo has already indicated that DFS stands ready to fill any enforcement void created by the new administration in order to protect the people and financial system of New York.[5]

Recent Developments and Trends in Sanctions and AML

Treasury's Office of Foreign Assets Control

Last year did not see any of the large, multi-agency enforcement actions that have characterized the sanctions space in recent years. OFAC levied only $21 million in civil penalties in 2016, as compared to $599 million in 2015 and $1.2 billion in 2014.[6] In lieu of major enforcement actions, in 2016 OFAC focused on initiating or managing an unprecedented number of sea changes in various sanctions

programs. These changes were effectuated through a number of executive orders, regulatory amendments and guidance documents, and were accompanied by a large increase in licensing applications.[7]

Sweeping Changes in OFAC Sanctions Programs. At the beginning of 2016, the nuclear-related secondary sanctions targeting Iran remained in full effect, many of the Cuba-related restrictions remained in force, the Burma and Sudan programs continued, and OFAC had yet to use its cyber-related authorities. A year later, much has changed. In addition to creating new opportunities, the sheer frequency and extent of changes in OFAC's programs—even those easing sanctions—can increase complexity, create confusion on the part of customers, and expand the opportunities for compliance foot faults.

Below, we outline the most significant changes in OFAC's sanctions programs and note some of the uncertainties that exist under the new administration.

- ***Iran Sanctions.*** As detailed in a prior Paul, Weiss memorandum,[8] January 16, 2016 marked "Implementation Day" of the nuclear deal with Iran, when President Obama lifted the nuclear-related secondary sanctions on Iran, removed a large number of Iranian persons[9] from OFAC lists, and issued various licenses, including General License H.[10] After Implementation Day, U.S. persons must continue to adhere to the U.S. embargo on Iran, which broadly prohibits them from engaging in or facilitating business dealings with Iran or its government, while non-U.S. persons must steer clear of the remaining U.S. secondary sanctions on Iran or face a potential cutoff from the U.S. financial system.[11]

  General License H authorizes non-U.S. companies owned or controlled by U.S. persons to do business with Iran, subject to various conditions.[12] This three-page license has caused a fair amount of uncertainty. It appears that both public and private U.S. companies have generally been reluctant to embrace the general license in light of various risks, including SEC disclosure requirements, banking and capital market difficulties, reputational concerns, the risk of debarment from state contracts, the remaining sanctions on Iran, and AML and corruption risks in Iran. Some companies have also been reluctant to use the license due to the difficulty of adhering to its conditions, including maintaining a high degree of separation between the U.S. company (and any U.S. persons) and the Iranian business and avoiding transactions with specific Iranian counterparties that remain prohibited under the license. Over the course of the year, OFAC issued guidance to clarify the use of General License H and other aspects of the easing of Iran sanctions, such as the use of U.S. dollars in trade with Iran, but many questions remain unresolved.[13]

  And while many non-U.S. companies have been eager to pursue opportunities in Iran, some—particularly in the case of global public companies—have been concerned by many of the risks described above. Indeed, a number of major European banks have declined to expand their business with Iran.[14]

  President Trump's campaign pledge to "dismantle" or renegotiate the "disastrous" Iran deal has likely given further encouragement to those who have stayed on the sidelines, although President Trump has also stated that he will "enforce the terms of the previous deal to hold Iran totally accountable."[15] If the deal remains intact, we would expect the Trump Administration to cut back on the prior administration's

attempts to implement the deal "in both letter and spirit"[16] and instead adhere more closely to the strict letter of the agreement.

Compounding the uncertainty around the fate of the nuclear deal is concern over how companies would navigate, as a practical matter, a sanctions "snapback," should one occur. Last year, OFAC described its intent to provide a 180-day wind down period in the event of snapback,[17] but even under this approach—which the Trump Administration could alter at will—it appears that companies would need to precipitously halt the provision of services or goods under existing contracts, absent a license.

Finally, outside the confines of the nuclear deal, the Trump Administration has already used its non-nuclear sanctions authorities to sanction over two dozen Iran-related individuals and entities.[18] Meanwhile, the new Congress is considering a number of broad Iran-related sanctions proposals.[19] For many U.S. and non-U.S. financial institutions, navigating the complexity and fluidity of the Iran sanctions environment ranks as a top concern.

- ***Cuba Sanctions.*** OFAC and the Commerce Department's Bureau of Industry and Security ("BIS") took various regulatory actions in 2016 to further ease Cuba sanctions and export controls. These actions authorized, among other things, "people-to-people" educational travel to Cuba; certain transactions involving Cuban-origin pharmaceuticals and joint medical research; civil aviation safety-related services; and the provision of certain insurance and reinsurance services.[20] The actions also authorized, under certain conditions, "U-turn" payments cleared through the U.S. financial system, the processing of U.S.-dollar monetary instruments presented indirectly by Cuban financial institutions, and the maintenance of U.S. bank accounts for certain Cuban nationals.[21] While these changes create opportunities for U.S. companies, they also create compliance challenges, including for the financial institutions that support these transactions.

  Despite the many changes implemented by the Obama Administration, the Cuba embargo remains in place, and OFAC continues to enforce the remaining prohibitions of the Cuba sanctions regulations. Meanwhile, President Trump has injected further uncertainty into this area by tweeting that if Cuba does not make further concessions, he would consider reversing the easing of sanctions.[22]

- ***Russia-Ukraine Sanctions.*** In response to Russia's occupation of Crimea in March 2014, the Obama Administration implemented three types of sanctions: designations of Specially Designated Nationals ("SDNs"); an embargo against Crimea; and "sectoral" sanctions.[23] These "sectoral sanctions," which are the first of their kind, target transactions involving new equity or debt of certain durations with designated entities in Russia's energy, defense, and financial sectors; these entities appear on OFAC's Sectoral Sanctions Identifications ("SSI") List. These sanctions also target the supply of certain goods, services, or technology in support of Russian deepwater, Arctic offshore, or shale exploration or production projects that involve designated Russian entities. In the later part of 2016, OFAC designated additional parties under these authorities.[24]

These sanctions were recently described by one former Treasury official as "the most sophisticated sanctions campaign the Treasury Department has ever, ever created."[25] And financial institutions have continued to struggle with their implementation, including the challenges of analyzing complex transactions under sectoral sanctions, applying the 50 percent rule (which blocks entities that, while not on the SDN list, are 50 percent or more owned, directly or indirectly, by one or more SDNs) in the Russian context, and enforcing—without the ability to rely on country information—the regional embargo on Crimea.

The future of Russia sanctions is unclear, with President Trump saying during his campaign that he would consider lifting these sanctions and recognizing Crimea as Russian territory.[26] But more recently, U.S. Ambassador to the United Nations Nikki Haley stated: "Our Crimea-related sanctions will remain in place until Russia returns control over the peninsula to Ukraine."[27] Meanwhile, a bipartisan group of senators has introduced a sweeping sanctions bill, the "Countering Russian Hostilities Act of 2017," which responds both to Russia's aggression in Ukraine and its cyber behavior. A second bipartisan group of senators has introduced the "Russia Sanctions Review Act," which would provide Congress a 120-day review period before the lifting of any sanctions targeting Russia, as well as a vote to approve or disapprove such an action.[28]

- ***North Korea Sanctions.*** In light of North Korea's ballistic missile testing and nuclear proliferation activities, the North Korea Sanctions and Policy Enhancement Act was enacted on February 18, 2016.[29] The following month, President Obama issued an Executive Order that, among other things, banned exports to, and new investment into, North Korea and expanded the grounds for further designations.[30] OFAC sanctioned additional North Korean persons throughout 2016 and into 2017—including, most notably, North Korean leader Kim Jong Un.[31] In addition, on June 1, 2016, the Treasury Department, citing North Korea's use of state-controlled financial institutions and front companies, issued a notice of finding that North Korea is a "jurisdiction of primary money laundering concern" under Section 311 of the USA PATRIOT Act.[32] FinCEN issued a related rule that requires, among other things, U.S. financial institutions to implement additional due diligence measures to prevent North Korean financial institutions from gaining indirect access to the U.S. financial system, such as through third-country bank's U.S. correspondent accounts.[33]

- ***Burma Sanctions.*** On October 7, 2016, President Obama terminated U.S. sanctions against Burma in light of the country's democratic progress, fulfilling his pledge to Burma's State Counsellor Aung San Suu Kyi.[34] Concurrently, FinCEN issued an administrative exception to suspend prohibitions relating to Burma's designation as a "jurisdiction of primary money laundering concern."[35] Despite these changes, financial institutions must continue to be vigilant about the risk of transactions with Burmese persons who remain on the SDN List because they were designated under another sanctions program, such as counter-narcotics.[36]

- ***Sudan Sanctions.*** While the rollback of Burma sanctions was widely anticipated, the Obama Administration's suspension of the bulk of Sudan sanctions took many by surprise. Citing "ongoing

engagement between the United States and Sudan" with regard to humanitarian issues and counterterrorism cooperation, on January 17, 2017, OFAC published a general license that immediately authorized all transactions previously prohibited by its Sudanese Sanctions Regulations.[37] The general license was issued in conjunction with an Executive Order by President Obama that will revoke the major sanctions on Sudan effective July 12, 2017, provided that the Secretary of State finds that Sudan has sustained its progress.[38] The Trump Administration will have to decide whether to complete this revocation and maintain the general license.[39]

Despite the general license, financial institutions should proceed with caution. A number of Sudanese persons are designated under other sanctions regimes that remain unaffected, including those with respect to Darfur and South Sudan. And while BIS did ease specific export licensing requirements,[40] many export/re-export restrictions remain. Additionally, Sudan remains listed as a State Sponsor of Terrorism, so business with Sudan may give rise to securities disclosure obligations.[41] Until there is further certainty as to President Trump's policy in this area, many financial institutions may decide to reject most or all transactions involving Sudan.

- ***Cyber Sanctions.*** In the first-ever use of its cyber-related sanctions authority, on December 29, 2016, OFAC imposed sanctions on five Russian entities (including Russia's Federal Security Service or "FSB") and four individuals in connection with their apparent efforts to interfere with the 2016 U.S. presidential election. These sanctions were issued under Executive Order 13757, which expanded the original (and unused) cyber sanctions executive order to authorize sanctions on those responsible for "tampering with, altering, or causing the misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions."[42]

  On February, 2, 2017, OFAC issued a general license authorizing certain transactions with the FSB.[43] While some initial reporting suggested this was the first step toward the Trump Administration's easing of sanctions targeting Russia, OFAC guidance suggests that the license was issued to fix an unintended consequence of the FSB designation, which was "unduly impact[ing]" U.S. companies that required authorization from the FSB to export certain IT products to Russia.[44]

- ***Kingpin Act Sanctions.*** In what it called "the culmination of a multi-year investigation," on February 13, 2017, OFAC designated Venezuela's Vice President (Tareck Zaidan El Aissami Maddah) as a Specially Designated Narcotics Trafficker under the Foreign Narcotics Kingpin Designation Act (the "Kingpin Act").[45] Treasury Secretary Stephen Mnuchin discussed the action at a White House press briefing, pointing out that the Trump Administration would continue to make appropriate use of sanctions, which Mnuchin described as "an important tool."[46] OFAC also designated or identified as blocked property 13 companies that comprised 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[.]"[47]

OFAC Enforcement Actions. Although OFAC's penalties in 2016 totaled only $21 million, some of its enforcement actions are nevertheless instructive, highlighting areas for self-assessment and potential improvement. As described below, the dominant theme of the OFAC actions involving financial institutions was the institutions' failures to identify that their customers were—or later became—SDNs, or were linked in some manner to SDNs or sanctioned countries. OFAC appears concerned about institutions that, whether because of systems or process-related deficiencies, fail to identify and act on information about their customers that was in the institutions' possession or otherwise readily at hand. Notably, last year OFAC also made greater use of "Findings of Violation," which involve no monetary penalty.

We describe a select number of OFAC enforcement actions below.

- ***Barclays.*** Barclays paid $2.48 million to settle allegations that, from 2008–2013, it processed funds transfers through the U.S. financial system on behalf of customers of its Zimbabwe affiliate that were owned 50 percent or more, directly or indirectly, by a Zimbabwe entity on the SDN list. This is thought to be the first OFAC action based solely on the 50 percent rule. OFAC stated that this action highlights the need for institutions to take "appropriate measures" when they have operations in countries with a "significant presence" of SDNs. According to OFAC's allegations, "Barclays attempted to comply with OFAC sanctions," but shortcomings in the Zimbabwe affiliate's Know-Your-Customer ("KYC") procedures resulted in failures to include data on the customers' related parties and beneficial owners in information that was provided to Barclays UK for sanctions screening.

  OFAC noted that an enforcement response may be particularly appropriate in these circumstances when a financial institution fails to act on records clearly indicating the SDN ownership of its customer or when the ownership information is publicly available and allows other banks to block such transactions.[48]

- ***TD Bank.*** On January 13, 2017, Canada-based TD Bank reached a $516,106 settlement with OFAC for purportedly processing transactions totaling over $2 million through the U.S. financial system in violation of Iran and Cuba sanctions.[49] The bank is alleged to have processed multiple transactions on behalf of customers that it knew or should have known were prohibited, including a Canadian customer that was Cuban-owned, account holders who were Cuban nationals residing in Canada, and a Canadian shipping company that was acting as a sales agent for an SDN in Iran.

  OFAC also issued a Finding of Violation because two of TD Bank's European subsidiaries allegedly processed over $92 million worth of securities-related transactions through the U.S. financial system on behalf of customers, despite purportedly having information that the customers were either resident in Iran or Cuba at the time of account opening or later moved there. According to OFAC, during much of the period in question, these TD Bank subsidiaries "did not appear to have" OFAC compliance programs in place. OFAC's press release stressed the importance of appropriate compliance measures when a bank

has subsidiaries in high risk industries, "such as securities firms." The action also "highlights the risk associated with online payment platforms when the financial institution is unable to restrict access for individuals and entities located in comprehensively sanctioned countries."[50]

- ***AXA Equitable Life Insurance* and *Humana, Inc.*** AXA received a Finding of Violation because, as alleged by OFAC, neither AXA nor its U.S. third-party administrator screened the names of policyholders serviced by the third party and therefore did not identify that three of its policyholders were subsequently added to the SDN list. A separate OFAC notice indicates that the third-party administrator was a subsidiary of Humana, which also received a Finding of Violation.[51]

- ***Compass Bank.*** Compass received a Finding of Violation arising out of allegations by OFAC that, due to a misconfiguration in its sanctions screening filter, dormant or inactive accounts were not screened against changes to the SDN list for more than four years. As a result, OFAC claimed, the bank failed to identify that two of its customers had been added to the SDN list. Moreover, OFAC alleged that, after a bank employee identified one of the SDNs as an account holder after reading a news report that made numerous references to the OFAC designation, the bank did not take any action at that time to review or block the account.[52]

- ***Halliburton Atlantic Limited ("HAL") and Halliburton Overseas Limited ("HOL").*** HAL reached a $300,000 settlement with OFAC on behalf of itself and HOL for alleged violations of Cuba sanctions.[53] HAL and HOL provided oil and gas goods and services to a consortium that had interests in an Angola concession. A state-owned Cuban company, Cuba Petroleo ("Cupet"), is alleged to have owned a five percent interest in the consortium. OFAC alleged that in providing goods and services within the concession for the benefit of the consortium, HAL and HOL were providing a benefit to Cuba. OFAC took the view that the companies knew or should have known of Cupet's interest in the consortium, and acted with reckless disregard by failing to conduct reasonable due diligence.

  This enforcement action, involving an attenuated connection to Cuba, is instructive for financial institutions, showing the importance of thorough due diligence in connection with financings and other transactions even when they do not appear to involve sanctioned countries.

- ***B Whale Corporation.*** In OFAC's first enforcement action under the Trump Administration, on February 3, 2017, OFAC issued a Finding of Violation to B Whale Corporation ("BWC"), a Taiwan-based shipping company, for allegedly transferring, in late 2013, over 2 million barrels of crude oil to its vessel (the M/V B Whale) from the Iranian vessel M/T Nainital, which was an SDN at the time.

  This enforcement action is notable due to its broad finding of jurisdiction. In June 2013, BWC entered into federal bankruptcy proceedings in Texas. OFAC determined that BWC was a U.S. person because it was present in the U.S. for bankruptcy proceedings at the time of the oil transfer. Additionally, OFAC determined that BWC's vessel was property under the jurisdiction of the bankruptcy court and thus subject to OFAC regulations, and, therefore, the oil transferred to it from the Nainital qualified as an importation from Iran to the United States as defined under the Iranian sanctions regulations.[54]

Treasury's Financial Crimes Enforcement Network

With the publication of the Panama Papers, 2016 brought renewed—if not unprecedented—attention to the challenges posed by global money laundering and shell companies. Among other things, the Panama Papers gave added urgency to FinCEN's multi-year rulemaking under the Bank Secrecy Act on customer due diligence ("CDD") and beneficial ownership, which was finalized in May 2016. FinCEN also made expanded use of its Geographic Targeting Order authority to collect information about shell company activity involving luxury real estate. On the enforcement front, last month's multi-agency resolution with Western Union for $586 million represented the largest AML penalty over the last year.

- ***The Panama Papers***. On April 3, 2016, journalists broke the story of approximately 11.5 million leaked documents from the Panamanian law firm Mossack Fonseca relating to hundreds of thousands of offshore entities.[55] Journalists associated with the International Consortium of Investigative Journalists ("ICIJ") wrote articles linking some of these offshore entities to fraud, tax evasion, and other illegal activities; the ICIJ also created a searchable database of information extracted from the documents. The fallout from the Panama Papers has been widespread, causing embarrassment to public officials in several countries and generating a flurry of investigative activity across the globe, including by authorities in Australia, Austria, Belgium, Costa Rica, France, India, Mexico, Norway, Panama, Spain, Sweden and the United Kingdom.[56]

  In the United States, Southern District of New York U.S. Attorney Preet Bharara quickly announced a criminal investigation.[57] DFS reportedly ordered seventeen banks to provide information on their dealings or contact with Mossack Fonseca.[58] Several months later, in August 2016, DFS imposed a $180 million penalty on Taiwan's Mega Bank and its New York branch (discussed below) based, in part, on alleged suspicious transactions with its Panamanian branch that appear to involve corporate entities formed by Mossack Fonseca.[59]

  As noted, FinCEN used the Panama Papers to highlight the importance of its CDD regulation, which it finalized in May 2016. At the same time, the Treasury and Justice Departments announced they would send new legislation to Congress. The Treasury proposal would require, among other things, all U.S. companies, at the time of formation, to file beneficial ownership information with Treasury.[60]

  Pro-reform groups have used the Panama Papers to urge FinCEN to finalize its long proposed rule seeking to close what they describe as a "major, decade-old gap" by extending BSA/AML requirements to registered investment advisors.[61] Relatedly, in December 2016, the Financial Action Task Force ("FATF") released its evaluation of the AML regulatory framework in the United States, finding that it has "some significant gaps, including minimal coverage of certain institutions and businesses [including] investment advisers (IAs), lawyers, accountants, real estate agents, trust and company service providers."[62] Thus, the Panama Papers seem poised to be a potential driver of new regulation and investigative activity for some time to come.

- ***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.[63] Banks and other covered financial institutions[64] are already in the process of implementing this rule, and compliance is required by May 11, 2018. The rule has two components:

    1. 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.

    2. The rule also 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).

  These requirements mark the most significant addition to the BSA/AML regime in recent years and better align the United States with international standards. They also pose meaningful resource and compliance difficulties for covered financial institutions. While covered banks have likely already been engaged in some version of the due diligence required by the rule, the rule adds various requirements that may require revisions to existing procedures; the rule also contains some vague, open-ended aspects. For example, while the collection of beneficial ownership information is only required for new accounts opened on or after May 11, 2018, FinCEN has emphasized in the preamble to the rule that the CDD requirement will require covered institutions to obtain beneficial ownership information on *existing* customers on a risk-based, event-driven basis. Similarly, FinCEN has indicated that it may expect financial institutions in certain risk-based circumstances to set a lower threshold than 25 percent for the collection of beneficial ownership information. The fact that FinCEN has grounded these expectations in a regulation that will be interpreted and applied by numerous agencies heightens the risk that institutions may find themselves behind the rising curve of regulatory expectations in this area.

- ***Geographic Targeting Orders ("GTOs").*** As described in a previous Paul, Weiss memorandum,[65] FinCEN used its GTO authority over the last year to require title insurers to collect and report beneficial ownership information on legal entities making cash purchases of high-end residential real estate in various U.S. cities. These actions were motivated by FinCEN's concerns that shell companies were being used to hide the use of luxury real estate for money laundering purposes. While FinCEN began by targeting only Manhattan and Miami, on July 27, 2016, FinCEN expanded the initiative to Los Angeles, San Francisco, San Diego, all boroughs of New York City, and Broward and Palm Beach counties.[66]

- ***Enforcement Action Against Western Union.*** On January 19, 2017, Western Union agreed to a forfeiture of $586 million to resolve AML and fraud investigations by the DOJ and various U.S. Attorneys' offices, FinCEN, and the Federal Trade Commission.[67] The DOJ resolution included a deferred prosecution agreement in which Western Union admitted to failing to implement and maintain an effective AML program and aiding and abetting wire fraud.[68] FinCEN assessed a $184 million penalty, which was deemed satisfied by the forfeiture.[69]

  The government alleged that, from 2004 to 2012, Western Union processed hundreds of thousands of transactions as part of what the DOJ described as an "international consumer fraud scheme," in which numerous Western Union agents were complicit.[70] Among the AML program failings alleged by FinCEN were Western Union's supposed failure to conduct adequate due diligence on its agents, such as by approving "new agents" that in fact were owned by persons who were previously terminated because of AML concerns.[71] The government also asserted that Western Union failed to terminate or suspend high-risk agents, and, while it identified needed policies and procedures, it failed to implement them for years.[72] The government further claimed that Western Union delayed filing suspicious activity reports ("SARs") and frequently failed to file SARs on its agents (as opposed to the agents' customers).[73]

  Although reached on the last day of the Obama Administration, this resolution is notable in showing the persistence of multi-agency civil and criminal investigations in the financial crimes space. It also demonstrates the agencies' continued focus on what they called a "flawed corporate culture" and a "failure of a culture of compliance," which they contend permitted the ignoring of mounting red flags over a span of years.

- ***Gibraltar Enforcement Action.*** Last year, FinCEN issued a series of enforcement actions in different industries, but the most notable action involving banks was its $1.5 million settlement with Gibraltar Private Bank and Trust Company for purportedly failing to file at least 120 SARs. This alleged failure is said to have allowed for a $1.2 billion Ponzi scheme to be perpetuated through the bank. The FinCEN order followed a consent order by the OCC, which had imposed a $2.5 million penalty.[74]

- ***Thomas Haider Litigation.*** The DOJ continues its litigation to enforce FinCEN's landmark $1 million penalty against Mr. Haider, the former chief compliance officer of MoneyGram, for asserted AML violations. As described in a prior publication,[75] this penalty exemplifies the focus on individual accountability in the AML area.

Department of Justice

An important question regarding DOJ enforcement in the sanctions/AML area is whether Attorney General Jeff Sessions will be willing, as his recent predecessors were, to pursue guilty pleas from financial institutions, despite the potential collateral consequences. Another question is whether he will decide to retain the Yates Memorandum[76] policy of emphasizing the prosecution of individuals responsible for corporate wrongdoing and requiring corporations to assist with these efforts. Attorney General Sessions made a strong statement about white collar criminal prosecutions in his confirmation hearing:

"Corporations are subject as an entity to fines and punishment for violating the law and so are the corporate officers. And sometimes, it seems to me . . . that the corporate officers who caused a problem should be subjected to more severe punishment than the stockholders of the company who didn't know anything about it."[77] It is too soon, of course, to know how this principle will be applied in practice.

In addition to leadership changes at Main Justice, there will be substantial turnover among U.S. Attorneys throughout the country. It has been reported, however, that Preet Bharara, who obtained a landmark sanctions guilty plea from BNP Paribas S.A., will remain the U.S. Attorney for the Southern District of New York.[78]

With respect to DOJ's enforcement activity over the last year, other than the Western Union matter described above, there were no significant enforcement actions involving sanctions/AML violations. In 2016, however, the DOJ issued guidance identifying criminal sanctions and export violations as a priority and encouraging self-disclosure. The DOJ also pursued a notable sanctions prosecution against an individual. In addition, the DOJ continues to litigate then-Judge John Gleeson's order releasing large portions of the HSBC monitor's report, a ruling that may impact other financial institutions that enter deferred prosecution agreements. We also discuss DOJ's $1 billion forfeiture action in connection with investigations of corruption at 1Malaysia Development Berhad ("1MDB"), a Malaysian sovereign wealth fund.

- ***Guidance on Voluntary Self-Disclosure of Sanctions/Export Violations.*** On October 2, 2016, the DOJ's National Security Division ("NSD") issued guidance announcing the high priority it places on sanctions and export violations.[79] An application of the Yates Memorandum, the guidance emphasizes that, for willful violations, the NSD is committed to holding companies criminally liable and to prosecuting culpable employees individually.[80]

  In a break from past practice, the guidance states that self-disclosure to the relevant regulatory agency (*e.g.*, OFAC, BIS, the State Department) is insufficient. Instead, if a violation may have been "willful" (*i.e.*, done with knowledge of illegality), a self-disclosure must also be made to the DOJ. This guidance may reflect the DOJ's desire to be more actively involved in these matters from their inception—and perhaps may also reflect a Justice Department view that it has not received sufficient referrals from the regulatory agencies.

  Notably, a footnote in the guidance states that it does not apply to financial institutions because of their unique reporting obligations, although the guidance encourages financial institutions nevertheless to self-disclose to the DOJ, noting that they "may benefit" from such disclosures. In our view, the guidance may result in increased reporting to the DOJ, which in turn could lead to further investigations of financial institutions suspected of having facilitated the transactions in question.

- ***Sanctions Prosecution of Reza Zarrab.*** In March 2016, the U.S. Attorney's Office for the Southern District of New York brought criminal charges against Reza Zarrab, alleging that Zarrab (a Turkish and Iranian national) and various co-conspirators made U.S. dollar payments on behalf of various Iranian

entities through a network of companies in Turkey and the U.A.E. Zarrab and his co-conspirators allegedly used these companies to hide the payments' Iranian origins, thus permitting the payments to clear through New York banks without being blocked.[81]

Zarrab was charged with defrauding OFAC by concealing the origin of the payments, defrauding the New York banks by causing them to unwittingly process these sanctioned transactions and risk sanctions penalties, and violating the primary sanctions statute, the International Emergency Economic Powers Act ("IEEPA"). Zarrab moved to dismiss the complaint, arguing, among other things, that transactions outside the United States between non-U.S. persons did not come within the reach of IEEPA, notwithstanding incidental dollar clearing at New York banks. The government countered, in part, that even if Zarrab was not a "U.S. person" under IEEPA, that statute also extends to "U.S. property" and Zarrab knowingly initiated transactions that would cause banks in the United States to clear payments, which were "U.S. property." The district court denied the motion to dismiss, finding that the government sufficiently alleged that Zarrab's conduct had a "domestic nexus," that IEEPA could reach the conduct in question, and that Zarrab exported financial services from the United States to Iran.[82]

This prosecution is notable for at least two reasons. First, it has forced the federal government to articulate its views on U.S. dollar clearing and IEEPA jurisdiction with more detail than it had previously done. Second, the government's position has cast the affected New York banks as victims of criminal fraud, rather than as perpetrators of strict liability sanctions offenses.

- ***Public Disclosure of Monitor Reports Under Deferred Prosecution Agreements.*** As discussed in a prior Paul, Weiss memorandum,[83] on January 28, 2016, then-U.S. District Judge John Gleeson ordered the unsealing of large portions of a report by the compliance monitor appointed as part of HSBC's 2012 deferred prosecution agreement with the DOJ. The court held that the First Amendment right of access to judicial documents outweighed the concerns cited by HSBC, the monitor, the DOJ, and foreign regulators. These concerns included that public release, even with redactions, would impair the work of the monitor and undermine foreign regulator cooperation that was premised on confidentiality. After ruling on proposed redactions, the court stayed the disclosure of the report pending appeal to the U.S. Court of Appeals for the Second Circuit.[84] Oral argument is scheduled for March 1, 2017.[85] The Second Circuit's resolution of this issue may impact DOJ, regulators, and financial institutions' understanding of the benefits and risks of deferred prosecution agreements in the sanctions/AML area.

- ***1MDB Investigation.*** In its largest forfeiture action under its Kleptocracy Initiative to date, the DOJ announced in June of last year that it was seeking the forfeiture of more than $1 billion of assets—including real estate, private jets, and art—purchased with funds misappropriated from 1MDB, a Malaysian sovereign wealth fund.[86] According to the DOJ, corrupt officials and their associates allegedly used a "series of complex transactions and fraudulent shell companies" with bank accounts around the world to launder the funds and ultimately route them through the U.S. financial system to buy these assets. There have been reports of related investigations of banks, showing how anti-corruption investigations can lead to increased AML scrutiny of financial institutions.[87]

Federal Banking Agencies

Sanctions/AML compliance continues to be an area of intense focus by the federal banking agencies. For example, the Office of the Comptroller of the Currency ("OCC") has observed that AML risks "remain high," with innovations designed to improve product and service offerings also creating "vulnerabilities that can be exploited by criminals." The OCC has also noted challenges by banks in their ability to "maintain the level and quality of expertise" needed to successfully implement AML controls. At the same time, the agency will also be alert to and question de-risking strategies that "may inadvertently impair financial inclusion."[88]

With respect to enforcement actions, among the OCC, Federal Reserve Board of Governors, and the Federal Deposit Insurance Corporation, only the OCC issued penalties of $1 million or more against banks last year in this area. Both penalties were for AML violations: a $2.5 million penalty against Gibraltar Private Bank (discussed above) and a $1 million penalty against Stearns Bank.[89]

The Federal Reserve Board and the New York Federal Reserve ("NY Fed"), however, took several actions last year based on AML deficiencies that did not involve monetary penalties. These actions were similar in requiring reforms to banks' AML policies and procedures, but they differed in form and some required additional non-monetary remedies.[90] For example:

- The NY Fed and DFS jointly entered written agreements with the Industrial Bank of Korea and National Bank of Pakistan and their New York branches to reform their AML processes. The latter agreement also mandated a lookback and the hiring of a consultant.
- The Federal Reserve Board issued AML consent orders against Habib Bank and the Agricultural Bank of China ("ABC") and their New York branches, which required lookbacks and the hiring of consultants. As discussed below, DFS later imposed a penalty on ABC.
- The NY Fed recently announced a written AML agreement with South Korea-based NongHyup Bank. DFS did not join the agreement, although the agencies worked together on the underlying examination.

President Trump will be able to nominate a new Comptroller of the Currency and new FDIC Chairman when Comptroller Thomas Curry's and Chairman Martin Gruenberg's terms end, respectively, in April and November of this year.[91] In addition, Federal Reserve Board Governor Daniel Tarullo, who was a vocal supporter of aggressive oversight and a proponent of strong compliance cultures, has recently announced that he will resign, which will leave three vacancies on the Board—even before Chair Janet Yellen's term expires in February of next year.[92] It is possible that President Trump's appointees to fill these roles could take weaker approaches to oversight in the sanctions/AML area, but doing so would requiring reversing the considerable institutional momentum and examination culture at each agency.

Securities and Exchange Commission

The SEC brought one AML enforcement action last year, reaching a $1 million settlement with broker-dealer E.S. Financial Services in connection with a brokerage account it maintained for an unidentified Central American bank.[93] According to the SEC, 23 non-U.S. citizens beneficially owned legal entities that maintained accounts with the Central American bank. Although these individuals interfaced directly with the broker-dealer, the company allegedly failed to perform appropriate customer identification procedures ("CIP") on these individuals for ten years until 2013.

The SEC's Office of Compliance Inspections and Examinations ("OCIE") lists money laundering and terrorist financing among its 2017 examination priorities.[94] OCIE is interested, among other things, in whether broker-dealers' AML programs are tailored to firms' specific risks, the functioning of the SAR process, and the effectiveness of independent testing.

Financial Industry Regulatory Authority

2016 continued to show the increasing focus by FINRA on broker-dealer AML enforcement:

- ***Raymond James.*** FINRA reached a $17 million settlement—its largest ever for AML compliance deficiencies—with Raymond James & Associates, Inc., and Raymond James Financial Services, Inc. ("Raymond James").[95] FINRA asserted that Raymond James' AML systems were not designed to handle the companies' growth, which forced them to rely upon a "patchwork" of procedures and systems across various departments to detect suspicious activity. FINRA also fined a former Raymond James AML compliance officer $25,000 and suspended her for three months.

- ***Credit Suisse Securities.*** FINRA reached a $16.5 million settlement with Credit Suisse Securities for purported deficiencies in its suspicious activity monitoring program between 2011 and 2015.[96] FINRA alleged that Credit Suisse's monitoring program failed to escalate and investigate high-risk activity and that the company's automated surveillance system for suspicious activity was not properly implemented, including "by failing to ensure that the data that was being fed into the system was adequate and by failing to utilize available scenarios that were applicable to the money-laundering risks presented by its business." FINRA also claimed that the company failed to devote adequate resources to resolving some of these deficiencies in a timely fashion and that the company had inadequate staffing to review the tens of thousands of alerts generated each year.[97]

- ***Citi International Financial Services ("CIFS").*** FINRA reached a $5.75 million settlement with CIFS in connection with alleged AML deficiencies involving foreign exchange transactions.[98] FINRA claimed that, between 2011 and 2013, CIFS processed securities transactions involving conversion between U.S. dollars and foreign currency, but lacked adequate AML monitoring systems and training commensurate with this increased money laundering risk.

FINRA identified AML as one of its top priorities in its 2016 Regulatory and Examination Priorities Letter, advising firms to "routinely test systems and verify the accuracy of data sources to ensure that all types of customer accounts and customer activity, particularly higher-risk accounts and activity, are properly identified and reviewed in a manner to detect and report potentially suspicious activity."[99]

In its 2017 priorities letter, FINRA stated that it intends to continue to address shortcomings in broker-dealers' AML programs, including "gaps in firms' automated trading and money movement surveillance systems caused by data integrity problems, poorly set parameters or surveillance patterns that do not capture problematic behavior such as suspicious microcap activity."[100]

New York Department of Financial Services

If 2016 is any indication, DFS will remain at the forefront of regulatory and enforcement activity in the sanctions/AML space for the foreseeable future. As noted, the regulator appears primed to potentially assume an even more active role during the Trump Administration. Underscoring this point, early this year, New York Governor Andrew Cuomo proposed legislation that would expand DFS's authority, including by empowering it to ban industry "bad actors" who commit certain forms of misconduct,[101] a proposal that has engendered some controversy in Albany.[102]

Below we discuss DFS's AML/sanctions rule and the agency's major enforcement actions over the last year.

- ***Part 504 Regulation on AML/Sanctions Programs.*** As described in a prior Paul, Weiss memorandum, on July 1, 2016, following soon after Maria Vullo's confirmation as Superintendent, DFS finalized a regulation, Part 504, that imposes transaction monitoring and sanctions filtering program requirements on DFS-regulated banks and branches.[103] According to DFS, the regulation was motivated by the agency's identification of monitoring and filtering deficiencies at multiple institutions attributable to a "lack of robust governance, oversight, and accountability at senior levels."[104]

  In previewing the rulemaking, then-Superintendent Benjamin Lawsky noted in a speech that deficiencies in transaction monitoring and filtering systems can result from "inadequate or defective design, or programming of the monitoring and filtering systems, faulty data input, or a failure to regularly update these detection scenarios, which may be attributed to lack of sophistication, knowledge, expertise, or attention by the management and/or employees."[105] He stated that a "whack-a-mole approach" using enforcement actions was insufficient because "we believe that there are likely widespread problems with transaction monitoring and filtering systems throughout the industry."

  The regulation went into effect on January 1, 2017. It has three main sets of requirements:

  1. The regulation requires that the transaction monitoring and sanctions filtering programs of the regulated institution (*e.g.*, a DFS-regulated New York branch) be "reasonably designed" and meet thirteen requirements, many of which are broadly worded. For example, the

regulation requires "end-to-end, pre- and post-implementation testing of the Transaction Monitoring Program," including, as relevant, a review of "governance, data mapping, transaction coding, detection scenario logic, model validation, data input and Program output."[106]

2. The regulation also contains eight requirements that apply to both programs, including "identification of all data sources that contain relevant data," and "validation of the integrity, accuracy and quality of data to ensure that accurate and complete data flows through" the filtering and monitoring programs. Other requirements relate to governance and management oversight, adequate funding, qualified personnel, training, and vendor selection.[107]

3. The regulation requires that either the Board of Directors or one or more Senior Officer(s) of the DFS-regulated institution annually certify compliance with the regulation. The first such certification is due April 15, 2018, which would cover the year ending 2017. Certifiers must affirm that they have taken "all steps necessary to confirm" that their institution's programs comply with the regulation and then certify to the best of their knowledge that the programs so comply. In finalizing the regulation, DFS noted that "[i]t is the Department's intent that this new certification requirement will cause the Board of Directors or Senior Officers to proactively ensure compliance." DFS further explained that, in light of comments it received, it was omitting language from the proposal that referred to potential criminal penalties for incorrect or false certifications. But DFS went on to note that if a bank's compliance program "is not reasonably designed and if the compliance finding is not based on a review of necessary documents and materials, the certifying individual(s) may appropriately be subject to the Superintendent's civil enforcement powers and, if the compliance finding was made with the intent to deceive, to criminal penalties."[108]

As discussed at a recent panel co-hosted by Paul, Weiss and Ernst & Young, the regulation's substantive requirements were intended by DFS to be consistent with federal sanctions/AML expectations.[109] But unlike at the federal level, DFS has now attempted to codify these expectations in a regulation using broadly worded language, which over time can be taken in more expansive directions by the agency. In this regard, one of the many challenges that New York branches of global banks face in implementing the regulation is identifying an appropriate scope for some of the regulation's requirements. For example, what is the scope of the data feeds that need to be validated? How broadly does an "enterprise-wide" risk assessment sweep?

Another set of challenges involves identifying who will perform the annual certifications and designing a well-documented process—whether involving sub-certifications or some other approach—that will produce the necessary materials and data to support the certification. Institutions will also need to decide how to handle certifications when there are material weaknesses that regulators or the institutions

themselves have identified. Interpreting and implementing Part 504 will be a top challenge this year for DFS-regulated institutions.

- ***Enforcement Actions Against Mega Bank, ABC, and Intesa.*** Following Maria Vullo's confirmation as Superintendent on June 15, 2016, DFS issued three notable consent orders last year against the following non-U.S. banks and their New York branches: Taiwan-based Mega International Commercial Bank ("Mega Bank"), ABC,[110] and Italy-based Intesa Sanpaolo ("Intesa"). In each order, DFS imposed a fine ($180 million, $215 million, and $235 million, respectively), required a sanctions/AML lookback, and required or extended a consultant or monitor. The orders mainly focus on AML issues, although they include sanctions components as well.[111]

  The Mega Bank, ABC, and Intesa orders have certain themes in common, which likely presage future DFS enforcement activity:

  1. DFS has emphasized senior accountability for sanctions/AML compliance. One of the consent orders begins with several paragraphs on the subject, including the passage below. Notably, however, none of the orders requires dismissals of managers or other employees.

     > "The ultimate responsibility for the design and implementation of these policies and systems belongs at the very top echelon of the institution. The board of directors and senior management must devote careful study to the design of the anti-money laundering and other compliance systems that lie at the core of this first line of defense. They must provide sufficient resources to undergird these systems and structures, including appropriate and evolving technology where cost effective. Adequate staffing must be put in place, and training must be ongoing. . . . When there is a material failure in a compliance program—in its structure, implementation, execution or policing—senior management must bear responsibility."[112]

  2. In these orders, DFS has demonstrated a willingness to put substantial weight on compliance deficiencies, rather than specific violative transactions, as grounds for sizable penalties. In one sense, these actions preview the kinds of actions that may be expected for violation of the program and procedural requirements of the new Part 504 regulation. For example, one or more of the orders cited the following purported deficiencies at the banks' respective New York branches:

     - A conflict of interest in the compliance program, in which one official had both business and compliance duties, as well as other deficiencies relating to compliance personnel continuity and expertise;

     - Failure to conduct appropriate due diligence on affiliated branches and their correspondent banking activities at the New York branch;

- Clearing transaction monitoring alerts without putting them into a central case management system as required by bank policy;
- Failure to conduct sufficient AML and sanctions risk assessments;
- Failure to periodically review transaction monitoring criteria and thresholds, as well as improperly configured transaction monitoring rules and the failure to update high risk jurisdiction ratings;
- Programming errors in the transaction monitoring system;
- Inadequate compliance oversight by the bank's Head Office;
- Inadequate internal audit function with respect to AML compliance; and
- Failure to follow through on remediation commitments made to DFS.

3. Relatedly, the consent orders are sometimes vague when they discuss potentially suspicious transactions or allegedly illegal underlying conduct, and it is unclear whether DFS found that the institutions failed to file required SARs.[113] And, notably, in two of the orders DFS explicitly stated that it "may undertake additional action" against each institution depending upon the results of the required sanctions/AML lookbacks.[114]

- ***Enforcement Action Against Deutsche Bank.*** On January 30, 2017, DFS issued a consent order against Deutsche Bank and its New York branch, 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.[115] The 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."[116] 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. (The U.K. Financial Conduct Authority concurrently issued a consent order against the bank imposing a penalty of £163 million.)

  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.

The 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 Anti-Terrorism Act: Private Litigation Risks Related to Sanctions/AML Enforcement

Financial institutions should continue to bear in mind the potential private litigation consequences of sanctions/AML enforcement. Over the last several years, there have been increasing lawsuits against financial institutions and other companies under the Anti-Terrorism Act ("ATA"), which provides U.S. nationals a private right of action and treble damages for injuries caused by acts of international terrorism.[117]

For example, in the most prominent ATA case in recent years, *Linde* v. *Arab Bank*, plaintiffs alleged that Arab Bank, Jordan's largest bank, knowingly provided banking services to Hamas and another terrorism-related organization. During discovery, Arab Bank withheld the production of certain customer account records after unsuccessfully seeking waivers from the bank secrecy laws of Jordan, Lebanon, and the Palestinian Territories. The district court responded by imposing discovery sanctions on Arab Bank, including a jury instruction that would permit the jury to infer that Arab Bank knowingly provided the alleged banking services.[118] The court questioned Arab Bank's good faith because, among other things, the bank had provided some of the contested documents to U.S. regulators as part of their investigations. After unsuccessful attempts to have the Second Circuit and Supreme Court reverse the discovery sanctions (in which the United States belatedly filed a brief criticizing the imposition of those sanctions),[119] the case went to trial in 2014 and the jury found Arab Bank liable. In May 2016, the court accepted a settlement for an undisclosed sum that reserved Arab Bank's ability to appeal the liability verdict.[120] The case stands as a sobering example of the liability that global banks face at the intersection of U.S. financial crimes laws and non-U.S. bank secrecy and privacy laws.

Over the past year, ATA litigation has taken a more expansive turn. For the first time in the statute's history, plaintiffs have alleged that crimes committed by drug cartels should be considered acts of international terrorism under the ATA.[121] The lawsuit, *Zapata* v. *HSBC*, filed in the Southern District of Texas, alleges that the bank intentionally and/or knowingly provided material support and financing to the drug cartels responsible for plaintiffs' injuries by maintaining accounts, processing funds, and failing to implement AML controls to detect, investigate and prevent such activity.

The lawsuit demonstrates the risk of follow-on litigation relating to sanctions/AML enforcement actions. Indeed, the *Zapata* complaint mines the bank's enforcement history and particularly the stipulation of facts accompanying its 2012 DOJ resolution. The risk of ATA litigation thus stands as a further reason that financial institutions must remain vigilant about admissions or other statements made in the enforcement context.

Suggestions for Strengthening Sanctions/AML Compliance

In light of the developments described above, we offer the following suggestions to senior management, general counsel, and compliance officers for further strengthening their institutions' sanctions/AML posture. Many of these suggestions have been abiding themes, but should nevertheless be revisited.

1. ***Exercise increased caution in light of a changed administration.*** Compounding the normal uncertainty that accompanies a change in administration is the fact that this transition follows so closely on the heels of major changes in a large number of sanctions programs. Moreover, at any moment, President Trump—who has stated that "we must as a nation be more unpredictable"—could make sudden and unexpected changes to the sanctions policies of the last administration. For example, it is possible that the new administration could act to roll back Russia-Ukraine sanctions. Additionally, President Trump has discussed terminating or renegotiating the Iran nuclear deal. And, insofar as the Iran deal stays intact, it is likely that the new administration will narrowly apply it when it comes to questions of compliance or licensing; as a result, financial institutions may want to operate conservatively when it comes to the many vagaries of interpreting the Joint Comprehensive Plan of Action ("JCPOA"), General License H, and other aspects of Iran sanctions relief.

All of this uncertainty argues for increased caution in compliance judgments and day-to-day vigilance to ensure a swift, institution-wide response to changes in U.S. sanctions policy.

2. ***Bolster tone at the top and the culture of compliance.*** This has been a prominent theme for many years, but its importance has only increased. As illustrated above, regulators (and monitors) continue to show profound interest in the tone and level of engagement of top management and the board of directors with respect to sanctions/AML compliance. For DFS-regulated institutions in particular, this message could not be clearer. A regulator or monitor's overall impression of an institution's tone at the top and compliance mindset can lead to significant differences in enforcement consequences in the event that violations are identified. The tone/culture question can be framed in many ways. For example, U.S. Attorney Preet Bharara asks whether an institution suffers from a culture of "minimalism" (*i.e.*, aspiring to the minimum necessary to be in compliance) and/or "formalism" (*i.e.*, focusing on the letter of the rules without also focusing on integrity and broader values).[122] Also, is the corporate culture one where "dissent is openly permitted, candor is duly fostered, and integrity is cultivated and even rewarded"?

For non-U.S. financial institutions, regulators are also particularly interested in whether the senior management at an institution's headquarters has embraced the institution's U.S. sanctions/AML compliance obligations, actively oversees these efforts, and provides the compliance function with adequate authority and funding.

With respect to the compliance function itself, regulators and monitors increasingly try to gauge whether the function displays a proactive, critical mindset versus a more passive and box-checking approach. For example, DFS criticized one bank's KYC approach for focusing on what documentation was collected at the expense of "shining a critical light on information provided by potential customers."[123] One indicator

of a bank's compliance mindset is how it reacts when it finds a problem. For example, when a transaction monitoring programming issue is found, does compliance proactively check whether the issue also occurs in other systems or other regions? How quickly does compliance move to do so and to inform senior ranks of the issue? Even if one's institution has taken significant steps in the area of compliance culture, we suggest asking what else can be done in 2017.

3. *Focus on data integrity, systems and programming issues.* As the wire-stripping cases course out of the system, regulators will turn to a next generation of enforcement matters. One of these types of cases may involve systems flaws that impair the quality of data flowing into the institution's sanctions screening and transaction monitoring systems. For example, DFS's new regulation places a considerable emphasis on "data integrity" and validating the "accuracy" and "completeness" of data flows. FINRA too has identified "data integrity problems" in describing the AML issues on which it is focused. Data issues are reportedly common in the financial industry, particularly in larger institutions that combine multiple legacy systems.[124] Other systems issues that regulators may increasingly focus on include flaws in programming or mapping within the filtering or monitoring software itself. Compliance, systems and audit professionals must continually evaluate whether what they think their systems scan matches the reality; testing can play an important role in this context. Financial institutions may wish to renew their focus on these data integrity and other systems issues—and think about them globally across the institution—to stay ahead of regulatory scrutiny.

4. *Further prepare for enforcement focused on compliance deficiencies rather than specific violative transactions.* As discussed above, DFS's actions against Mega Bank, ABC, and Intesa may indicate a trend in DFS enforcement in which sizable penalties are based on holistic reviews of AML (and, to a lesser extent, sanctions) compliance programs and governance structures and are less tethered to specific violative transactions. DFS may then require lookbacks and pursue further enforcement action depending on the results. Indeed, if the wire-stripping cases are nearing their completion, other regulators in addition to DFS may find themselves giving greater attention to compliance program flaws. This points to the need for financial institutions to ensure that they have not only established the key components of sanctions/AML compliance programs—including robust risk assessments, strong KYC processes, well-tested filtering and monitoring systems, sufficient personnel for managing alerts and investigations, and a strong audit function—but that they continually seek to strengthen and expand these components, on a global basis, to keep up with regulators' ever rising expectations.

Among other measures, financial institutions should ensure that they have an effective approach for evaluating new enforcement actions and assessing whether they indicate any room for improvement. As one regulator put it, it is "compliance malpractice" to fail to heed the warnings of other enforcement actions.[125] In addition, institutions not regulated by DFS might consider using the Part 504 regulation as an instructive checklist.

5. *Bolster customer due diligence and daily customer screening across the institution.* The main theme of OFAC's financial institution cases last year was the failure to identify the prohibited status of certain customers, often despite the fact that such information was within the institution's possession or readily accessible. The reasons for these problems included weak procedures, inadequate information sharing across an institution's branches, and systems misconfigurations. Financial institutions should continue to bolster their KYC and CDD efforts, even beyond the changes that will be needed to implement FinCEN's new regulation. Institutions should also strengthen their screening of customers. And, as evidenced by DFS's consent order with 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.

6. *Strengthen due diligence on non-U.S. branches and other affiliates.* Since at least HSBC's December 2012 deferred prosecution agreement, it has been known that regulators expect banks to conduct due diligence on their non-U.S. branches and other affiliates as though they were unaffiliated banks. DFS's consent order with Mega Bank addressed this issue, citing the New York branch for its supposed failure to (1) determine whether its foreign affiliates had in place adequate AML processes and controls, (2) ensure that it had an understanding of the effectiveness of the AML regimes of the jurisdictions in which its affiliates' customers operate, and (3) follow up on account activity that did not fit the "foreign affiliates' customers' strategic profile."[126] It is sometimes institutionally difficult for a U.S. branch to think of or treat other branches (much less the head office) in this manner, but regulators will generally expect to see thorough diligence, including a well-documented review of the non-U.S. branch's compliance systems, products, customer types, and other risk factors.

Last year, the federal banking agencies, OFAC, and FinCEN released a "fact sheet" that summarizes federal expectations regarding banks' diligence on foreign correspondent banks; a similar approach should be taken to a bank's own affiliates.[127] Although the fact sheet was meant to reassure industry and discourage de-risking, it nevertheless highlights the high and somewhat open-ended nature of the expectations in this area, including with respect to the obligation to conduct diligence on a correspondent's customers.

Recent Developments and Trends in Cybersecurity

Cybersecurity continues to be among the most important and fastest growing governance and regulatory concerns for financial institutions and their boards of directors, senior management and general counsel. This emphasis was only reinforced by the many high-profile cyber events last year, including the Russian hacking of Democratic National Committee emails, the $80 million cyber theft from the Bangladesh Central Bank's account at the NY Fed, Yahoo's disclosure that more than 1 billion accounts had been hacked in 2013, the continued cyberattacks against the SWIFT network, and the hacking and publication of the Panama Papers.[128] The OCC has reported that the severity of cyber threats is increasing and, among

other things, has pointed to the success of cyber extortion campaigns and their increasing use by cyber criminals.[129]

The last year has seen significant cybersecurity regulatory developments, which are still unfolding. Most notably, on February 17, 2017, DFS issued a final cybersecurity regulation that is the first of its kind. Last fall, the federal banking agencies also initiated a process to establish "enhanced" cybersecurity standards. The issuance of cybersecurity regulations can be seen as a harbinger of increased examination attention and, potentially, enforcement actions. With increasingly detailed cybersecurity regulatory requirements, financial institutions may find that they have less ability to be seen as the victims of cybercrime than as objects of regulatory criticism and enforcement.

As discussed below, the SEC, CFTC, and CFPB also took cyber-related regulatory or enforcement actions last year, evidencing a financial-sector wide focus on this area. FinCEN also issued guidance on the filing of SARs involving cyber incidents.

DFS Cybersecurity Rulemaking

On September 13, 2016, DFS proposed a new regulation that would require covered financial institutions to establish and maintain cybersecurity programs that satisfy certain requirements. The regulation was proposed following a survey by DFS of the cybersecurity practices of some 200 regulated banking institutions and insurance companies, as well as discussions with cybersecurity experts on emerging trends and risks. The proposal covered banks, insurance companies, and other financial services institutions regulated by DFS, with certain exceptions for smaller institutions.[130] A prior Paul, Weiss memorandum describes the proposal in more detail.[131]

On December 28, 2016, after receiving over 150 comments, DFS issued a revised proposed regulation for additional comment.[132] The new proposal clarified terms, relaxed certain requirements, and delayed the proposed effective date from January 1, 2017 to March 1, 2017, with a transition period of 180 days (or up to two years for certain provisions).

On February 16, 2017, DFS issued the final regulation, which was substantially unchanged from the revised proposal.[133] As previously planned, it will become effective upon publication in the New York State Register on March 1, 2017.

The regulation will require covered institutions to implement and maintain a "cybersecurity program" and a "cyber security policy," which address information and systems security, access controls, disaster recovery plans, customer data privacy, risk assessments, and incident response, among other elements. The regulation will also require the designation of a Chief Information Security Officer ("CISO"), regular penetration testing and retention of audit trails, employee training, and multi-factor authentication in certain situations. A covered entity will have to "assess its specific risk profile and design a program that addresses its risk in a robust fashion."

As with DFS's sanctions/AML regulation, the cybersecurity rule will require the Board of Directors or one or more Senior Officer(s) to file an annual certification with DFS regarding compliance with the regulation.

Notably, the regulation will also require covered entities to give notice to DFS within 72 hours of any "cybersecurity events" (1) impacting the covered entity, of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body, or (2) that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity. The rule defines "cybersecurity event" also to include unsuccessful attempts at network intrusions.

While many elements of the regulation are consistent with existing federal guidance, such as Federal Financial Institutions Examination Council ("FFIEC") guidance, other elements go beyond current expectations, such as the requirement that broadly defined "nonpublic information" must be encrypted both in transit and at rest—a potentially significant new burden. Implementing these new DFS requirements alongside the extensive federal regulatory guidance in this area is likely to prove costly and complex.

Federal Banking Agencies Begin Rulemaking Process on Enhanced Cybersecurity Standards

Approximately one month after DFS's proposal, on October 19, 2016, the Federal Reserve Board, the FDIC, and the OCC jointly issued an advance notice of proposed rulemaking seeking comment on a new set of enhanced cybersecurity standards for certain institutions under their supervision.[134]

As described in a prior Paul, Weiss memorandum,[135] the proposal would cover banks and bank holding companies (on an enterprise-wide basis, including subsidiaries) with total assets of $50 billion or more, U.S. operations of foreign banking organizations with total U.S. assets of $50 billion or more, financial market utilities and non-bank financial companies supervised by the Federal Reserve Board, and third party service providers, with respect to services provided to banks and their affiliates that are covered entities. The final standards may take the form of a policy statement or guidance or a "detailed regulation."

The enhanced standards aim to "increase the operational resilience" of covered entities and reduce the impact of a cyber event on the financial system by establishing enhanced cybersecurity practices in five areas: (1) cyber risk governance; (2) cyber risk management; (3) internal dependency management; (4) external dependency management; and (5) incident response, cyber resilience, and situational awareness. The enhanced standards would "emphasize the need for covered entities to demonstrate effective cyber risk governance; continuously monitor and manage their cyber risk within the risk appetite and tolerance levels approved by their boards of directors; establish and implement strategies for cyber resilience and business continuity in the event of a disruption; establish protocols for secure, immutable, transferable storage of critical records; and maintain continuing situational awareness of their operational status and

cybersecurity posture on an enterprise-wide basis." They would also direct entities to develop comprehensive recovery strategies with recovery time objectives ("RTOs").

The proposal reflects a two-tiered structure, with enhanced standards for covered entities and an even higher set of standards for an entity's "sector-critical systems"—that is, systems that are "critical to the functioning of the financial sector." Among other things, the sector-critical standards would require that covered entities establish an RTO of two hours for their sector-critical systems to recover from a cyber event.

It appears that if the federal agencies' efforts are eventually finalized, both the federal rules and DFS's regulation could apply simultaneously to most New York branches of non-U.S. banks with over $50 billion in U.S. assets, absent an accommodation by one of the regulators.

Other Financial Regulatory Actions

Other financial regulatory agencies increased their engagement in cybersecurity and data protection issues in 2016, including:

- ***SEC.*** On June 8, 2016, the SEC announced a $1 million settlement with Morgan Stanley Smith Barney LLC ("MSSB"), a registered broker-dealer and investment advisor, involving alleged failures to protect customer information.[136] The SEC claimed that MSSB failed to adopt written policies and procedures reasonably designed to protect customer data, as required by the SEC's safeguards rule (Regulation S-P). According to the SEC, as a result of these failures, an employee misappropriated data regarding approximately 730,000 accounts and transferred it to his personal server. The data was subsequently hacked by third parties and posted on the internet for sale.

  The settlement was among the first of its kind by the SEC, which had settled two safeguards rule matters for $75,000 and $100,000, respectively, in 2015 and 2016.[137] In addition, the SEC has again ranked cybersecurity, including testing and implementation of cybersecurity procedures and controls, among its examination priorities for 2017.[138]

- ***CFTC.*** On September 8, 2016, the CFTC adopted amendments to its system safeguards rules, which require designated contract markets, swap execution facilities, swap data repositories, and derivatives clearing organizations to maintain cybersecurity programs.[139] The amendments enhance and clarify existing requirements relating to cybersecurity testing and system safeguards risk analysis by defining five types of cybersecurity testing, including (1) vulnerability testing, (2) penetration testing, (3) controls testing, (4) security incident response plan testing, and (5) enterprise technology risk assessment. The amendments also provide minimum frequency requirements for testing.

  These regulations reflect then-CFTC Chairman Timothy Massad's observation that "[t]he risk of cyberattack probably represents the single greatest threat to the stability and integrity of our markets today."[140] Then-Commissioner (now Acting Chairman) Christopher Giancarlo similarly stated that "cyber

and system security" should be regulators' "first priority in time and attention."[141] At the same time, he also cautioned about excessive enforcement: "Market participants who abide by the [systems safeguards] rule should not be afraid of a 'double whammy' of a destructive cyber-attack followed shortly thereafter by a CFTC enforcement action. Being hacked, by itself, cannot be considered a rule violation subject to enforcement."

- ***CFPB.*** As described in a prior Paul, Weiss memorandum,[142] on March 2, 2016, the CFPB entered the cybersecurity arena for the first time with the issuance of a consent order against online payment platform Dwolla, Inc., for allegedly deceiving consumers about its data security practices.[143] Although there was no allegation of a data breach, the CFPB imposed relatively intrusive remedial requirements given the size of the company, including requiring it to retain an independent expert to annually conduct data-security audits for five years. The consent order also required the company to train employees and improve data security practices across a number of areas and pay a $100,000 penalty.

  The CFPB's action relied on its "unfair, deceptive, or abusive" ("UDAAP") authority and was in the mold of past Federal Trade Commission actions finding that companies committed "deceptive" acts by misrepresenting their data security practices. Notably, both the CFPB and the federal banking agencies have the authority to pursue "deceptive" acts by banks within their respective, and often overlapping, jurisdictions.

FinCEN Guidance on the Reporting of Cyber Incidents

In October 2016, FinCEN issued an advisory at the intersection of cybersecurity and AML. The advisory described financial institutions' obligations to file SARs in response to "cyber-events," which are defined as an attempt to compromise or gain unauthorized access to electronic systems.[144] Among other things, the advisory stated that if a financial institution suspects that a cyber event was intended "in whole or in part, to conduct, facilitate, or affect a transaction or a series of transactions," it should be considered reportable under the BSA. The advisory also stated that SARs should include available cyber-related information, whether related to cyber events or other activity such as fraudulent wire transfers. Cyber-related information should include IP addresses with timestamps, virtual-wallet information, device identifiers, and cyber-event information. According to FinCEN, the purpose of the advisory was to clarify existing obligations under the BSA and not to change BSA requirements or other regulatory obligations relating to the reporting of cyber incidents.

Suggestions for Strengthening Cybersecurity

1. ***Prepare for a tougher regulatory approach to cybersecurity, potentially including enforcement actions.*** Banks have thus far not experienced sizable regulatory penalties for cyber breaches. However, the focus by federal regulators and DFS on cybersecurity rulemaking portends tougher examinations in this area and, potentially, enforcement actions. As one NY Fed official said of the development of enhanced cybersecurity standards: "[O]ur goal for U.S. branches is to transform their response to cybersecurity challenges from ad hoc responses to *more clearly defined and articulated*

processes and standards. . . . U.S. supervisors are proposing *a more enforceable set of standards* that go beyond the guidelines we have offered to date."[145] Thus, as in the sanctions/AML area, banks and other financial institutions should increasingly prepare to be treated not as the victims of criminal conduct, but as objects of investigation for failure to maintain systems that could have, but failed to, thwart criminal activity. As discussed above, the SEC has already taken a step down this path, fining a firm $1 million for allegedly faulty systems security that allowed an employee to steal customer data.

Boards and senior management should thus continue to invest time and resources into bolstering cybersecurity and further integrating it into their institutions' overall compliance framework. Institutions that are or may become subject to DFS or federal banking agency cyber regulations should be prepared for probing examinations into risk assessments, clear and robust policies and procedures, governance, vendor management, testing, audit—and rigorous documentation of all of the above. Institutions that will not be subject to these regulations may wish to refer to these regulations for guidance to stay ahead of regulatory expectations. And, having a strong program in place is only the beginning—any cybersecurity program must be dynamic and must actively manage risk.

In bolstering their programs, institutions should also be mindful of the federal Cybersecurity Information Sharing Act of 2015 ("CISA"), which makes it easier to share cyber threat indicators and other helpful information with the federal government, state and local governments, and other companies and private entities. This law and related federal guidance is discussed in detail in a prior Paul, Weiss memorandum.[146]

2. *Review external policies and statements regarding data security.* CFPB's action against Dwolla signals the possibility that CFPB, or the federal banking agencies, could take similar actions under their "deceptive" authority against banks or other financial institutions, alleging that their policies or statements about their data security practices are false or misleading. Institutions that have not recently done so should comprehensively review all such policies and statements to ensure that the language used is accurate and defensible.

3. *Emphasize employee training.* Much that is involved in cybersecurity preparedness is technical in nature and is largely the province of IT professionals, but this should not lead to the neglect of more mundane efforts, such as constant employee communication and training on cybersecurity. Phishing attacks continue to be a prominent method of access into institutions' systems. Employee errors including mishandling passwords, using personal email, and misplacing laptops and other devices also contribute to institutions' cyber vulnerabilities. Training should also cover "business email compromise" schemes, in which criminals digitally impersonate executives and email internal accounting and human resource offices to obtain information to facilitate fraud and identity theft.[147] Finally, the SEC action against MSSB discussed above serves as a reminder that institutions also need to maintain a strong insider threat program.

4. *Clarify roles between U.S. branches and the bank's headquarters.* For non-U.S. banks, one issue that regulators have remarked on is the potential for unclear roles and divisions of responsibility

between the U.S. branch and headquarters with respect to information technology and cybersecurity.[148] For example, while headquarters auditors may be familiar with global systems that are present at the U.S. branch, they may be less familiar with U.S.-specific systems and thus may not review these systems or subject them to vulnerability testing. Financial institutions should define clear roles and responsibilities between the branch and head office and ensure that an outside audit function exists that can test U.S. systems.

5. *Continue to monitor the private litigation environment and bolster incident response planning.* From consumer class actions to derivative suits, financial institutions and other companies continue to face cyber-related litigation. It remains to be seen how successful these suits will be; many plaintiffs have run into standing and other hurdles. Financial institutions, however, should take notice of the Seventh Circuit's decision last year in *P.F. Chang's*,[149] which, following in the path of that court's *Neiman Marcus* decision,[150] found that customers had standing to sue following a data breach of credit and debit card numbers based on future injuries (the substantial risk that hackers would make fraudulent use of the information) and present injuries (including procuring identity theft monitoring services). While the Supreme Court's decision last year in *Spokeo, Inc.* v. *Robins*[151] may help block certain cybersecurity suits on standing grounds, it is still too soon to tell how courts will apply that decision.

The *P.F. Chang's* and *Niemen Marcus* decisions also illustrate how certain post-breach statements and actions by the affected companies can be relied upon by plaintiffs and courts to support standing. Companies in these situations have few good alternatives, but this nevertheless points to the importance of careful incident response planning and execution. We discuss the cybersecurity landscape, including private litigation and incident response planning, in more detail in a prior Paul, Weiss memorandum.[152]

* * *

We will continue to monitor sanctions, AML and cybersecurity 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
212-373-3061
cboehning@paulweiss.com

Susanna M. Buergel
212-373-3553
sbuergel@paulweiss.com

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

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

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

Jeh Charles Johnson
212-373-3093
jjohnson@paulweiss.com

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

Lorin L. Reisner
212-373-3250
lreisner@paulweiss.com

Richard C. Tarlowe
212-373-3035
rtarlowe@paulweiss.com

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

Associates Raj Borsellino, Evan J. Meyerson, Jeffrey Newton, Andrew D. Reich, Matthew J. Rosenbaum, Mary Anne Schlapprizzi, Kaveri Vaid, Sarah K. Weber, law clerks Kamil Ammari and Stephen Speirs contributed to this client alert.

[1] As former Treasury Secretary Jacob Lew stated—in remarks that also cautioned about the risks of sanctions overuse—sanctions "have become a powerful force in service of clear and coordinated foreign policy objectives—smart power for situations where diplomacy alone is insufficient, but military force is not the right response." Jacob Lew, Secretary, U.S. Dep't of the Treasury, Remarks of Secretary Lew on "The Evolution of Sanctions and Lessons for the Future" at the Carnegie Endowment for International Peace (Mar. 30, 2016), *available* here.

[2] *See* Paul, Weiss, *FCPA Enforcement and Anti-Corruption Developments: 2016 Year in Review* (Jan. 19, 2017), *available* here.

[3] Cory Bennett, *Trump: US Cyber Powers "So Obsolete,"* THE HILL (Mar. 28, 2016), *available* here.

[4] Jordan Fabian, *Trump Scraps Signing of Cybersecurity Executive Action*, THE HILL (Jan. 31, 2017), *available* here.

[5] Evan Weinberger, *NY To Keep Up Pressure On Banks In Age of Trump*, Law360 (Nov. 15, 2016), *available* here.

[6] U.S. Dep't of the Treasury, 2016 Enforcement Information, *available* here.

[7] In June 2016, then-Acting OFAC Director John Smith stated that OFAC had received "hundreds, if not thousands" of license applications in the five months since implementation of the Joint Comprehensive Plan of Action ("JCPOA"), and noted that OFAC was "stretched to the limit" in terms of resources. *See* Samuel Rubenfeld, *OFAC Beefs Up Licensing Division Due to Iran-Deal Requests*, WALL ST. J. (June 16, 2016), *available* here.

[8] *See* Paul, Weiss, *Understanding the Changes to the Iran Sanctions Regime: OFAC Issues Guidance, General Licenses on JCPOA Implementation Day* (Jan. 20, 2016), *available* here.

[9] Throughout, "persons" encompasses individuals, companies, and other entities.

[10] On Implementation Day, in addition to General License H, OFAC also announced a new general license permitting the importation of Iranian foodstuffs and carpets into the U.S., as well as a new statement of licensing policy regarding the export, sale, lease, or transfer of commercial passenger aircraft parts and services.

[11] Non-nuclear related U.S. secondary sanctions against Iran remain in place, including sanctions targeting Iran's support for terrorism, its ballistic missile program, and its abuse of human rights. *See* U.S. Dep't of the Treasury, Press Release, Treasury Sanctions Those Involved in Ballistic Missile Procurement for Iran (Jan. 17, 2016), *available* here.

[12] U.S. Dep't of the Treasury, General License H, Authorizing Certain Transactions Relating to Foreign Entities Owned or Controlled by a United States Person (Jan. 16, 2016), *available* here.

[13] For example, on June 8, 2016, OFAC issued new frequently asked questions ("FAQs") on General License H, including further guidance on the ability to change policies and procedures to permit Iran-related business and guidance on the recusal or walling-off of U.S. persons. *See generally* U.S. Dep't of the Treasury, Frequently Asked Questions Relating to the Lifting of Certain U.S. Sanctions Under the Joint Comprehensive Plan of Action ("JCPOA") on Implementation Day ("JCPOA FAQ"), section K, C(16) (last updated Dec. 15, 2016), *available* here. On October 7, 2016, OFAC issued guidance on the ability of non-U.S. persons to do business with Iran in U.S. dollars, provided that these transactions do not "involve, directly or indirectly" the U.S. financial system or any U.S. person (including U.S. banks' foreign branches). *See id.* at C(7).

[14] *See, e.g.*, Stuart Levey, *Kerry's Peculiar Message About Iran for European Banks*, WALL ST. J. (May 12, 2016) (op-ed by HSBC's Chief Legal Officer), *available* here; Laurence Normal, *U.S., EU Urge European Banks, Businesses to Invest in Iran*, WALL ST. J. (May 19, 2016), *available* here.

[15] *See* Donald J. Trump, Speech to the American Israel Public Affairs Committee (Mar. 21, 2016), *available* here. Secretary Tillerson has also called for "a full review" of the Iran nuclear deal, but implied the Administration may seek to strictly enforce, rather than dismantle, the agreement. *See Tillerson Faces Tough Questions on Iran, Russia*, AL-MONITOR (Jan. 11, 2017), *available* here. On December 15, 2016, the Iran Sanctions Extension Act was enacted into law, extending the Iran Sanctions Act of 1996 through December 2026. *See* Iran Sanctions Extension Act, Pub. Law. No. 114-277. As a result of this extension, to comply with U.S. commitments made in the JCPOA, President Trump will need to take action to waive the relevant sanctions imposed by the Iran Sanctions Act that were lifted on Implementation Day.

[16] Former Treasury Secretary Lew stated: "Since Iran has kept its end of the deal, it is our responsibility to uphold ours, in both letter and spirit." Lew, *supra* note 1. Similarly, then-Secretary of State John Kerry stated: "We have lifted the sanctions we said we would lift and we have completely kept faith with both the black-and-white print as well as the spirit of this effort. In fact, I have personally gone beyond the absolute requirements of the lifting of sanctions to personally engage with banks and businesses and others who have a natural reluctance after several years of sanctions to move without fully understanding what they are allowed to do and what they are not allowed to do." Matthew Lee, *Kerry: US Open to Further Clarifying Iran Sanctions Relief*, ASSOCIATED PRESS (June 15, 2016), *available* here.

[17] *See* JCPOA FAQ, Questions M.4., M.5.

[18] Following Iran's launch of a ballistic missile in January 2017, on February 3, 2017, OFAC designated 13 individuals and 12 entities—including companies in Iran, Lebanon, China, and the UAE—under various non-nuclear sanctions authorities related to Iran. *See* U.S. Dep't of the Treasury, Press Release, Treasury Sanctions Supporters of Iran's Ballistic Missile Program and Iran's Islamic Revolutionary Guard Corps – Qods Force (Feb. 3, 2017), *available* here.

[19] *See, e.g.*, Iran Nonnuclear Sanctions Act of 2017, H.R. 808, 115th Cong. (2017), *available* here; Iran Ballistic Missile Sanctions Act, S. 15, 115th Cong. (2017), *available* here.

[20] For detailed summaries of the various amendments, *see* U.S. Dep't of the Treasury, Press Release, Fact Sheet: Treasury and Commerce Announce Further Amendments to the Cuba Sanctions (Jan. 26, 2016), *available* here; U.S. Dep't of the Treasury, Press Release, Fact Sheet: Treasury and Commerce Announce Significant Amendments to the Cuba Sanctions Regulations Ahead of President Obama's Historic Trip to Cuba (Mar. 15, 2016), *available* here; and U.S. Dep't of the Treasury, Press Release, Treasury and Commerce Announce Further Amendments to Cuba Sanctions Regulations (Oct. 14, 2016), *available* here.

[21] Cuban Assets Control Regulations, 31 C.F.R. §§ 515.571, 515.584 (2016). For additional guidance from OFAC regarding the contours of the authorizations regarding banking services and the use of U.S. dollars for transactions involving Cuba, *see* U.S. Dep't of the Treasury, Office of Foreign Assets Control, FAQs Related to Cuba, Questions 44, 52, *available* here.

[22] On November 28, 2016, in reference to Obama Administration agreements with Cuba in furtherance of normalization, then-President-elect Trump tweeted: "If Cuba is unwilling to make a better deal for the Cuban people, the Cuban/American people and the U.S. as a whole, I will terminate deal." Donald J. Trump (@realdonaldtrump), Twitter (Nov. 28, 2016, 9:02 AM), *available* here.

[23] On sectoral sanctions, *see* U.S. Dep't of the Treasury, Office of Foreign Assets Control, Frequently Asked Questions 370-454, *available* here.

[24] *See* U.S. Dep't of the Treasury, Press Release, Treasury Sanctions Individuals and Entities for Sanctions Evasion and Activities Related to the Conflict in Ukraine (Sept. 1, 2016), *available* here; U.S. Dep't of the Treasury, Press Release, Treasury Sanctions Individuals for Activities Related to Russia's Occupation of Crimea (Nov. 14, 2016), *available* here; U.S. Dep't of the Treasury, Press Release, Treasury Sanctions Individuals and Entities In Connection with Russia's Occupation of Crimea and the Conflict in Ukraine (Dec. 20, 2016), *available* here. Separate from Ukraine-related sanctions against Russia, OFAC has continued to designate Russian persons under the Magnitsky Act, a 2012 law targeting global human rights abusers and passed in response to the death of Sergei Magnitsky in a Russian prison. *See, e.g.*, U.S. Dep't of the Treasury, Office of Foreign Assets Control, Magnitsky-related Designations (Jan. 9, 2017), *available* here.

[25] Remarks of Former Assistant Treasury Secretary for Terrorist Financing Daniel Glaser to the Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance: Securing American Interests (Feb. 6, 2017), *available* here.

[26] *See, e.g.*, Tyler Pager, *Trump to Look at Recognizing Crimea as Russian Territory, Lifting Sanctions*, POLITICO (July 27, 2016), *available* here.

[27] *See* Nicole Gaouette and Richard Roth, *UN Ambassador Haley Hits Russia Hard on Ukraine*, CNN (Feb. 3, 2017), *available* here.

[28] The proposed legislation is co-sponsored by Senators Graham, Rubio, McCain, Brown, Cardin, and McCaskill. Senator Rubio stated his belief that the legislation would have the support of a "veto-proof majority." *See* Manu Raju, *Senators Seek Hill Veto Power over Trump on Russia*, CNN (Feb. 7, 2017), *available* here.

[29] *See* North Korea Sanctions and Policy Enhancement Act of 2016, Pub. L. No. 114-122 (Feb. 18, 2016). The law requires the President to impose sanctions targeting North Korean persons involved in human rights violations, threats to cybersecurity, and proliferation activities related to weapons of mass destruction.

[30] *See* The White House, Press Release, Executive Order – Blocking Property of the Government of North Korea and the Workers' Party of Korea, and Prohibiting Certain Transactions with Respect to North Korea (Mar. 16, 2016), *available* here.

[31] *See, e.g.*, U.S. Dep't of the Treasury, Office of Foreign Assets Control, North Korea Designations (July 6, 2016), *available* here; U.S. Dep't of the Treasury, Office of Foreign Assets Control, North Korea Designations; Non-proliferation Designations (Dec. 2, 2016), *available* here; U.S. Dep't of the Treasury, Office of Foreign Assets Control, North Korea Designations (Jan. 11, 2017), *available* here.

[32] *See* U.S. Dep't of the Treasury, Press Release, Treasury Takes Actions to Further Restrict North Korea's Access to The U.S. Financial System (June 1, 2016), *available* here.

[33] Imposition of Special Measure Against North Korea as a Jurisdiction of Primary Money Laundering Concern, 81 Fed. Reg. 78,715 (Nov. 9, 2016) (to be codified at 31 C.F.R. § 1010).

[34] *See* U.S. Dep't of the Treasury, Press Release, Treasury Implements Termination of Burma Sanctions Program (Oct. 7, 2016), *available* here.

[35] In 2003, FinCEN found that Burma was a "jurisdiction of primary money laundering concern" under Section 311 of the USA PATRIOT Act and prohibited U.S. financial institutions from maintaining correspondent accounts for Burmese banks. FinCEN has stated that it "intends to rescind its action in its entirety when Burma has made sufficient progress in addressing" money laundering, corruption, and narcotics-related activities. *See* Press Release, U.S. Dep't of the Treasury, Press Release, Implements Termination of Burma Sanctions Program (Oct. 7, 2016), *available* here.

[36] *Id.*

[37] *See* U.S. Dep't of the Treasury, Press Release, Treasury to Issue General License to Authorize Transactions with Sudan (Jan. 13, 2017), *available* here. The General License became effective upon publication in the *Federal Register* on January 17, 2017.

[38] *See* Exec. Order No. 13,761, 82 Fed. Reg. 5,331 (Jan. 13, 2017), *available* here.

[39] Some public reporting has indicated that the decision to ease Sudan sanctions "came with the full approval of the incoming Trump administration[.]" *See* Khalid Abdelaziz, *Move to Lift Sudan Sanctions Came After Trump Approval, Months of Talks*, REUTERS (Jan. 14, 2017), *available* here. But other reporting quotes senior Obama Administration officials noting that "they couldn't predict whether Trump would reverse the policy." *See* Josh Lederman & Matthew Lee, *Obama Ends US Economic Embargo of Long-Estranged Sudan*, ASSOCIATED PRESS (Jan. 13, 2017), *available* here.

[40] In conjunction with OFAC's issuance of its general license, BIS issued a Final Rule amending Export Administration Regulations ("EAR") Section 742.10, which liberalizes its approval standards for the licensing of exports related to civil transportation, including railroads and aviation. *See* Revisions to Sudan Licensing Policy, 82 Fed. Reg. 4,781 (Jan. 17, 2017) (to be codified at 15 C.F.R. pt. 742), *available* here.

[41] The SEC Office of Global Security Risks has taken the position that business with designated terrorism-supported countries would generally be material to an average investor and therefore should be disclosed in securities filings. *See generally* U.S. Sec. & Exch. Comm'n, Office of Global Security Risk (last modified Mar. 2, 2005), *available* here.

[42] *See* U.S. Dep't of the Treasury, Press Release, Issuance of Amended Executive Order 13694; Cyber–Related Sanctions Designations (Dec. 29, 2016), *available* here. The original cyber-related Executive Order was EO 13694. Concurrently, BIS added the five designated entities to its Entity List, which prohibits the export, reexport, or transfer of any item subject to the EAR to the list entities.

[43] U.S. Dep't of the Treasury, Office of Foreign Assets Control, General License No. 1 (Feb. 2, 2017), *available* here.

[44] *See* U.S. Dep't of the Treasury, Office of Foreign Assets Control, Cyber-related Sanctions FAQs, Questions 501-504 (Feb. 8, 2017), *available* here.

[45] *See* U.S. Dep't of the Treasury, Press Release, Treasury Sanctions Prominent Venezuelan Drug Trafficker Tareck El Aissami and His Primary Frontman Samark Lopez Bello (Feb. 13, 2017), *available* here.

[46] CNN, *Mnuchin: Current sanctions on Russia in place* (Feb. 14, 2017), *available* here.

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

[48] The February 8, 2016 OFAC enforcement information is *available* here.

[49] The January 13, 2017 OFAC enforcement information is *available* here.

[50] OFAC's reference in the enforcement information to the inability "to restrict access for individuals and entities located in comprehensively sanctioned countries" may relate to an inability to screen and block IP addresses. *See* here. OFAC has referenced IP blocking (*i.e.*, blocking customers using computers in certain locations) in at least two other actions in a manner suggesting that OFAC considers IP blocking to be an element of an appropriate compliance screening program. *See, e.g.*, the November 24, 2015 OFAC enforcement information for Barracuda Networks, Inc., stating that "Barracuda knew or had reason to know that it was exporting goods, technology, and services to Iran and Sudan because IP addresses associated with those countries were used to contact the company," *available* here. *See, also*, the December 21, 2010 OFAC enforcement information for Wells Fargo Bank, N.A., stating that a mitigating factor in assigning the penalty was that the bank "created and implemented a risk-based OFAC compliance program, which includes the use of Internet Protocol addresses to identify registered users located in Iran," *available* here.

[51] The August 2, 2016 OFAC enforcement information is *available* here and here.

[52] The July 27, 2016 OFAC enforcement information is *available* here.

[53] The February 25, 2016 OFAC enforcement information is *available* here.

[54] The February 3, 2017 OFAC enforcement information is *available* here. In describing its determination to issue a Finding of Violation, OFAC noted as an aggravating factor that BWC took steps to conceal the transfer of Iranian oil, including by leaving shipping logs blank. As a mitigating factor, OFAC noted that all of BWC's assets appear to have been liquidated in bankruptcy.

[55] *See generally* Giant Leak of Offshore Financial Records Exposes Global Array of Crime and Corruption, THE INT'L CONSORTIUM OF INVESTIGATIVE JOURNALISTS (Apr. 3, 2016), *available* here.

[56] *See, e.g.*, Neil Chenoweth, *Panama Papers: ATO Investigating More than 800 Australian Clients of Mossack Fonseca*, SYDNEY MORNING HERALD (Apr. 4, 2016), *available* here; Francois Murphy & Kirsti Knolle, *Austrian Watchdog Investigates Two Banks After Panama Papers Leak*, REUTERS (Apr. 4, 2016), *available* here; Lars Andersen, *Panama Papers–Ministry of Finance to Investigate Arrangements in Question*, BRUSSELS TIMES (Apr. 4, 2016), *available* here; *Mexico to Investigate 33 People Named in "Panama Papers,"* FOX NEWS LATINO (Apr. 7, 2016), *available* here; Johan Ahlander & Mia Shanley, *FSA Says Including All Sweden's Major Banks in Panama Papers Probe*, REUTERS (Apr. 8, 2016), *available* here; Jill Treanor, *Regulator Widens Inquiry into UK Firms' Links with Panama Papers Tax Havens*, THE GUARDIAN (Apr. 26, 2016), *available* here.

[57] Matt Zapotosky, *U.S. Launches "Criminal Investigation" Involving Panama Papers*, WASH. POST (Apr. 20, 2016), *available* here.

[58] *See* Greg Farrell, Tom Schoenberg & Katherine Chiglinsky, *New York Wants Foreign Banks to Hand Over Panama Records*, BLOOMBERG (Apr. 20, 2016), *available* here; Greg Farrell, *Goldman Sachs Gets Panama Request from New York Bank Regulator*, BLOOMBERG (May 11, 2016), *available* here.

[59] *See* Samuel Rubenfeld, *Bank Fined for AML Failures, Panama Papers Links*, WALL ST. J. (Aug. 22, 2016), *available* here.

[60] *See* U.S. Dep't of the Treasury, Press Release, Treasury Announces Key Regulations and Legislation to Counter Money Laundering and Corruption, Combat Tax Evasion (May 5, 2016), *available* here; Dep't of Justice, Press Release, Justice Department Proposes Legislation to Advance Anti-Corruption Efforts (May 5, 2016), *available* here. Congress did not act on the proposed legislation, and it is unclear whether such initiatives would find a place on the new President and Congress's legislative agenda.

[61] *See* Letter from AFL-CIO et al. to Jack Lew, Secretary, U.S. Dep't of the Treasury, Shaun Donovan, Director, U.S. Office of Management & Budget, and Jennifer Shasky Calvery, Director, U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network (Apr. 4, 2016), *available* here.

[62] Fin. Action Task Force, Anti-Money Laundering and Counter-Terrorist Financing Measures - United States, Mutual Evaluation Report (2016), *available* here.

[63] *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).

[64] Covered institutions under the CDD rule include banks, broker-dealers, mutual funds, and futures commission merchants and introducing brokers in commodities.

[65] *See* Paul, Weiss, FinCEN Imposes Anti-Money Laundering Reporting Requirements on "All Cash" Luxury Real Estate Purchases in Manhattan and Miami (Feb. 2, 2016), *available* here.

[66] FinCEN, Press Release, FinCEN Expands Reach of Real Estate "Geographic Targeting Orders" Beyond Manhattan and Miami (Jul. 27, 2016), *available* here.

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

[68] *See id.* at ECF No. 3.

[69] U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, Press Release, FinCEN Fines Western Union Financial Services, Inc. for Past Violations of Anti-Money Laundering Rules in Coordinated Action with DOJ and FTC (Jan. 19, 2017), *available* here.

[70] *United States* v. *The Western Union Company*, No. 1:17-cr-00011 (M.D. Pa. Jan. 19, 2017), ECF No. 3-1 ¶¶ 1–4.

[71] *Id.* ¶ 68.

[72] *Id.* ¶ 29.

[73] *Id.* ¶ 59.

[74] U.S. Dep't of the Treasury, Comptroller of the Currency, Consent Order for the Assessment of a Civil Money Penalty in the Matter of Gibraltar Private Bank and Trust Company, 2016-018 (Feb. 23, 2016), *available* here.

[75] Roberto J. Gonzalez & Jessica S. Carey, *The Government's Making AML Enforcement Personal: Compliance Professionals and Senior Executives Are Increasingly in Focus*, NAT'L LAW J. (Feb. 22, 2016), *available* here.

[76] The Yates Memorandum is discussed in a prior Paul, Weiss memorandum, *New DOJ Memo by DAG Yates Intended to Increase Prosecutions of White Collar Executives and Other Employees* (Sept. 11, 2015), *available* here.

[77] Attorney General Nomination: U.S. Senate Confirmation Hearing of Jeff Sessions Before the S. Judiciary Comm., 115th Cong. 125 (2017) (statement of Jeff Sessions, Senator from Alabama).

[78] Benjamin Weiser and Nick Corasaniti, *Preet Bharara Says He Will Stay On as U.S. Attorney Under Trump* , N.Y. TIMES (Nov. 30, 2016), *available* here.

[79] U.S. Dep't of Justice, National Security Division, *Guidance Regarding Voluntary Self-Disclosures, Cooperation, and Remediation in Export Control and Sanctions Investigations Involving Business Organizations* (Oct. 2, 2016), *available* here.

[80] The guidance states that even where a company submits a self disclosure, fully cooperates, and implements timely and appropriate remediation, aggravating factors, representing heightened threats to national security, could limit the credit obtained.

[81] U.S. Dep't of Justice, Press Release, Turkish National Arrested for Conspiring to Evade U.S. Sanctions Against Iran, Money Laundering and Bank Fraud (Mar. 21, 2016), *available* here.

[82] *United States* v. *Zarrab*, No. 15 Cr. 867 (RMB), 2016 WL 6820737 (S.D.N.Y. Oct. 17, 2016).

[83] Paul, Weiss, *U.S. District Court Orders Compliance Monitor's Report Unsealed Pursuant to First Amendment Right of Public Access to Judicial Documents* (Feb. 1, 2016), *available* here.

[84] *United States* v. *HSBC Bank USA, N.A.*, No. 12 Cr. 763 (E.D.N.Y.), ECF No. 70.

[85] *United States* v. *HSBC Bank USA, N.A.*, No. 16-308-cr (2d Cir.), ECF No. 193.

[86] U.S. Dep't of Justice, Press Release, United States Seeks to Recover More than $1 Billion Obtained from Corruption Involving Malaysian Sovereign Wealth Fund (July 20, 2016), *available* here. This matter is discussed in Paul, Weiss's recent end-of-year FCPA review, *available* here.

[87] *See, e.g.*, Greg Farrell, *New York Bank Regulator to Examine Goldman's Dealings with 1MDB*, BLOOMBERG (June 10, 2016), *available* here.

[88] OCC, Semiannual Risk Perspective, Fall 2016, *available* here.

[89] U.S. Dep't of the Treasury, Comptroller of the Currency, Consent Order for a Civil Money Penalty in the Matter of Stearns Bank, N.A., 2016-048 (Apr. 18, 2016), *available* here.

[90] *See* N.Y. Dep't of Fin. Servs., Press Release, Industrial Bank of Korea Agrees to Strengthen Anti-Money Laundering Compliance and Controls at Bank's New York Branch (Mar. 1, 2016), *available* here; N.Y. Dep't of Fin. Servs., Press Release, National Bank of Pakistan Agrees to Enhance Anti-Money Laundering Compliance and Controls (Mar. 24, 2016), *available* here; N.Y. Dep't of Fin. Servs., Press Release, NYDFS Announces Enforcement Action Against Habib Bank Limited (Dec. 17, 2015), *available* here; N.Y. Dep't of Fin. Servs., Press Release, DFS Fines Agricultural Bank of China $215 Million for Violating Anti-Money Laundering Laws and Masking Potentially Suspicious Financial Transactions (Nov. 4, 2016), *available* here; Bd. of Governors of the Fed. Reserve System, Press Release, Federal Reserve Board Issues Enforcement Action with NongHyup Bank (Jan. 26, 2017), *available* here.

[91] *See Trump's Chance to Redefine the Regulators*, WALL ST. J. (Jan. 18, 2017), *available* here.

[92] Mr. Tarullo's term would otherwise have expired in 2022. *See* Ryan Tracy, *Daniel Tarullo, Federal Reserve Regulatory Point Man, to Resign*, WALL ST. J. (Feb. 10, 2017), *available* here.

[93] U.S. Sec. & Exch. Comm'n, Press Release, SEC: Miami Firm Broke Anti-Money Laundering Protocols (Feb. 4, 2016), *available* here.

[94] U.S. Sec. & Exch. Comm'n, Office of Compliance Inspections and Examinations, Examination Priorities for 2017 (Jan. 12, 2017), at 4-5, *available* here.

[95] Fin. Indus. Regulatory Auth., Press Release, FINRA Fines Raymond James $17 Million for Systemic Anti-Money Laundering Compliance Failures (May 18, 2016), *available* here.

[96] Fin. Indus. Regulatory Auth., Press Release, FINRA Fines Credit Suisse Securities (USA) LLC $16.5 Million for Significant Deficiencies in its Anti-Money Laundering Program (Dec. 5, 2016), *available* here.

[97] FINRA reached a $5.75 million settlement with Citi International Financial Services ("CIFS") in connection with alleged AML deficiencies involving foreign exchange transactions. FINRA claimed that between 2011 and 2013, CIFS processed securities transactions involving conversion between U.S. dollars and foreign currency, but lacked adequate AML monitoring systems and training commensurate with this increased money laundering risk.

[98] FINRA, Letter of Acceptance, Waiver and Consent No. 2013036434501 (Dec. 20, 2016).

[99] Fin. Indus. Regulatory Auth., 2016 Regulatory and Examination Priorities Letter (Jan. 5, 2016), at 4, *available* here.

[100] Fin. Indus. Regulatory Auth., 2017 Annual Regulatory and Examination Priorities Letter (Jan. 4, 2017), at 8, *available* here.

[101] *See* N.Y. State, Office of the Governor, Governor Cuomo Announces the 6th Proposal of the 2017 State of the State: Banning Bad Actors from the Financial Services Industry for Egregious Conduct (Jan. 10, 2017), *available* here. The proposed legislation would, among other things, add a section to New York's Financial Services Law disqualifying certain individuals from the banking or insurance industries if, after a hearing, the Superintendent finds they have committed misconduct severe enough to have a direct bearing on their fitness or ability to continue participating in the relevant industry.

[102] Governor Cuomo's proposal has prompted pushback from Attorney General Eric Schneiderman. *See* Joel Stashenko, *AG Calls Cuomo Plan to Strengthen State Financial Regulator "Wholly Unnecessary,"* N.Y.L.J. (Feb. 16, 2017), *available* here.

[103] The regulation also applies to "all check cashers and money transmitters" licensed by DFS.

[104] NY DFS Superintendent's Regulations § 504.1.

[105] Benjamin Lawsky, Address at Columbia Law School, "Financial Federalism: The Catalytic Role of State Regulators in a Post-Financial Crisis World" (Feb. 25, 2015), *available* here. Referring to a recent matter in which a DFS-installed monitor ran transactions through its own filtering systems, Lawsky added that "[w]hat regulators have not done is actively tested the effectiveness of the filtering systems banks are using. That needs to change."

[106] N.Y. Comp. Codes R. & Regs. tit. 3, §§ 504.3(a), (b).

[107] *Id.* § 504.3(c).

[108] XXXVIII N.Y. Reg. 16 (July 20, 2016).

[109] *See id.* ("The Department believes that the revised regulation is consistent with the federal framework . . . .").

[110] Paul, Weiss served as counsel to ABC with respect to the DFS consent order.

[111] The three orders cited violations of the same set of New York laws and regulations: N.Y. Comp. Codes R. & Regs. tit. 3, § 116.2 (requiring compliance with federal BSA/AML requirements and requiring that banks have risk-based policies and procedures to ensure OFAC compliance to the "maximum extent practicable"); N.Y. Banking Law § 200-c (requiring New York branches of foreign banks to maintain and make available appropriate books and records); and N.Y. Comp. Codes R. & Regs. tit. 3, § 300.1 (requiring that a bank submit a report to the Superintendent immediately upon the discovery of fraud, dishonesty, making of false entries and omission of true entries, and other misconduct). In the Intesa order, DFS also cited the bank's failure to comply with a prior agreement with DFS and the NY Fed.

[112] N.Y. Dep't of Fin. Servs., Consent Order Under New York Banking Law §§ 39 and 44 in the Matter of Agricultural Bank of China Ltd. and Agricultural Bank of China New York Branch (Nov. 4, 2016), at ¶¶ 7-8.

[113] Of course, the failure to maintain an effective AML program is a federal BSA/AML violation, which has figured prominently in past federal enforcement actions. These program violation findings, however, have usually been accompanied by more specific findings regarding underlying suspicious or illegal conduct and findings regarding SARs that should have been, but were not, filed in a timely fashion.

[114] N.Y. Dep't of Fin. Servs., *supra* note 112, at ¶ 80; N.Y. Dep't of Fin. Servs., Consent Order Under New York Banking Law §§ 39 and 44 in the Matter of Mega International Commercial Bank Co., Ltd., and Mega International Commercial Bank Co. Ltd. - New York Branch (Aug. 19, 2016), at ¶ 61.

[115] 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).

[116] Landon Thomas Jr., *Deutsche Bank Fined in Plan to Help Russians Launder $10 Billion*, N.Y. TIMES (Jan. 30, 2017), *available* here.

[117] 18 U.S.C. § 2331 *et seq.*

[118] *Linde* v. *Arab Bank, PLC*, 269 F.R.D. 186 (E.D.N.Y. 2010).

[119] Brief for the United States as Amicus Curiae, *Arab Bank, PLC* v. *Linde*, No. 12-1485 (U.S. May 23, 2014), 2014 WL 2191224.

[120] *Linde* v. *Arab Bank, PLC*, No. 04-cv-2799, 2016 WL 6094184 (E.D.N.Y. May 24, 2016).

[121] *Zapata* v. *HSBC Holdings*, No. 16-00030 (S.D. Tex. filed Feb. 9, 2016).

[122] Preet Bharara, U.S. Attorney, Remarks on "Criminal Accountability and Culture" (Nov. 10, 2016), *available* here.

[123] N.Y. Dep't of Fin. Servs., *supra* note 115, at ¶ 46.

[124] *See* Ben DiPietro, *The Morning Risk Report: New York Law Adds Teeth to Federal AML Oversight*, WALL ST. J. (Jan. 24, 2017), *available* here.

[125] Richard Cordray, Director, Consumer Fin. Protection Bureau, Remarks at the Consumer Bankers Association (Mar. 9, 2016), *available* here.

[126] N.Y. Dep't of Fin. Servs., *supra* note 114, at ¶ 17.

[127] U.S. Dep't of the Treasury and Federal Banking Agencies, Joint Fact Sheet on Foreign Correspondent Banking: Approach to BSA/AML and OFAC Sanctions Supervision and Enforcement (Aug. 30, 2016), *available* here. This fact sheet was discussed in a previous memorandum. *See* Paul, Weiss, *Treasury and Federal Banking Agencies Clarify BSA/AML and Sanctions Enforcement Standards for Foreign Correspondent Banking Relationships* (Sept. 1, 2016), *available* here.

[128] *See, e.g.*, Rick Gladstone, *Bangladesh Bank Chief Resigns After Cyber Theft of $81 Million*, N.Y. TIMES (Mar. 15, 2016), *available* here; Michael Corkery, *Once Again, Thieves Enter Swift Financial Network and Steal*, N.Y. TIMES (May 12, 2016), *available* here. In light of the SWIFT attacks, the FFIEC issued additional guidance to remind financial institutions of the need to actively manage the risks associated with interbank messaging and wholesale payment networks. *See* Fed. Fin. Institutions Examination Council, Joint Statement: Cybersecurity of Interbank Messaging and Wholesale Payment Networks (June 7, 2016), *available* here.

[129] OCC, Semiannual Risk Perspective, Fall 2016, *available* here.

[130] Cybersecurity Requirements for Financial Services Companies (proposed Sept. 13, 2016) (to be codified at N.Y. Comp. Codes R. & Regs. tit. 23, pt. 500) (not yet published in New York Register), *available* here.

[131] Paul, Weiss, *New York DFS Proposes New Rules on Cybersecurity* (Sept. 15, 2016), *available* here.

[132] Cybersecurity Requirements for Financial Services Companies (proposed Dec. 28, 2016) (to be codified at N.Y. Comp. Codes R. & Regs. tit. 23, pt. 500) (not yet published in New York Register), *available* here.

[133] Cybersecurity Requirements for Financial Services Companies (Feb. 16, 2017) (to be codified at N.Y. Comp. Codes R. & Regs. tit. 23, pt. 500) (not yet published in New York Register), *available* here.

[134] Enhanced Cyber Risk Management Standards (proposed Oct. 19, 2016) (to be codified at 12 C.F.R. pts. 30, 364), *available* here.

[135] Paul, Weiss, *Federal Banking Agencies Issue Advanced Notice of Proposed Rulemaking on Enhanced Cybersecurity Standards* (Oct. 21, 2016), *available* here.

[136] U.S. Sec. & Exch. Comm'n, Order Instituting Administrative and Cease-And-Desist Proceedings, Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, and Sections 203(e) and 203(k) of the Investment Advisers Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Cease-And-Desist Order, in the Matter of Morgan Stanley Smith Barney LLC (June 8, 2016), *available* here.

[137] U.S. Sec. & Exch. Comm'n, Press Release, SEC Charges Investment Adviser with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach (Sept. 22, 2015), *available* here; U.S. Sec. & Exch. Comm'n, 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 Craig Scott Capital, LLC, Craig S. Taddonio, and Brent M. Porges (Apr. 12, 2016), *available* here.

[138] U.S. Sec. & Exch. Comm'n, *supra* note 94, at 4 .

[139] System Safeguards Testing Requirements (Sept. 8, 2016) (to be codified at 17 C.F.R. pts. 37, 38, & 49), *available* here.

[140] Timothy Massad, Chairman, U.S. Commodity Futures Trading Comm'n, Statement of Chairman Timothy Massad on the System Safeguards Testing Final Rules (Sept. 8, 2016), *available* here.

[141] J. Christopher Giancarlo, Commissioner, U.S. Commodity Futures Trading Comm'n, Statement of Commissioner J. Christopher Giancarlo Regarding Proposed Rule on System Safeguards Testing Requirements (Dec. 16, 2015), *available* here.

[142] Paul, Weiss, *The CFPB Enters the Cybersecurity Arena with Its First Enforcement Action* (Mar. 4, 2016), *available* here.

[143] Consumer Fin. Protection Bureau, Consent Order in the Matter of Dwolla, Inc. (Mar. 2, 2016), *available* here.

[144] U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime (Oct. 25, 2016), *available* here; *see also* U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, Frequently Asked Questions (FAQs) (Oct. 25, 2016), *available* here.

[145] F. Christopher Calabia, Keynote Address at the Institute for International Bankers Annual Seminar on Risk Management and Regulatory Examination/Compliance Issues (Oct. 24, 2016) (emphasis added), *available* here.

[146] Paul, Weiss, *New Federal Guidance on the Cybersecurity Information Sharing Act of 2015: What General Counsel Need to Know* (Feb. 23, 2016), *available* here.

[147] OCC, Semiannual Risk Perspective, Fall 2016, *available* here.

[148] *See* Calabia, *supra* note 145.

[149] *See Lewert* v. *P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016).

[150] *See Remijas* v. *Neiman Marcus Group, LLC.*, 794 F.3d 688 (7th Cir. 2015).

[151] *Spokeo, Inc.* v. *Robins*, 136 S. Ct. 1540 (2016).

[152] Paul, Weiss, *Cybersecurity Update: Heightened Concerns, Legal and Regulatory Framework, Enforcement Priorities, and Key Steps to Limit Legal and Business Risks* (Sept. 30, 2015), *available* here.