Client Alert | Financial Institutions Advisory / International Trade

Review of Anti-Money Laundering and Sanctions Policy and Enforcement

January 2019

Authors: **Kevin Petrasic**, **Paul Saltzman**, **Nicole Erb**, **Jeremy Kuester**, **Cristina Brayton-Lewis**, **John Wagner**

TABLE OF CONTENTS:

Executive Summary

This anti-money laundering and sanctions review provides an overview and insights with respect to material developments in the United States regarding Bank Secrecy Act ("BSA")/anti-money laundering ("AML") and economic sanctions policy and enforcement in 2018. Going forward, White & Case expects to publish a similar review on a semi-annual basis to provide financial institutions with regular updates and insights. Future editions will also address material developments outside of the United States.

Financial Institutions Advisory

- Bank Regulation, compliance and risk management
- Financial services digital transformation, including AI and RegTech
- Payments
- AML/BSA
- Blockchain and digital assets
- Regulatory and supervisory remediation, investigations and enforcement
- Bank recovery, restructuring, and resolution
- Marketplace and online lending
- Capital and liquidity regulation
- Consumer financial services
- Banking board and senior management governance
- Market Infrastructure, financial market utilities and CCPs

This review discusses key developments and trends in BSA/AML and economic sanctions policy and enforcement on an agency-by-agency basis, including rule implementations, enforcement actions and agency statements suggesting future priorities and actions. In addition, this review discusses potential legislative changes to BSA/AML and economic sanctions policy under consideration by US lawmakers.

In reviewing developments throughout 2018, several trends are apparent:

Growing convergence between OFAC and FinCEN actions:

- Throughout the year, there was an apparent synchronization between actions by the US Department of the Treasury's ("Treasury's") Office of Foreign Assets Control ("OFAC") and Treasury's Financial Crimes Enforcement Network ("FinCEN"). The coordination between agencies also suggests that greater coordination is expected among AML and sanctions compliance teams at financial institutions to ensure that assets are blocked and transactions rejected in compliance with sanctions and that suspicious activity reports ("SARs") of possible sanctions evasion are submitted to FinCEN.

Enforcement and personal liability:

- Federal regulators continue to bring a large number of enforcement actions and assess substantial monetary penalties as the Trump administration pursues its law enforcement and countering the financing of terrorism ("CFT") agenda. Regulators are also focused on individual accountability for violations, as demonstrated through the many actions pursued against individuals discussed below and emphasized in remarks delivered by Deputy Attorney General Rod Rosenstein in May 2018.[1] Regulators and the Department of Justice ("DOJ") have not been pursuing individual executives and compliance officers for simple failures of compliance, but rather for egregious conduct, including deliberate attempts to circumvent or sideline compliance controls or to actively hide from or misrepresent information to regulators.

Agency coordination:

- In his May 2018 remarks, Deputy Attorney General Rosenstein also announced a new policy to encourage coordination among the DOJ and other government enforcement agencies when imposing multiple penalties for the same conduct, with the goal of enhancing coordination while avoiding duplicative penalties, or "piling on." The various agencies have made a point of emphasizing their coordination and consideration of penalties imposed by other agencies in several enforcement actions this year. The extent to which federal agencies and state actors, such as the New York State Department of Financial Services ("DFS"), will succeed in coordinating remains to be seen. In addition, a working group of FinCEN and federal banking agencies released two joint statements in 2018 that respectively encourage industry innovation in BSA/AML compliance and address resource sharing among smaller institutions. This working group continues to meet regularly, and FinCEN Director Kenneth Blanco has identified the group's priorities as including: (i) industry innovation; (ii) reviewing the risk-based approach to the examination process; (iii) reviewing agencies' approach to BSA/AML supervision and enforcement; (iv) exploring concrete ways to increase the value of BSA/AML data across stakeholders; and (v) streamlining SAR reporting while retaining value to law enforcement.

Digital currencies:

- Federal regulators have cited BSA/AML compliance as an area of continued focus and in many cases have specifically mentioned digital currencies and other developing financial technologies as a key risk to which they will be paying attention going forward.[2] In November 2018, OFAC took action against two Iran-based individuals for helping to exchange bitcoin ransom payments on behalf of Iranian cyber actors and, in doing so, for the first time publicly attributed digital currency addresses to designated individuals.[3]

Legislative developments:

- Bipartisan support appears to exist in both the Senate and House to “modernize” the BSA and otherwise make BSA/AML compliance more effective and efficient, although no such legislation was approved by Congress during the 115th Congress. However, certain bills proposed during the 115th Congress are expected to serve as a starting point for legislative proposals in the 116th Congress, which convened in early 2019.

Developments and Trends in Policy and Enforcement

US Department of the Treasury

On December 20, 2018, Treasury issued the National Strategy for Combating Terrorist and Other Illicit Financing (“National Illicit Finance Strategy”), pursuant to Sections 261 and 262 of the Countering America’s Adversaries Through Sanctions Act of 2017 (“CAATSA”).[4] The National Illicit Finance Strategy describes and assesses current US government efforts to combat illicit finance threats and risks and identifies priorities, objectives and potential areas for future improvement. It also highlights US interagency and intergovernmental efforts to combat illicit finance domestically and internationally, including enforcement measures that include sanctions, prosecutions and asset forfeiture, as well as improvements in information-sharing mechanisms and updated guidance to aid financial institutions in detecting and combating illicit finance threats. Treasury also issued national risk assessments for terrorism financing, nuclear proliferation financing and money laundering.[5] Together, these assessments are intended to help the public and private sectors understand the terrorist financing, proliferation financing and money laundering methods used in the United States, the threat actors behind these methods and vulnerabilities exploited and the risks that these activities pose to the US financial system and national security.

The Office of Foreign Assets Control (OFAC)

In recent years, the United States has relied increasingly upon existing and new laws to enforce US sanctions against non-US parties in an effort to ensure non-US parties will uphold US foreign policy and national security interests abroad.[6] Since 2015, OFAC has collected more than US$800 million in 46 civil penalties/settlements from both US and non-US companies for violations of US sanctions laws—this does not include amounts paid to other US and non-US authorities.

Since 2010, the United States has increased both the scope and frequency of enforcement of so-called “secondary sanctions,” which can be imposed against non-US persons even where there is no connection to the United States or a US person. Secondary sanctions generally target “sanctionable activities” by non-US persons outside the United States, such as trade with North Korea or dealings with designated Iranian parties. As a general matter, US authorities do not impose civil or criminal monetary penalties for violations of secondary sanctions, because the violation typically lacks a connection to the United States or US persons. But the imposition of secondary sanctions measures can be just as serious, if not more so, than the imposition of monetary penalties.

For example, US authorities can designate the non-US violator on the US List of Specially Designated Nationals and Blocked Persons (“SDN List”), thereby closing or restricting the violator’s access to US commercial and financial markets, or freezing any assets of the violator in the United States or in the possession of a US person (*e.g.*, a US financial institution). Secondary sanctions thus operate as a powerful deterrent against dealings by non-US persons with US-sanctioned countries or blocked parties, even in the absence of any US nexus. The US statutes providing for secondary sanctions include, but are not limited to, the Iran and Libya Sanctions Act of 1996, the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 ("CISADA"), the Ukraine Freedom Support Act of 2014 ("UFSA") and CAATSA.

Sanctions Policy Developments

Iran

On May 8, 2018, President Donald Trump announced that the United States would withdraw from the Joint Comprehensive Plan of Action ("JCPOA").[7] Following two wind-down periods, on August 6 and November 5, 2018, the United States re-imposed the sanctions that had been lifted under the JCPOA. In connection with the re-imposition of sanctions, OFAC posted additional and amended FAQs,[8] designated or redesignated more than 700 individuals, entities, aircraft and vessels on the SDN List,[9] and amended the Iranian Transactions Sanctions Regulations ("ITSR").[10] Non-US financial institutions, in particular, should be aware of their potential exposure under US secondary sanctions, even as other countries participating in the JCPOA seek to maintain the status quo. Many of the 700 persons designated to the SDN List had been previously designated and were delisted pursuant to the JCPOA, or were previously located on the executive order 13599 List, which was subsumed into the SDN List on November 5. Persons previously designated on the 13599 List will have a notation indicating this, and may also be designated under additional authorities. OFAC clarified in related FAQs that certain Iranian financial institutions designated only under executive order 13599 are not subject to the full array of US sanctions on Iran.[11]

Russia/Ukraine

On April 6, 2018, OFAC designated seven Russian individuals, 12 companies deemed to be owned or controlled by those individuals, 17 senior Russian officials and the state-owned Russian weapons trading company Rosoboroneksport and its subsidiary the Russian Financial Corporation Bank (RFC Bank) on the SDN List.[12] These persons were designated for, among other things, operating in the Russian energy sector, being an official of the Government of the Russian Federation, acting for or on behalf of, directly or indirectly, a senior official of the Government of the Russian Federation or being owned or controlled 50% or more by a designated individual.

The designations included individuals named in Treasury's January 29, 2018 report to Congress identifying "Russian Senior Foreign Political Figures and Oligarchs in the Russian Federation and Russian Parastatal Entities," as required by Section 241 of CAATSA.[13] OFAC issued two initial general licenses to provide for the wind-down of United States dealings with the following designated entities: EN+ Group PLC ("EN+"), JSC EuroSibEnergo ("ESE"), GAZ Group and United Company Rusal PLC ("Rusal") among others, as well as any other entity owned 50% or greater by one or more of the entities named in the licenses.[14] Certain of these licenses have been renewed periodically and extended to account for the ongoing negotiations with OFAC to delist EN+ and Rusal from the SDN List through Oleg Deripaska's divestment and relinquishment of control of these entities.[15]

President Trump issued an executive order on September 20, 2018 in connection with Title II of CAATSA and UFSA.[16] The executive order authorizes the imposition of an array of finance-related sanctions on parties engaging in certain sanctionable activity under CAATSA or UFSA, such as prohibitions on credit transfers or payments subject to US jurisdiction between financial institutions or by, through or to financial institutions involving any interest of a sanctioned person, or denial of the issuance of specific licenses for export or re-export of goods or technology to the sanctioned person.

On September 20, 2018, OFAC also designated Chinese entity Equipment Development Department (EDD) and its director Li Shangfu to the SDN List for engaging in significant transactions with persons on the CAATSA Section 231 List of Specified Persons ("LSP")—persons that are part of, or operating for or on behalf of, the defense or intelligence sectors of the Government of the Russian Federation.[17] In addition, OFAC also imposed CAATSA Section 235 menu-based sanctions on the two Chinese parties. These were the first sanctions imposed on non-US persons under CAATSA Section 231. As a complement to the sanctions maintained by OFAC, the State Department took corresponding action to designate the same Chinese persons and 33 other persons to the LSP for being a part of, or operating for or on behalf of, the defense or intelligence sectors of the Government of the Russian Federation pursuant to CAATSA Section 231.[18]

On December 19, 2018, OFAC notified Congress of its intent to terminate sanctions imposed on EN+, Rusal, and ESE in 30 days from December 19.[19] OFAC and the three entities have memorialized a framework for delisting in the "Terms of Removal," to ensure a sufficient decrease in Oleg Deripaska's ownership and to eliminate his control of these entities. This agreement will enable these entities to meet the criteria for delisting, the terms of which include: (i) reducing Mr. Deripaska's direct and indirect shareholding stake; (ii) overhauling the composition of the En+ and Rusal boards of directors; (iii) taking other restrictive steps related to their corporate governance; and (iv) committing to full transparency with Treasury by undertaking extensive, ongoing auditing, certification and reporting requirements. Congress has an opportunity to review the Notice to Congress over the 30-day period, and may enact a joint resolution of disapproval that if enacted has the power to block this delisting by OFAC. OFAC has stated that it will monitor closely these entities' compliance with the Terms of Removal and that OFAC reserves the right to relist these entities should they fail to comply with the Terms of Removal. Mr. Deripaska will remain on the SDN List. On January 4, 2019, Senator Chuck Schumer introduced a joint resolution of disapproval, citing the short review time as reason to introduce the resolution while Congressional Committee review was ongoing.[20] Senator Schumer stated that he had not concluded that Congress should categorically disapprove of the delisting, but rather that given Congressional rules on joint resolutions, he thought it prudent to introduce a resolution that could be passed before the end of the 30-day Congressional review period.

Also on December 19, 2018, OFAC designated 18 Russian individuals and four entities to the SDN List pursuant to CAATSA Section 224 over allegations of election interference, cyber hacking of several international nonpolitical organizations, acting on behalf of sanctioned oligarch Oleg Deripaska and the March 2018 Novichok nerve agent attack.[21] As a complement to the sanctions maintained by OFAC, the State Department took corresponding action under CAATSA to designate 12 of the same persons to the LSP for being part of, or operating for or on behalf of, the defense or intelligence sectors of the Government of the Russian Federation.

Venezuela

Throughout 2018, President Trump signed several executive orders addressing Venezuela sanctions. A March 19, 2018 executive order prohibits all transactions by a US person or within the United States that relate to or provide financing for any digital currency, digital coin or digital token, issued by, for or on behalf of the Government of Venezuela on or after January 9, 2018.[22]

An executive order issued on May 21, 2018 prohibits all transactions by a US person or within the United States that relate to or provide financing for: (i) the purchase of any debt owed to the Government of Venezuela, including accounts receivable; (ii) any debt owed to the Government of Venezuela that is pledged as collateral, including accounts receivable; or (iii) the sale, transfer, assignment, or pledging as collateral by the Government of Venezuela of any equity interest in any entity in which the Government of Venezuela has a 50% or greater ownership interest.[23]

An executive order issued on November 1, 2018 authorized the blocking of all property and interests in property that are in or come within the United States or the possession or control of any US person of any person determined by the Secretary of the Treasury, in consultation with the Secretary of State: (i) to operate in the gold sector of the Venezuelan economy or in any other subsequently designated sector; (ii) to be responsible for or complicit in, or to have directly or indirectly engaged in, any transaction involving deceptive practices or corruption and the Government of Venezuela or projects or programs administered by the Government of Venezuela, or to be an immediate adult family member of such a person; or (iii) to have materially assisted, sponsored, supported or to be owned or controlled by any person or property blocked by the order.[24] OFAC issued FAQs throughout the year in connection with the executive orders.[25] Amongst others, four current or former Venezuelan government officials were designated for allegedly engaging in political repression and corruption as part of the Maduro government.

Digital Currency

On March 19, 2018, President Trump issued an executive order prohibiting US persons from dealing in any digital currency issued by, for or on behalf of the Government of Venezuela on or after January 9, 2018.[26] The prohibition is applied expansively. Concurrently, OFAC issued FAQs addressing digital currencies, and providing that, for the purposes of the executive order, the “petro” and “petrogold” were each considered a “digital currency, digital coin, or digital token,” covered under the Executive Order.[27] The FAQs take the prohibition further, specifying that the prohibition applies to US persons who participated in the pre-sale for a Government of Venezuela-issued “digital currency, digital coin, or digital token” before the effective date of the executive order. However, OFAC will consider related license applications on a case-by-case basis of the facts and circumstances of a particular application.

On November 28, 2018, OFAC designated two Iran-based individuals to the SDN List for their roles in exchanging bitcoin ransom payments on behalf of Iranian cyber actors in connection with the “SamSam” ransomware scheme, which targeted corporations, hospitals, universities and government agencies.[28] These designations were the first time OFAC added a digital currency address—the cryptocurrency version of a bank account/routing number—to the SDN List. In connection with this action, OFAC updated its FAQs on virtual currencies, originally published on March 19, 2018, to address how an institution should block digital currency and communicate such an action to its customers.[29]

Nicaragua

An executive order issued on November 27, 2018 authorized the blocking of all property and interests in property which are in the possession or control of any US person or that come within the United States, of any person determined: (i) to be responsible for or complicit in, or to have engaged in, serious human rights abuse in Nicaragua, actions or policies that undermine democratic processes or institutions in Nicaragua, actions or policies that threaten the peace, security, or stability of Nicaragua or any transaction or series of transactions involving deceptive practices or corruption by, on behalf of, or otherwise related to the Government of Nicaragua or a current or former government official; (ii) to be a leader or official of an entity that has, or whose members have, engaged in any such activity; (iii) to be a present or former official of the Government of Nicaragua; (iv) to have materially assisted, sponsored or provided financial, material or technological support for, or goods or services in support of, any such activity; or (v) to be owned or controlled by, or to have acted on behalf of, directly or indirectly, any person blocked under the executive order.[30] OFAC designated two senior Nicaraguan officials on the SDN List in connection with the executive order.

North Korea

OFAC, in coordination with the Department of State and the US Coast Guard, issued an advisory on February 23, 2018 regarding sanctions risks related to North Korea shipping practices, in which OFAC alerted persons globally to deceptive shipping practices used by North Korea to evade sanctions.[31] On July 23, 2018, Treasury, the Department of State and the Department of Homeland Security issued an advisory to highlight sanctions evasion tactics used by North Korea.[32] Both advisories provide businesses, including financial institutions, with information about deceptive practices employed by North Korea, so that they may better implement effective due diligence policies, procedures and internal controls to ensure compliance with applicable legal requirements.

On March 5, 2018, OFAC amended the North Korea Sanctions Regulations to implement certain executive orders and to reference the North Korean Sanctions and Policy Enhancement Act of 2016 and CAATSA.[33]

OFAC also published updated frequently asked questions ("FAQs") addressing the North Korea sanctions program.[34]

Syria

On November 20, 2018, OFAC, in coordination with the Department of State and the US Coast Guard, issued an advisory regarding sanctions risks related to shipping petroleum to Syria, in which OFAC alerted persons globally to the risk of petroleum-related shipments to Syria violating US sanctions on Syria and Iran.[35] The advisory provides businesses, including financial institutions, with information about deceptive practices employed by the Syrian petroleum shipping industry, so that they may better implement effective due diligence policies, procedures, and internal controls to ensure compliance with applicable legal requirements.

Foreign Interference in United States Elections

On September 12, 2018, President Trump signed an executive order to authorize the imposition of sanctions on persons located outside of the United States that interfere in or undermine public confidence in US elections.[36] The order authorizes the blocking of property or interests in property of any person determined by the Secretary of the Treasury, in consultation with the Secretary of State, Attorney General and Secretary of Homeland Security:

- to have directly or indirectly engaged in, sponsored, concealed or otherwise been complicit in foreign interference in a US election (or to have materially assisted, sponsored, or provided support to anyone who carried out such activities); or
- to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property or interests in property are blocked pursuant to the order.

The order also directs the Director of National Intelligence ("DNI") to conduct an assessment following any federal elections of whether foreign interference occurred, to be delivered to the President, the Secretaries of State, Treasury, Defense and Homeland Security, and the Attorney General. The order also directs that the Department of Homeland Security and the DOJ must—upon receipt of the DNI assessment—prepare and deliver a report to the President and relevant agencies evaluating the extent and impact of any foreign interference. The Secretary of the Treasury shall review the DNI assessment and subsequent report, and, in consultation with the Secretaries of State and Homeland Security and the Attorney General, impose "all appropriate sanctions" pursuant to the executive order. There have yet to be any designations under this executive order, but as noted above, several Russian individuals were designated to the SDN List under other authorities over allegations of election interference.

Cuba

On November 15, 2018, the US Department of State designated 26 entities to the List of Restricted Entities and Subentities Associated with Cuba ("Cuba Restricted List").[37] Designation to the Cuba Restricted List results when the US government determines that an entity or subentity is under the control of, or acting for or on behalf of, the Cuban military, intelligence or security services, or personnel with which direct financial transactions would disproportionately benefit the personnel or listed Cuban services at the expense of the Cuban people or private enterprise in Cuba. Persons subject to US jurisdiction are generally prohibited from engaging in direct financial transactions with entities designated on the Cuba Restricted List. The Department of Commerce's Bureau of Industry and Security ("BIS") also follows a general policy of denying export licenses for export or reexport involving entities and Subentities designated on the Cuba Restricted List. This is the first set of designations since the Cuba Restricted List's creation in 2017. The designated entities include 16 hotels owned by the Cuba military.

Sudan

Most transactions with Sudan have been authorized pursuant to a General License since January 17, 2017. On June 29, 2018, OFAC published a final rule to remove the Sudanese Sanctions Regulations ("SSR") from the Code of Federal Regulations.[38] US persons are no longer prohibited from engaging in transactions that were previously prohibited solely under the SSR. An OFAC license is still required for certain exports and re-exports to Sudan of agricultural commodities, medicine, and medical devices as a result of Sudan's continued inclusion on the State Sponsors of Terrorism List. In addition, US persons and non-US persons are still required to obtain any licenses required by BIS to export or re-export to Sudan certain items (commodities, software, and technology) on the Commerce Control List, with certain exceptions.

Forthcoming Guidance on Effective Economic Sanctions Compliance Programs

On December 3, 2018, Treasury Under Secretary Sigal Mandelker previewed anticipated guidance from OFAC regarding what constitutes an effective economic sanctions compliance program, which would include:

- Ensuring senior management commitment to compliance;
- Conducting frequent risk assessments to identify and mitigate sanctions-specific risks;
- Developing and deploying internal controls in order to identify, interdict, escalate, report, and maintain records pertaining to prohibited activity;
- Engaging in testing and auditing to identify and correct weaknesses and deficiencies; and
- Ensuring all relevant personnel, particularly those in high-risk areas or business units, are provided tailored training.[39]

Enforcement Actions

Settlement with US Holding Company for Apparent Violations of Belarus Sanctions

On December 20, 2018, OFAC announced a US$7.8 million settlement with a US holding company to settle potential civil liability for 26 apparent violations of the Belarus Sanctions Regulations.[40] OFAC found that between January 18, 2012 and October 27, 2015, the holding company and/or one of its US subsidiaries violated the Belarus Sanctions Regulations by approving 26 purchases of a chemical from a Belarusian SDN. In addition, the holding company's Hungarian subsidiary also purchased the chemical from the SDN, with the approval of senior executives of the holding company. OFAC considered the following aggravating factors: (i) the holding company acted with reckless disregard for US economic sanctions requirements and/or failed to exercise a minimal degree of caution or care in avoiding the conduct that led to the apparent violations and failed to incorporate OFAC compliance checks in its overall risk mitigation strategy; (ii) personnel, including senior and executive-level managers, were aware of—and participated in—the conduct that led to the apparent violations; (iii) the holding company approved the Hungarian subsidiary's purchase of a significant volume of chemicals from the SDN for a period of several years, resulting in significant harm to the sanctions program objectives and conferring more than US$18 million to a Belarusian government entity; (iv) the holding company and US subsidiary are large entities that engage in a significant volume of international trade and cross-border transactions; and (v) specifically for action after February 2015, senior personnel actively discussed US sanctions related to the SDN raised by third parties but did not review the company's US legal obligations and continued to approve SDN transactions. OFAC considered the following mitigating factors: (a) neither the holding company nor its US subsidiary received a penalty notice or Finding of Violation from OFAC in the five years preceding the earliest apparent violations; (b) the holding company and US subsidiary cooperated with OFAC's investigation, including by voluntarily self-disclosing the apparent violations, providing detailed and well-organized information for OFAC's review, and by agreeing to toll the statute of limitations for a total of 643 days; and (c) the holding company and US subsidiary confirmed that they have terminated the conduct that led to the apparent violations and have taken steps to minimize the risk of recurrence of similar conduct in the future.

Settlement with Chinese Oil and Gas Company for Apparent Violations of Iran Sanctions

On December 12, 2018, OFAC announced a US$2.8 million settlement with an oil and gas company based in China for 11 apparent violations of the ITSR, concurrent with a separate settlement between the company and BIS.[41] According to OFAC, the company exported or re-exported, or attempted to export or re-export, US-origin goods ultimately intended for end-users in Iran by way of China and the UAE. OFAC alleged that the company knew or had reason to know that items in some of the shipments were ultimately intended for Iran. OFAC considered the following aggravating factors, among others: (i) the company willfully violated the ITSR by engaging in and systematically obfuscating conduct it knew to be prohibited by company policy and economic sanctions, and continued to engage in such conduct even after the US government began to investigate the conduct; (ii) employees, including several management-level personnel, had contemporaneous knowledge of the transactions in question; (iii) employees took actions to conceal the nature of the transactions from the US government; and (iv) the company falsified information on Electronic Export Filings and made other false statements to the US government in the course of the investigation. OFAC also considered the following mitigating factors: (a) the company has no prior sanctions history with OFAC; (b) the company cooperated with OFAC's investigation by disclosing possible violations involving other sanctions programs and responding to OFAC's requests for information regarding Iran; (c) the company agreed to toll the statute of limitations; and (d) the company took remedial steps and corrective actions to prevent a recurrence of the apparent violations.

Settlement with Global Technology and Services Company for Apparent Violations of Ukraine Sanctions

On November 27, 2018, OFAC announced a settlement of US$87,507 with a US global technology and services company, on behalf of its former subsidiary, to settle potential civil liability for three apparent violations of the Ukraine Related Sanctions Regulations.[42] OFAC found that between July 31, 2014 and January 15, 2015, the subsidiary sold switch limiters, switches and silicon diode switch limiter samples through distributors in Canada and Russia to a person blocked pursuant to Executive Order 13661. OFAC noted that the company voluntarily self-disclosed the apparent violations on behalf of the subsidiary and that the apparent violations constituted a non-egregious case.

Settlement with Global European Bank for Apparent Violations of Multiple Sanctions

On November 19, 2018, OFAC announced a US$53.9 million settlement agreement with a global European bank for apparent violations of the Cuban Assets Control Regulations ("Cuban Regulations"), the SSR and the ITSR involving more than a thousand transactions processed to or through the United States or involving US financial institutions.[43] The settlement was part of a broader settlement by the bank with other federal agencies. This matter is discussed further below under "Department of Justice."

Settlement with Large US Commercial Bank for Apparent Violations of Multiple Sanctions

On October 5, 2018, OFAC announced a settlement of approximately US$5.3 million with a large US bank to settle potential civil liability for 87 apparent violations of the Cuban Regulations, the ITSR and the Weapons of Mass Destruction Proliferators Sanctions Regulations.[44] OFAC found that the bank operated a net settlement mechanism that resolved billings by and among various airlines and other participants in the airline industry on behalf of its client, a US entity and its approximately 100 members, and a non-US entity and its more than 350 members. According to OFAC, between January 2008 and February 2012, the bank processed 87 transactions through the US financial system that may have contained interests attributable to a sanctions-targeted party. OFAC found that the bank did not appear to have a process to independently evaluate the participating member entities of the non-US entity for OFAC sanctions risk prior to January 2012, despite receiving red flag notifications regarding OFAC-sanctioned members on at least three occasions. OFAC noted that the bank voluntarily self-disclosed the violations. Separately, OFAC found that the bank violated the Foreign Narcotics Kingpin Sanctions Regulations and the SSR when, between August 2011 and April 2014, it processed 85 transactions totaling US$46,127.04 and maintained eight accounts on behalf of six customers identified on the SDN List.

Settlement with Automotive Electronics Company for Apparent Violations of Iran Sanctions

On September 13, 2018, OFAC announced a US$1.5 million settlement with a global automotive electronics company to settle potential civil liability in connection with the issuance by the company of 39 invoices for sales to a counterparty that OFAC alleges the company knew or had reason to know distributed most, if not all, of its products to Iran.[45] OFAC also found that the company did not have a compliance program in place at the time of the alleged violations.

OFAC had previously issued the company a Penalty Notice on July 21, 2014, which the company challenged in the US District Court for the District of Columbia and later appealed to the US Court of Appeals for the District of Columbia ("DC Circuit"). The DC Circuit affirmed in part the District Court's summary judgment in favor of OFAC, remanding the case to the District Court with instructions to remand to OFAC for further consideration. Upon remand, OFAC and the company reached the September 13, 2018 settlement, settling all related litigation and the original OFAC Penalty Notice. This settlement amount reflects OFAC's further consideration of the case, in light of the DC Circuit's partial remand and pursuant to the General Factors under OFAC's Economic Sanctions Enforcement Guidelines. OFAC considered the following mitigating factors in reaching a settlement: the company (i) had not received a Penalty Notice or a Finding of Violation in the five years preceding the transactions at issue in this case; (ii) is a small business; and (iii) provided OFAC with some cooperation, including entering into an agreement to toll the statute of limitations for one year. OFAC considered the following aggravating factors: (a) the alleged violations showed a systematic pattern of conduct; (b) the company exported goods valued at more than US$2.8 million; and (c) the company had no compliance program at the time of the alleged violations.

Settlement with Global Networking and Telecommunications Company for Apparent Violations of Sudan Sanctions

On June 6, 2018, OFAC announced a US$145,893 settlement with Sweden- and Texas-based entities within a global networking and telecommunications group to settle potential civil liability for an apparent violation of the International Emergency Economic Powers Act and the SSR in connection with work on satellite equipment destined for Sudan.[46]

Treasury's Financial Crimes Enforcement Network

Customer Due Diligence Rule

Compliance Date for Covered Financial Institutions

Beginning on May 11, 2018, covered financial institutions were required to comply with FinCEN's Customer Due Diligence Requirements for Financial Institutions (the "CDD Rule"),[47] which was finalized on May 11, 2016. Covered financial institutions subject to the CDD Rule are federally regulated banks and federally insured credit unions, mutual funds, brokers or dealers in securities, futures commission merchants and introducing brokers in commodities.

The CDD Rule requires covered financial institutions to identify, verify and record the identity of the beneficial owners of all legal entity customers, including corporations, limited liability companies, partnerships and similar entities at the time a new account is opened, subject to certain exceptions. In addition, the CDD Rule added a new fifth pillar that must be included in a covered financial institution's AML program: appropriate risk-based procedures for conducting ongoing customer due diligence to understand the nature and purpose of customer relationships and to conduct ongoing monitoring to identify and report suspicious transactions, and, on a risk basis, to maintain and update customer information.

FAQs Regarding the CDD Rule

Prior to the May 2018 compliance date, FinCEN released new FAQs regarding the CDD Rule on April 3, 2018.[48] Among other things, the FAQ responses address the 25% beneficial ownership threshold, methods of verifying beneficial ownership information, collection and maintenance of beneficial ownership information, the scope of the definition of "legal entity customer" and requirements to understand the nature and purpose of a customer relationship.

Administrative Rulings

FinCEN also issued rulings providing certain exceptive relief to covered financial institutions with respect to the CDD Rule. Concurrent with the May 11, 2018 compliance date, FinCEN issued a ruling to provide exceptive relief from the requirement to collect and verify the beneficial owner of a legal entity customer opening a premium financing account when there is a possibility of a cash refund.[49] On September 7, 2018, FinCEN granted exceptive relief from the requirement that covered financial institutions identify and verify the identity of the beneficial owner(s) when a legal entity customer opens a new account as a result of a rollover, renewal, modification or extension of certain types of accounts.[50]

Exceptive Relief

In response to a request from a consortium of banks, the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("Federal Reserve"), the Federal Deposit Insurance Corporation ("FDIC") and the National Credit Union Administration ("NCUA"), collectively the Federal Banking Agencies ("FBAs"), issued an Order, with the concurrence of FinCEN, relieving premium finance companies from their obligation to maintain a customer identification program for commercial customers seeking to finance the purchase of property and casualty insurance policies.[51] Premium finance loans provide short-term financing to businesses to facilitate their purchases of property and casualty insurance policies. According to the Order, FinCEN has determined that these types of loans present a low risk of money laundering because of the purposes for which the loans are extended and limitations on the ability of a customer to use such funds for any other purpose. FinCEN had also previously identified property and casualty insurance policies themselves as not an effective means for laundering money.

This Order represents the first instance in which the FBAs and FinCEN have granted exceptive relief under the authority set forth in 31 C.F.R. § 1020.220(b) implementing section 326(a) of the USA PATRIOT Act, 31 U.S.C. § 5318(l)(5). While limited to the specific facts and analysis identified in the Order, the grant of relief represents a new opening to discuss with financial regulators the reasonable application of AML rules to different products, services and industry sectors.

Joint Statement Encouraging Innovative Approaches to BSA/AML Compliance

On December 3, 2018, FinCEN and the FBAs issued a joint statement to encourage banks to consider, evaluate and, where appropriate, responsibly implement innovative approaches to meet their BSA/AML compliance obligations (for more information, see the White & Case Client Alert available here).[52] Importantly, FinCEN and the FBAs expressed an openness to engagement and dialogue with bank management on innovative approaches to BSA/AML compliance programs that increase the effectiveness of those programs and allow banks to maximize the use of their BSA/AML resources. In particular, the agencies recognized that pilot programs undertaken by banks, in conjunction with existing BSA/AML processes, are an important means of testing and validating the effectiveness of innovative approaches. Banks are encouraged to engage with the agencies early in these pilots, and FinCEN will consider requests for exceptive relief to facilitate testing and potential use of new technologies, provided that banks maintain the overall effectiveness of their BSA/AML programs.

Resource Sharing among Smaller Institutions

FinCEN joined the FBAs in releasing a joint statement to address instances in which banks may decide to enter into collaborative arrangements to share resources to manage their BSA/AML obligations more efficiently and effectively.[53] The statement was directed towards banks with a community focus, less complex operations and lower-risk profiles for money laundering or terrorist financing, and does not does not apply to collaborative arrangements or consortia formed for the purpose of sharing information under Section 314(b) of the USA PATRIOT Act ("Section 314(b)"). The agencies highlighted the following as functions that might be conducted utilizing shared resources: (i) reviewing, updating and drafting BSA/AML policies and procedures;

(ii) reviewing and developing risk-based customer identification and account monitoring processes; and (iii) tailoring monitoring systems and reports for the risks posed.

Advisories

Human Rights Abuses Enabled by Corrupt Senior Foreign Political Figures and their Financial Facilitators

Updating guidance from a decade prior, FinCEN published on June 12, 2018 an advisory highlighting the connection between corrupt senior foreign political figures and their enabling of human rights abuses.[54] The advisory identifies several typologies and red flags, many drawn from sanctions actions, that are indicative of the methods used by corrupt senior foreign political figures to move and hide the proceeds of their corruption. In particular, facilitators may access the financial system to obscure and launder the illicit proceeds of high-level political corruption by using shell companies, misappropriating state assets and exploiting the real estate sector. The advisory reminds financial institutions of their obligations under the BSA to report suspected illicit activity by these facilitators. It also highlights the activities of those who have been subject to sanctions for providing facilitation services to human rights abusers and others engaged in corruption.

Risks of Proceeds of Corruption from Nicaragua

In response to growing political and economic instability in Nicaragua, FinCEN issued an advisory warning financial institutions of the risk of proceeds of crime and corruption entering the US financial system as a consequence of capital flight.[55] FinCEN drew special attention to senior foreign political figures connected to the regime of Nicaraguan President Daniel Ortega, who may be seeking to protect their assets from further unrest, potential sanctions or other factors. While providing a summary of sanctions actions against Nicaraguan officials under the Global Magnitsky sanctions program, which enables Treasury to target corrupt officials, human rights abusers and corrupt actors and their facilitators, the advisory itself did not provide any unique typologies or red flags. Instead, it referred financial institutions to review the red flags in the June 2018 "Advisory on Human Rights Abuses Enabled by Corrupt Senior Foreign Political Figures and Their Financial Facilitators" (above).

Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System

Preceding the full re-imposition on November 5, 2018 of sanctions lifted under the JCPOA, FinCEN issued a detailed advisory to help financial institutions (both domestically and abroad) better detect and, if appropriate, report potentially illicit transactions related to the Islamic Republic of Iran.[56] The advisory highlighted Iran's uses of financial institutions, worldwide, to illicitly access the international financial system and obscure its activities in contravention of US and other sanctions regimes. Relying on extensive case examples from previous sanctions actions, the advisory provided a level of detail that few advisories have provided in the recent past.

Virtual Currency and Fintech Innovation

In his August 9, 2018 remarks, Director Kenneth Blanco discussed FinCEN's approach to virtual currency and financial innovation.[57] Blanco noted that individuals and entities engaged in the business of accepting and transmitting physical currency or convertible virtual currency from one person to another or to another location are money transmitters subject to the AML and CFT requirements of the BSA and its implementing regulations and accordingly must: (i) register with FinCEN as a money services business; (ii) develop, implement and maintain an AML program designed "to prevent the [money service business] from being used to facilitate money laundering and terrorist finance"; and (iii) establish recordkeeping and reporting measures, including filing SARs and Currency Transaction Reports ("CTRs"). Blanco also noted that FinCEN is working closely with the US Securities and Exchange Commission ("SEC") and the Commodity Futures Trading Commission ("CFTC") for coordinated policy development and regulatory approaches and with law enforcement and the DOJ on enforcement matters in the virtual currency space. Blanco again touched on virtual currency and emerging technologies in his August 14, 2018 remarks, a speech in which he also focused on his wish to see more information sharing through the Section 314(b) program and the value of BSA data to law enforcement and regulatory agencies.[58]

In a February 13, 2018 speech, Treasury Under Secretary Mandelker discussed the efforts of Treasury's Officer of Terrorism and Financial Intelligence ("TFI") to track technological innovations involving virtual currency.[59] Through FinCEN, Treasury regulates virtual currency exchangers as money transmitters and requires them to meet BSA obligations. Mandelker noted that virtual currency businesses are subject to comprehensive, routine AML/CFT examinations similar to financial institutions in the securities and futures markets. TFI works in partnership with the IRS to examine virtual currency exchangers under regulations for money transmitters and with the SEC and CFTC to ensure that dealings in virtual currency appropriately address BSA/AML obligations. Mandelker said that TFI is also encouraging international partners to strengthen their virtual currency frameworks, as the lack of AML/CFT regulation of virtual currency providers worldwide greatly exacerbates illicit financing risks. Mandelker reiterated her focus on eliminating vulnerabilities related to technological innovations, including those associated with virtual currencies, in a December 3, 2018 speech.[60]

Geographic Targeting Orders

On November 15, 2018, FinCEN again re-issued and revised its Geographic Targeting Orders ("GTO") directed against the use of shell companies in "all-cash" purchases of residential real estate.[61] First issued in January 2016, the Orders focused only on high-end real estate transactions in Manhattan and Miami-Dade County. The orders have been re-issued and revised several times since then, adding jurisdictions and varying the threshold for reporting based on local property values. In August 2017, Congress expanded FinCEN's GTO authority to include transactions involving wire transfers in Section 275 of CAATSA. In this most recent issuance, the GTOs cover counties in 12 major metropolitan areas: Boston, Chicago, Dallas-Fort Worth, Honolulu, Las Vegas, Los Angeles, Miami, New York City, San Antonio, San Diego, San Francisco and Seattle. The purchase amount threshold is now set at US$300,000 for each covered area and purchases using virtual currencies must be reported.

Enforcement Actions

Civil Money Penalty against US Broker-dealer for Shortcomings in BSA/AML Program for Brokerage and Banking-like Services

On December 17, 2018, FinCEN announced the assessment of a US$14.5 million civil money penalty against a US broker-dealer subsidiary of a large European investment bank, of which US$5 million would be paid to Treasury and the remainder would be paid to the SEC and the Financial Industry Regulatory Authority ("FINRA").[62] According to FinCEN, the broker-dealer failed to develop and implement an appropriate, risk-based BSA/AML program that adequately addressed the risks associated with accounts that included both traditional brokerage and banking-like services. FinCEN found that the company failed to detect and report suspicious activity through certain accounts, particularly accounts that exhibited little to no securities trading, and failed to address the use of securities accounts for the purpose of moving funds rather than trading securities. FinCEN also found that the company failed to allot sufficient resources to BSA/AML compliance, which resulted in failures to timely file SARs. FinCEN specifically acknowledged its close coordination with the SEC and FINRA in the settlement of the action. This matter is discussed further below under "Securities and Exchange Commission" and "Financial Industry Regulatory Authority."

Civil Money Penalty against US Casino for Alleged AML Program Failures

On May 3, 2018, FinCEN assessed a civil money penalty of US$8 million against a casino in California for its failure to implement and maintain an effective AML program and failure to detect and adequately report suspicious transactions in a timely manner.[63] FinCEN suspended US$3 million of the penalty pending the casino's compliance with undertakings to: (i) hire a qualified independent consultant to review the effectiveness of the AML program for each year during a two-year period; (ii) employ a compliance officer to ensure day-to-day compliance with obligations under the BSA; (iii) adopt and implement an AML program that includes policies, procedures and internal controls for obtaining and utilizing information from propositional players and creating, retaining and utilizing records related to backline betting, kum kum betting and kum kum banking; (iv) hire a qualified independent consultant to conduct a "look-back"; and (v) certify compliance with the undertakings.

US$613 million Civil Money Penalty against US Commercial Bank for Alleged Transaction Monitoring and Suspicious Activity Reporting Failures

On February 15, 2018, FinCEN, along with the DOJ, OCC and Federal Reserve, announced US$613 million in penalties against a US bank holding company and its national bank subsidiary for BSA violations.[64]

The DOJ entered into a deferred prosecution agreement with the bank holding company related to charges that it had, through the bank subsidiary, failed to establish and implement an adequate AML program from at least 2011 to 2014 and failed to report certain suspicious activity from at least 2011 to 2013.[65] The DOJ found that the bank capped the number of alerts generated by its transaction monitoring systems based on staffing levels and resources and failed to monitor non-customer transactions by a prominent money transfer company at branches of the bank, which resulted in the bank failing to monitor, investigate and report substantial numbers of suspicious transactions flowing through the bank. In addition, the deferred prosecution agreement provides that the bank's then Chief Compliance Officer concealed the bank's practices from the OCC. The DOJ also found that the bank willfully failed to timely report suspicious banking activities of a longtime customer, despite being on notice of facts giving rise to suspicion that the customer had used and was using the bank to launder more than US$2 billion of proceeds from an illegal payday lending scheme. The bank also entered into a consent order with the OCC,[66] while the bank holding company and a subsidiary of the bank entered into a consent order with the Federal Reserve.[67]

In addition to the findings of the DOJ, OCC and the Federal Reserve, FinCEN also determined that the bank filed thousands of CTRs from 2014 to 2015 that provided materially inaccurate information by failing to provide the names of the money services businesses that were the ultimate beneficiaries of the transactions.[68]

The US$613 million in penalties included a US$453 million civil forfeiture to the DOJ, a US$15 million penalty imposed by the Federal Reserve, a US$75 million penalty imposed by the OCC and a US$70 million penalty imposed by FinCEN.[69]

Section 311 Action against Latvian Bank Results in Bank's Resolution

On February 13, 2018, FinCEN issued a finding and notice of proposed rulemaking, pursuant to Section 311 of the USA PATRIOT Act ("Section 311"), seeking to prohibit the opening or maintaining of a correspondent account in the United States for, or on behalf of, a Latvian bank.[70] FinCEN's action was based on its finding in the proposed rulemaking that the Latvian bank was a foreign bank of primary money laundering concern. According to FinCEN, the bank had institutionalized money laundering as a pillar of the bank's business practices, with its management permitting the bank and its employees to orchestrate money laundering schemes, solicit high-risk shell company activity that enabled the bank and its customers to launder funds, maintain inadequate controls over high-risk shell company accounts and seek to obstruct enforcement of Latvian AML/CFT rules in order to protect such business practices.

Section 311 grants FinCEN the authority to alert the US financial sector to foreign institutions that are of primary concern and, through the public rulemaking process, cut them off from the US financial sector, if necessary. To invoke this authority, FinCEN must find that reasonable grounds exist for concluding that a jurisdiction outside of the United States, one or more financial institutions operating outside of the United States, one or more classes of transactions within or involving a jurisdiction outside of the United States, or one or more types of accounts is of primary money laundering concern. In its proposed rulemaking, FinCEN proceeded on the basis of the fifth special measure of Section 311, which permits FinCEN to prohibit or impose conditions on the opening or maintaining in the United States of correspondent or payable-through accounts for, or on behalf of, a foreign banking institution, if such correspondent account or payable-through account involves a foreign financial institution found to be of primary money laundering concern.

On February 23, 2018, the European Central Bank ("ECB") determined that the bank was failing or likely to fail and would be resolved under the laws of Latvia and Luxembourg.[71] The ECB noted that following FinCEN's

February 13 announcement, the bank experienced an abrupt wave of withdrawals of deposits and a lack of access to US dollar funding, which resulted in the bank being unable to make payments in US dollars.

Department of Justice

Agency Coordination and "Piling On"

On May 9, 2018, Deputy Attorney General Rosenstein announced a new policy to encourage coordination among the DOJ and other government enforcement agencies when imposing multiple penalties for the same conduct, with the goal of enhancing coordination while avoiding duplicative penalties, or "piling on."[72] Rosenstein named the SEC, CFTC, Federal Reserve, FDIC, OCC and OFAC as agencies with which the DOJ coordinates and noted that additional federal, state, local and foreign authorities are interested in joining the DOJ's efforts. The policy provides no private right of action and is not enforceable in court, but has been incorporated into the US Attorneys' Manual and is intended to guide the DOJ's decisions.

Among other things, the policy provides that:

- In parallel and/or joint corporate investigations and proceedings involving multiple DOJ components and/or other federal, state or local enforcement authorities, DOJ attorneys should remain mindful of their ethical obligation not to use criminal enforcement authority unfairly to extract additional civil or administrative monetary payments.
- In resolving a case with a company that multiple DOJ components are investigating for the same misconduct, DOJ attorneys should coordinate with one another to avoid the unnecessary imposition of duplicative fines, penalties and/or forfeiture against the company.
- The DOJ should, as appropriate, coordinate with and consider the amount of fines, penalties and/or forfeiture paid to other federal, state, local or foreign enforcement authorities that are seeking to resolve a case with a company for the same misconduct.
- The DOJ should consider all relevant factors in determining whether coordination and apportionment is appropriate, including the egregiousness of a company's misconduct, statutory mandates regarding penalties, fines and/or forfeitures, the risk of unwarranted delay in achieving a final resolution and the adequacy and timeliness of a company's disclosures and its cooperation with the DOJ.

The following month, the Federal Reserve, FDIC and OCC issued a joint statement regarding coordination among federal banking agencies during formal enforcement actions.[73] The statement provides that when a federal banking agency determines it will take a formal enforcement action, it should evaluate whether the enforcement action involves the interests of another agency and, if so, the agency proposing the enforcement action should notify the other agency. If two or more agencies consider bringing a complementary action, they should coordinate the preparation, processing, presentation, potential penalties, service and follow-up of the enforcement action.

Focus on Individual Wrongdoing

In the speech in which he announced the "piling on" policy, Deputy Attorney General Rosenstein also discussed the DOJ's focus on identifying and holding accountable culpable individuals within firms, with the goal in every case to reduce the likelihood of future violations by punishing individual wrongdoers.

Enforcement Actions

Deferred Prosecution Agreement and Penalties of US$1.34 billion in Connection with Global European Bank's Alleged Violations of Cuba Sanctions

On November 19, 2018, the DOJ announced criminal charges against a global European bank for allegedly conspiring to violate the Trading with the Enemy Act ("TWEA") and its implementing regulations for the bank's role in processing billions of dollars of US dollar transactions using the US financial system in connection with credit facilities involving Cuba.[74] Various other federal agencies are imposing civil penalties against the bank.

The bank agreed to a deferred prosecution agreement, under which it must pay penalties exceeding US$1.34 billion to federal and state prosecutors and regulators, refrain from all future criminal conduct and implement remedial measures. The penalty is composed of a US$717.2 million civil forfeiture action, US$162.8 million to the New York County District Attorney's Office, US$53.9 million to OFAC, US$81.3 million to the Federal Reserve and US$325 million to DFS.

According to documents filed by the DOJ, from approximately 2004 through 2010, the bank operated 21 credit facilities that provided significant money flow to Cuban banks, entities controlled by Cuba and Cuban and foreign corporations for business conducted in Cuba, which "Cuban Credit Facilities" involved substantial US-cleared payments through US financial institutions, in violation of TWEA and the Cuban Regulations. In total, the bank allegedly engaged in more than 2,500 sanctions-violating transactions amounting to close to US$13 billion through US financial institutions. The DOJ found that the bank avoided detection, in part, by making inaccurate or incomplete notations on payment messages that accompanied these sanctions-violating transactions in a deliberate practice of concealing the Cuban nexus of US dollar payments that were made in connection with those facilities. According to the filings, despite the awareness of the bank's senior management and compliance group that the bank had engaged in this unlawful conduct, the bank did not disclose its conduct to OFAC or any other US regulator or law enforcement agency until well after the commencement of the US government's investigation.

National Bank Subsidiary of Netherlands Banking Group Pleads Guilty to Felony Conspiracy for Concealing AML Program Deficiencies and Obstructing OCC Examinations

On February 7, 2018, a US national bank subsidiary of a Netherlands-based banking group pled guilty to felony conspiracy for impairing, impeding and obstructing the OCC, its primary regulator, by concealing deficiencies in its AML program and obstructing OCC examinations. The bank was required to forfeit over US$368 million.[75]

According to filings, the bank received regular alerts of transactions by "High-Risk" customers, or through accounts deemed to be "High-Risk," that had been the subject of prior SARs filed by the bank, many sourced from Mexico. The bank allegedly created and implemented policies and procedures to prevent adequate investigations into these suspicious transactions, customers and accounts. This included a "Verified List," whereby the bank purportedly instructed employees that no further review of transactions involving customers on the "Verified List" was required, regardless of risk indicators. The bank allegedly encouraged its staff to increase the size of the "Verified List" between 2009 and 2012. The bank admitted to failing to monitor and conduct adequate investigations into these transactions and to submit SARs to FinCEN. In addition, the bank solicited cash-intensive customers from Mexico and elsewhere, but failed to employ adequate BSA/AML policies and procedures to address the known associated risks.

According to the DOJ, three bank executives agreed to knowingly obstruct the OCC's 2012 periodic examination, including by providing the OCC with false and misleading information about the bank's BSA/AML program and making false and misleading statements to the OCC regarding the existence of reports by a third-party consultant detailing the deficiencies and resulting ineffectiveness of the bank's BSA/AML program. Further, the bank demoted or terminated two employees who raised questions about the adequacy of the BSA/AML program.

In connection with the guilty plea, the OCC issued a consent order and imposed a US$50 million civil money penalty related to failings of the bank's BSA/AML program and its obstruction of the OCC's examinations.[76] On April 16, 2018, the OCC filed a civil case against the bank's former Chief Compliance Officer for allegedly concealing from the OCC a report prepared by a consulting firm that identified deficiencies with the bank's BSA/AML program.[77] The OCC seeks a civil money penalty of US$50,000 and an industry employment bar.

Office of the Comptroller of the Currency

BSA/AML Compliance as a Key Supervisory Focus and Risk

Throughout 2018, the OCC emphasized BSA/AML compliance as a key supervisory focus and risk for institutions. In its Fall 2018 Semiannual Risk Perspective, the OCC reported that BSA/AML compliance risk remains elevated in light of the complex environment in which banks operate. Of particular note, the OCC cautioned that the underlying technology that supports innovation in fintech and regtech and development of product and service solutions may also be used to facilitate illicit activity, thereby increasing BSA/AML and OFAC risk exposure.[78] The OCC struck a similar theme in its Fiscal Year 2019 Bank Supervision Operating Plan, saying that it plans to continue its emphasis on determining whether AML compliance programs are keeping pace with changing risk environments and regulatory developments.[79]

In June testimony before the House Financial Services Committee and Senate Committee on Banking, Housing, and Urban Affairs ("Senate Banking Committee"), Comptroller of the Currency Joseph Otting discussed the OCC's desire to enhance and make more efficient BSA/AML compliance.[80] Comptroller Otting highlighted several potential improvements, which could be pursued through legislation, and in some case regulatory, action:

- Allowing regulators to schedule and scope BSA/AML examinations on a risk-basis and identifying ways to conduct associated examinations in a more efficient manner;
- Considering changes to the threshold requiring mandatory reporting of SARs and CTRs and simplifying reporting forms and requirements;
- Working with law enforcement to provide feedback to banks so that they understand how SARs and other BSA report filings are used and can provide the most useful information; and
- Exploring the use of technologies to reduce reporting burden and provide more effective access.

Enforcement Actions

Civil Money Penalty Against US Commercial Bank for Failure to Achieve Compliance with 2015 Consent Order and Subsequent SAR Shortcomings

On October 23, 2018, the OCC announced its assessment of a US$100 million civil money penalty against two affiliated national banks for deficiencies in their respective BSA/AML programs.[81] The penalty is related to the OCC's 2015 consent order issued to the banks, which identified failures to adopt and implement compliance programs that adequately cover the required BSA/AML program elements due to an inadequate system of internal controls and ineffective independent testing and to file all necessary SARs.[82] The OCC found that the banks failed to timely achieve compliance with the 2015 consent order from July 1, 2016 to July 6, 2017, and, subsequent to the 2015 consent order, failed to file additional SARs and initiated wire transfer transactions that contained inadequate or incomplete information.[83]

Industry Bar and US$100,000 Civil Money Penalty against Former Employee of Miami Branch of Canadian Bank

On September 12, 2018, the OCC issued a consent order against a former employee of the Miami, Florida, branch of a Canadian bank, barring him from industry employment and imposing a US$100,000 civil money penalty.[84] The OCC found that, from January to November 2013, the employee facilitated transactions to allow clients and others to make international money transfers between Brazil and the United States, which transactions were for high-risk clients and other individuals residing in a high-risk jurisdiction, and the majority of which had no known legal or business purpose. The employee did not conduct adequate due diligence on the transactions or on the parties to the transactions. The OCC found that the individual withheld material information and concealed certain information from the bank regarding these activities.

Civil Money Penalties Assessed against Former Executives of Bank and Trust Company

On June 21, 2018, the OCC issued consent orders against two former executives of a Florida bank and trust company.[85] The OCC found that the individuals, each of whom had BSA/AML compliance responsibilities within the organization, helped to author a report recommending opening accounts for a family relationship with close ties to a previously proposed relationship that was declined for BSA/AML risk reasons. The report failed to include publicly available negative news and the close connection between the proposed relationship and the previously declined relationship. The OCC imposed respective civil money penalties of US$15,000 and US$35,000.

Civil Money Penalties and Industry Bars against Former Executives and Directors of California Bank Previously Subject to OCC Action

From February through April 2018, the OCC issued consent orders against seven former executives and directors of a small California national bank, which was itself the subject of an OCC consent order for BSA compliance violations in February 2017.[86] The OCC made the following findings and imposed the following penalties:

- The former president, chief executive and chairman caused or participated in violations of previous consent orders against the bank, failed to take necessary actions to correct deficiencies resulting in the previous consent orders, knowingly caused the bank's risk profile to increase by recruiting higher-risk businesses as clients without ensuring the bank had a commensurate BSA/AML program to manage such risk and circumvented account opening procedures, including customer due diligence and enhanced due diligence procedures (US$175,000 penalty, removal and industry employment bar).[87]
- The former executive vice president and director caused or participated in violations of previous consent orders against the bank, failed to take necessary actions to correct deficiencies resulting in the previous consent orders and knowingly caused the bank's risk profile to increase by recruiting higher-risk businesses as clients without ensuring the bank had a commensurate BSA/AML program to manage such risk (US$70,000 penalty and industry employment bar).[88]
- The former executive vice president and chief financial officer circumvented account opening procedures, including customer due diligence and enhanced due diligence procedures (US$20,000 penalty).[89]
- A former chairman of the board caused or participated in violations of previous consent orders against the bank and failed to take necessary actions to correct deficiencies resulting in the previous consent orders (US$20,000 penalty).[90]
- The chief banking officer and former chief operating officer caused or participated in violations of previous consent orders against the bank, failed to take necessary actions to correct deficiencies resulting in the previous consent orders, hindered the BSA department's effectiveness by interfering with the BSA officer's ability to make risk determinations and remediate deficiencies, knowingly made false statements to the OCC and failed to ensure that the bank's operations department had sufficient internal controls (US$5,000 penalty).[91]
- Two former directors caused or participated in violations of previous consent orders against the bank and failed to take necessary actions to correct deficiencies resulting in the previous consent orders (each, a US$5,000 penalty).[92]

Civil Money Penalty Against New York Branch of Chinese Bank for Various Shortcomings in BSA/AML and OFAC Compliance

On April 24, 2018, the OCC issued a consent order against the New York branch of a Chinese bank for deficiencies in the branch's BSA/AML compliance program and compliance with OFAC requirements.[93] The shortcomings identified by the OCC include: (i) an inadequate system of internal controls, ineffective independent testing, a weak BSA Officer function and insufficient training; (ii) systemic deficiencies in transaction monitoring systems, resulting in alert and investigation backlogs and failures to file SARs in a timely manner; and (iii) systemic deficiencies in customer due diligence, enhanced due diligence and customer risk rating processes. The OCC imposed a US$12.5 million civil money penalty.

Consent Orders to Washington and New Jersey National Banks Requiring Improvements in BSA/AML Compliance

In February 2018, the OCC issued consent orders to national banks based in Washington and New Jersey, in each case requiring the respective bank to take a series of actions to develop, implement and comply with an adequate BSA/AML compliance program.[94]

Federal Reserve Board

Risks of Cryptocurrencies

In a May 15, 2018 speech concerning cryptocurrencies, digital currencies and distributed ledger technologies, Federal Reserve Governor Lael Brainard discussed the BSA/AML vulnerability of some cryptocurrencies. Governor Brainard argued that cryptocurrencies that store in their ledger little to no information about the identity of owners essentially mimic a bearer instrument, whereby the holder is presumed to be its owner. Governor Brainard raised the concern that digital currencies that mimic bearer instruments and can be used across borders have the potential to facilitate illicit activities and associated money laundering.[95]

Enforcement Actions

Fine Against Global European Bank for Apparent Violations of Cuba Sanctions

On November 19, 2018, the Federal Reserve announced that it had fined a global European bank US$81.3 million for its unsafe and unsound practices, primarily related to violations of US sanctions against Cuba.[96] This matter is discussed in greater detail above under "Department of Justice."

Civil Money Penalty against US Operations of Taiwan-based Bank for BSA/AML Violations

On January 17, 2018, the Federal Reserve and the Illinois Department of Financial and Professional Regulation, Division of Banking, announced a US$29 million penalty against the US operations of a Taiwan-based bank for BSA/AML violations.[97] According to the consent order, the applicable regional Federal Reserve Banks discovered significant deficiencies relating to the risk management and BSA/AML compliance of the bank's New York, Chicago and Silicon Valley branches.[98] In addition to the monetary penalty, the bank is required to strengthen the board of directors and US senior management oversight of BSA/AML compliance across its US operations. Each of the named branches is required to submit enhanced BSA/AML compliance programs to the applicable regional Federal Reserve Bank and, in the case of the Chicago branch, to the Illinois Division of Banking.

Agreements with Banks Requiring Improved BSA/AML Compliance

On October 22, 2018, the Federal Reserve Bank of Kansas City and the Oklahoma State Banking Department entered into an agreement with an Oklahoma bank that requires the bank to, among other measures, submit a written plan to improve the bank's BSA/AML compliance program.[99]

On July 2, 2018, the Federal Reserve Bank of New York entered into an agreement with a bank based in Pakistan and its New York branch requiring the bank to adopt a written plan to enhance BSA/AML and OFAC compliance and to retain an independent third party to conduct a comprehensive compliance review.[100]

On March 12, 2018, the Federal Reserve issued a consent order against a Chinese bank and its New York branch requiring the branch to adopt a written plan to enhance BSA/AML and OFAC compliance and to retain an independent third party to conduct a review of its US dollar clearing transaction activity from July 1, 2016, through December 31, 2016 to determine whether suspicious activity involving high risk customers or transactions at, by or through the branch was properly identified and reported.[101]

Federal Deposit Insurance Corporation

BSA/AML and Technological Change

In November 13, 2018 remarks, FDIC Chairman Jelena McWilliams noted that the FDIC will keep an open mind to technological changes, discussing how advancements in technology and data analytics will change the way the FDIC and other regulators approach oversight, particularly in the areas of BSA/AML compliance. Chairman McWilliams said that new technology can introduce risk, but it can also help regulators and institutions identify and mitigate risk sooner and can present opportunities to ease regulatory compliance burdens.[102]

Enforcement Actions

Ninth Circuit Upholds FDIC's Reliance on FFIEC BSA/AML Examination Manual in Assessing Penalties

On March 12, 2018, the Ninth Circuit upheld the FDIC's assessment of penalties against a California bank, holding in relevant part that the BSA and its implementing regulations were not unconstitutionally vague and that the FDIC lawfully relied on the Federal Financial Institutions Examination Council's ("FFIEC") BSA/AML Examination Manual.[103] While recognizing that interpretations, like those contained in policy statements, agency manuals and enforcement guidelines, lack the force of law, the panel held that such interpretations "can clarify what conduct is expected of a person subject to a particular regulation and thus mitigate against vagueness."[104] This ruling strengthens the amount upon which financial institutions should rely on the FFIEC BSA/AML Examination Manual for guidance on examiner expectations.

Interestingly, the FDIC, along with the Federal Reserve, OCC and NCUA, issued an interagency statement in September 2018 to clarify the role of supervisory guidance.[105] Among the practices that the FBAs sought to clarify is that examiners would not criticize a supervised financial institution for a "violation" of supervisory guidance. However, in some situations, examiners may refer to such guidance to provide examples of safe and sound conduct, appropriate consumer protection and risk management practices, and other actions for addressing compliance with laws or regulations to highlight unsafe or unsound practices.

Consent Agreement with Small South Carolina Bank Regarding BSA/AML and OFAC Compliance

On September 24, 2018, the FDIC entered into a consent agreement with a small South Carolina bank that requires the bank to revise its BSA program to ensure compliance with all BSA/AML and OFAC requirements.[106] The bank is also required to perform a risk assessment, the results of which must inform a revised system of internal controls addressing, at a minimum, suspicious activity monitoring and reporting, customer due diligence and enhanced due diligence.

Consent Agreement with Small Maryland Bank Regarding BSA/AML Compliance

On April 26, 2018, the FDIC issued a consent order against a small Maryland bank requiring the bank to, among other things, revise and implement a system of internal controls designed to ensure full compliance with BSA requirements, addressing, at a minimum, suspicious activity monitoring and reporting, customer due diligence and enhanced due diligence.[107]

Securities and Exchange Commission

Cryptocurrencies

In February 6, 2018 testimony before the Senate Banking Committee, SEC Chairman Jay Clayton said the SEC is monitoring the cryptocurrency-related activities of the market participants it regulates, including brokers, dealers, investment advisers and trading platforms, and noted that such market participants should be ensuring that their cryptocurrency activities are not undermining their AML and know-your-customer obligations.[108] Chairman Clayton testified that market participants should treat payments and other transactions made in cryptocurrency as if cash were being handed from one party to the other.

Enforcement Actions

Settlement with US Broker-dealer for Failing to Report Suspicious Transactions in Customer Accounts

On December 17, 2018, the SEC announced settled charges against a US broker-dealer subsidiary of a large European investment bank for failing to report suspicious transactions in customer accounts, in an action coordinated with FinCEN and FINRA.[109] According to the SEC, the company failed to file SARs on certain suspicious movements of funds through its customers' accounts from at least 2011 to 2013 and did not properly review suspicious transactions flagged by its internal monitoring systems and failed to detect suspicious transactions involving the movement of funds between certain accounts in suspicious long-term patterns. This matter is discussed in greater detail above under "Treasury's Financial Crimes Enforcement Network" and below under "Financial Industry Regulatory Authority."

Settlement with Investment Banking and Securities Brokerage Firm regarding Alleged SAR Shortcomings

On July 9, 2018, the SEC announced that it had settled charges set forth in a complaint against a US banking and securities brokerage firm that the firm had failed to file SARs on suspicious transactions of independent advisers that it terminated from using the firm to custody client accounts.[110] The complaint alleges that the firm terminated 83 independent advisers in 2012 and 2013 for engaging in activity that the firm determined violated its internal policies and presented risk to it or its customers, but failed to file SARs on the suspicious transactions of 37 of these terminated advisers. The SEC found that the firm did not have clear or consistent policies and procedures regarding the types of transactions on which SARs needed to be filed and in certain instances "applied an unreasonably high standard" for determining whether to file a SAR. The SEC cited the following examples of failures to file SARs where the firm suspected or had reason to suspect that the terminated adviser had engaged in a range of suspicious transactions not involving the outright misappropriation or misuse of client funds: (i) transactions involving possible undisclosed self-dealing or conflicts of interest; (ii) charging client accounts excessive advisory fees; (iii) potentially fraudulent transactions in client accounts; (iv) posing as a client to effect or confirm transactions in the client account; and (v) executing client trades and/or collecting advisory fees without being properly registered as an adviser. The firm agreed to pay a US$2.8 million civil penalty under the settlement.

SEC Wins Partial Summary Judgment in US District Court Case regarding Complaint against Brokerage Firm for SAR Deficiencies

On March 30, 2018, the United States District Court for the Southern District of New York granted in part the SEC's motion for summary judgement in a case stemming from the SEC's 2017 complaint against a Utah-based brokerage firm for violations related to its alleged practice of clearing transactions for microcap stocks that were allegedly used in manipulative schemes to harm investors.[111] The SEC alleged that the firm, which acted as a clearing broker-dealer, routinely and systematically failed to file SARs for stock transactions that it flagged as suspicious, and in the SARs that it did file, frequently omitted the information that formed the bases for its suspicion. The SEC also alleged that the firm was not timely in filing certain of SARs. The brokerage unsuccessfully moved for summary judgment on the ground that the SEC lacks the delegated authority to bring enforcement actions seeking civil penalties for violations of the BSA. The court granted in part summary judgment in favor of the SEC with respect to its allegations that the firm failed to file SARs in certain situations, filed inadequate SARs in other instances and filed certain SARs up to 211 days late. In reaching its decisions with respect to the late SARs, the court relied on FinCEN guidance from May 2006[112] to determine that the firm's 30-day window to file each of the five SARs in question was triggered when the information that triggered the duty to file the SAR was available to the firm, which was "the very time that the five transactions reported in these SARs occurred."

Settlement with US- and China-based Broker-dealers and Employee for Alleged SAR Failures

On May 16, 2016, the SEC announced settled charges against broker-dealers in New York and China for failing to report suspicious sales of billions of penny stock shares.[113] The SEC stated that, from October 2013 to June 2014, the New York firm, acting as an introducing broker, liquidated more than 12.5 billion penny stock shares for seven customers, with the Chinese firm clearing the transactions. The New York firm did not file any SARs for the transactions, despite red flags including similar trading patterns and sales in issuers who lacked revenues and products. The Chinese firm also failed to file any SARs for the transactions, although it did prohibit trading in penny stocks by certain of the seven customers. The New York firm agreed to a settlement requiring it to pay a US$1 million penalty,[114] while the Chinese firm agreed to a settlement requiring it pay a US$860,000 penalty.[115] In addition, the New York firm's AML officer, who the SEC found aided and abetted and caused the firm's violations, agreed to a settlement requiring him to pay a US$15,000 penalty and subjecting him to industry and penny stock bars for at least three years.[116] In a related settlement, the Chinese firm agreed to pay FINRA a US$5.3 million penalty and retain an independent compliance consultant.[117]

Settlement with New York Brokerage and Certain Employees for Failure to File SARs

On March 28, 2018, the SEC announced a settlement with a New York-based brokerage firm after finding that the firm had violated the BSA by failing to file SARs on suspicious transactions that raised red flags indicating the transactions were potentially related to the market manipulation of low-priced securities.[118] The firm agreed to pay a US$750,000 penalty and to adopt the recommendations of an independence compliance expert,[119] and, under a separate consent with FINRA, agreed to pay an additional US$550,000 penalty.[120]

The SEC found the firm's chief executive officer to have caused the BSA violations and two former compliance officers to have aided and abetted the violations and under a separate settlement the individuals agreed to pay penalties of US$40,000, US$20,000 and US$20,000, respectively.[121] One of the former compliance officers also agreed to a prohibition from serving in a compliance or AML capacity in the securities industry.

Financial Industry Regulatory Authority

Fine of Multinational Investment Bank for Alleged AML Failures Spanning Over Five Years

On December 26, 2018, FINRA announced that it had imposed a US$10 million fine on a US-based multinational investment bank for purported BSA/AML program and supervisory failures spanning more than five years.[122] FINRA found the company's BSA/AML program exhibited three primary shortcomings: (i) the AML surveillance system did not receive critical data from several systems, undermining the firm's surveillance of tens of billions of dollars of wire and foreign currency transfers, including transfers to and from countries known for having high money-laundering risk; (ii) the firm failed to devote sufficient resources to review alerts generated by its automated AML surveillance system, and consequently its analysts often closed alerts without sufficiently conducting and/or documenting their investigations of potentially suspicious wire transfers; and (iii) the firm's AML Department did not reasonably monitor customers' deposits and trades in penny stock for potentially suspicious activity. FINRA also found that the company failed to implement its policies, procedures and controls to ensure that it conducted risk-based reviews on a periodic basis of the correspondent accounts maintained for certain foreign financial institutions. FINRA considered the "extraordinary corrective measures" the firm took to expand and enhance its AML-related programs when determining the fine amount.

Settlement with US Broker-dealer for Failing to Report Suspicious Transactions in Customer Accounts, including Foreign Currency Wire Transfers and Penny Stocks

On December 17, 2018, in connection with related actions by FinCEN and the SEC, FINRA announced a US$4.5 million fine of a US broker-dealer subsidiary of a large European investment bank for failing to establish and implement BSA/AML programs reasonably designed to monitor certain high-risk transactions in customer accounts, including foreign currency wire transfers.[123] In addition, FINRA imposed a US$500,000 fine on an affiliate of the company for failing to establish and implement BSA/AML programs reasonably designed to monitor certain high-risk transactions in penny stocks. This matter is discussed in greater detail above under “Treasury’s Financial Crimes Enforcement Network” and “Securities and Exchange Commission.”

Settlement with Proprietary Trading and Retail Securities Firm for Deficient BSA/AML Program

On August 3, 2018, FINRA reached a settlement with a proprietary trading and retail securities firm with respect to its failure to develop and implement an AML program reasonably designed to comply with the BSA.[124] FINRA found that the company failed to establish and implement policies and procedures that could reasonably be expected to detect and cause the reporting of potentially suspicious activity relating to the liquidation of shares of low-priced securities. Specifically, FINRA found that the manual review employed by the firm was not reasonably designed to detect patterns of potentially suspicious activity that might occur over time, and that the firm failed to detect activities as potentially suspicious despite numerous red flags. The firm was assessed a US$40,000 penalty in connection with the settlement.

Settlement with US Brokerage Firm regarding Shortcomings in AML Procedures

On May 22, 2018, FINRA reached a settlement with a retailer of foreign sovereign debt, listed US equity securities, structured notes and mutual funds which worked with foreign introducers that referred specific transactions to the firm.[125] FINRA found that the firm’s AML procedures did not identify whether the foreign introducers were high-risk entities or engaged in high-risk activities and did not adequately review the foreign introducers’ referred transactions or wire transactions for red flags. In addition, FINRA found that the firm’s AML program was insufficient to identify and investigate potentially suspicious patterns of outgoing wire transfer activity in the Swiss bank accounts of its customers that were dual customers of the firm and its Swiss bank affiliate. The firm agreed to pay an US$800,000 penalty and to adopt and implement revised supervisory systems and written procedures.

Settlement with Broker/Investment Advisor for Inadequate Detection and Investigation of Suspicious Transactions

On April 10, 2018, FINRA reached a settlement with an Arkansas-based broker and investment advisor that generates revenues through equities, mutual funds and an investment advisory business.[126] FINRA found that the company did not adequately detect and investigate potentially suspicious transactions occurring in certain accounts of longtime customers for purposes of determining whether to file SARs. The company allegedly did not adequately implement its AML written procedures by investigating potentially suspicious money movement, and instead relied on its clearing firm to raise red flags. In addition, FINRA found that the firm’s annual independent AML compliance program tests were inadequate. The firm agreed to pay a US$200,000 penalty.

Settlement with Securities Firm for Failure to Identify and Document Potentially Suspicious Transactions

On March 28, 2018, FINRA reached a settlement with a securities firm for its failure to identify and in some cases document its detection and investigation of potentially suspicious transactions involving customer accounts that engaged primarily in high levels of money movement with little or no corresponding securities transactions.[127] The firm agreed to pay a US$100,000 penalty and to adopt and implement revised supervisory systems and written procedures.

Settlement with Brokerage Services Provider for Inadequate Monitoring of Liquidation of Microcap Securities

On January 2, 2018, FINRA reached a settlement with a New York-based brokerage services provider in connection with its failure to establish and implement policies and procedures that could be reasonably expected to detect and cause the reporting of potentially suspicious activity relating to the liquidation of millions of shares of microcap securities.[128] FINRA found that, given the high volume transactions, the firm’s manual surveillance methods were not reasonably designed to detect patterns of suspicious activity that might occur over time. The firm agreed to pay a US$70,000 penalty and to submit a certification that its policies, systems and procedures and training are reasonably designed with respect to the firm's compliance with FINRA rules and BSA requirements.

Commodity Futures Trading Commission

Enforcement Action for Alleged Failure to Register as a Futures Commission Merchant ("FCM") and Implement AML Procedures

On September 27, 2018, the CFTC filed a civil enforcement action in the US District Court for the District of Columbia against a Marshall Islands-based firm and its chief executive officer and owner.[129] The complaint charges the defendants with engaging in unlawful retail commodity transactions, failing to register as a FCM and supervisory violations for failing to implement procedures to prevent money laundering.[130] An entity that is required to be registered as an FCM must maintain and implement an adequate supervisory system that includes KYC/customer identification program procedures to prevent money laundering and other illicit activity. The CFTC seeks, among other things, monetary penalties and a permanent injunction prohibiting the defendants from engaging in the conduct discussed in the complaint.

New York State Department of Financial Services

Enforcement Actions

US$40 million Fine against United Arab Emirates Bank and its New York Branch for Compliance Deficiencies

On October 10, 2018, DFS announced that it had fined a bank based in the United Arab Emirates and its New York branch US$40 million for violations of BSA/AML laws in the New York branch's US dollar clearing operations.[131] Pursuant to a consent order, the bank must immediately hire a third-party compliance consultant to oversee and address deficiencies in the branch's compliance function, including compliance with BSA/AML requirements, federal sanctions laws and New York law and regulations. [132] The bank must also hire a third party "lookback consultant" to conduct a review of the branch's transaction clearing activity for April 2016 to September 2016, along with other remedial actions. The bank is also required to submit to DFS a written revised BSA/AML compliance program for the New York branch, a written program for the reporting by the New York branch of all known or suspected violations of law or suspicious transactions to law enforcement and supervisory authorities, a written enhanced customer due diligence program and a written plan to enhance oversight, by the management of the bank and the New York branch, of the branch's compliance with BSA/AML requirements, New York State laws and regulations and OFAC regulations. The consent order is the result of examinations by DFS and the Federal Reserve Bank of New York.

US$60 million Fine against Worldwide Money Transfer Company following Related Action by Federal Agencies

On January 4, 2018, DFS announced that it fined a prominent money transfer company US$60 million in connection with a consent order for violations of New York BSA/AML laws.[133] The consent order followed a DFS investigation, which found that between at least 2004 and 2012, the firm willfully failed to implement and maintain an effective AML program to prevent and report suspected criminal fraud, money laundering and illegal "structuring" schemes (executing a transaction in a specific pattern, such as breaking up a larger sum into smaller transactions, pattern, to avoid triggering reporting obligations). According to DFS, despite having evidence that a substantial number of its agents were engaging in suspicious activity, the company continued to maintain relationships with such partners and never disclosed the suspicious activity to DFS. The company's parent previously entered in a deferred prosecution agreement with the DOJ, settled civil charges brought by the Federal Trade Commission and consented to a civil monetary penalty imposed by FinCEN in connection with the activities giving rise to the DFS action.[134]

Proposed Legislative Changes to BSA/AML Policy

The 115th Congress considered various legislative proposals to modernize the BSA. Several notable pieces of legislation were introduced that would have, among other things, required the collection of beneficial ownership information at the time of an entity's formation, increased the dollar threshold for SAR reporting and otherwise revised the SAR process, permitted SAR sharing with foreign branches and affiliates, expanded the purposes for which information can be shared under Section 314(b) and created a FinCEN no-action letter procedure (see the table below for notable legislative proposals). Certain bills were passed by the House, but no such legislation has yet received full consideration by both houses.

Both the Senate Banking Committee and House Financial Services Committee expressed bipartisan interest in BSA reform throughout 2018. The Senate Banking Committee held hearings at which it considered possible reforms in January and November 2018, and BSA/AML reform was also on the agenda during hearings of other House and Senate committee hearings throughout 2018.[135] Regulator testimony at these hearings demonstrated several areas of potential reform:

- **Information sharing**: In November testimony before the Senate Banking Committee, Grovetta Gardineer of the OCC discussed the OCC's support of legislation to expand the information sharing safe harbor in Section 314(b) beyond money laundering and terrorist financing to include mortgage fraud, cyber fraud and other financial crimes, and to eliminate or modify the notice requirement to FinCEN, which may limit the ability of financial institutions to share information.[136]
- **Reporting thresholds**: In June testimony before the House Financial Services Committee, Comptroller of the Currency Joseph Otting expressed his support for legislation to change the threshold requiring mandatory reporting of SARs and CTRs and simplify reporting forms and requirements.[137] In November testimony before the Senate Banking Committee, FinCEN Director Kenneth Blanco and Steven D'Antuono of the Federal Bureau of Investigation ("FBI") cautioned against any changes to thresholds that could reduce the amount of information made available to law enforcement.[138]
- **Beneficial ownership**: In February testimony before the Senate Judiciary Committee, Acting Deputy Assistant Attorney General M. Kendall Day of the Criminal Division stated that the CDD Rule should be considered just the first step toward greater transparency.[139] Day called for legislative action to "ensure that criminals cannot hide behind nominees, shell corporations and other legal structures to frustrate law enforcement," with the goal of reducing the United States' vulnerability to criminals seeking access to its financial system, facilitating law enforcement investigations and bringing the United States into compliance with international AML and CFT standards. In November testimony before the Senate Banking Committee, both FinCEN Director Blanco and the FBI's D'Antuono expressed support for legislation to require the collection of beneficial ownership information at the time of any entity's formation.
- **Liability for SAR filing**: In November testimony before the Senate Banking Committee, the OCC's Gardineer suggested that Congress consider a technical correction to clarify that the BSA's safe harbor provides protection from civil liability for SARs made to appropriate authorities, and that an institution does not face the risk of civil litigation for complying with federal law under a "good faith" test imposed by a court.[140]
- **Regular review of BSA/AML regulations**: In November testimony before the Senate Banking Committee, the OCC's Gardineer suggested legislation to require regular review of BSA/AML regulations, similar to the process under the Economic Growth and Regulatory Paperwork Reduction Act (EGRPRA), which does not apply to all BSA/AML regulations.[141] FinCEN Director Blanco suggested that such an approach might be ill advised, as it would create an additional layer of bureaucracy.

Although the 115th Congress did not pass meaningful BSA/AML or sanctions legislation, proposals of the outgoing Congress are expected to serve as the starting point for legislative proposals in the 116th Congress. The following table provides an overview of certain notable proposals introduced by the outgoing Congress.

Legislation	Status	Key Provisions
Corporate Transparency Act of 2017 (H.R. 3089; companion bill S. 1717)	Introduced in House on June 28, 2017	Requires an entity that forms a corporation or limited liability company to disclose information about its beneficial owners. If the state of formation does not require the disclosure of beneficial ownership information, then the entity must file beneficial ownership information with FinCEN. Directs Treasury to require persons engaged in the business of forming corporations or limited liability companies to establish AML programs Imposes a civil penalty and authorizes criminal penalties for providing false or fraudulent beneficial ownership information or for willfully failing to provide complete or updated beneficial ownership information
AML and CTF Modernization Act (H.R. 4373)	Introduced in House on November 13, 2017	Increases dollar thresholds for SAR, CTR, CMIR and Form 8300 filing requirements Authorizes SAR sharing with foreign branches and affiliates that are in FATF countries and that maintain adequate policies Permits Section 314(b) sharing in connection with any specified unlawful activity Requires FinCEN to establish a procedure to issue written administrative rulings in response to inquiries concerning the conformance of specific BSA-related conduct
Enhancing Suspicious Activity Reporting Initiative Act (H.R. 5094)	Introduced in House on February 26, 2018 Passed by House on June 25, 2018	Directs the Department of Homeland Security to: (1) develop a strategy to improve its operations and activities related to training, outreach and information sharing for suspicious activity reporting to prevent acts of terrorism; (2) establish a working group to advise it on suspicious activity reporting; and (3) provide a briefing to the congressional homeland security committees on its operations and activities related to suspicious activity reporting
Cooperate with Law Enforcement Agencies and Watch Act of 2018 (H.R. 5783; companion bill S. 3045)	Introduced in House on May 11, 2018 Passed by House on June 25, 2018	Limits a financial institution's liability for maintaining a customer account in compliance with a written request by a federal, state, tribal or local law enforcement agency
Counter Terrorism and Illicit Finance Act (H.R. 6068) (H.R. 6858, H.R. 6861 and H.R. 6865 include similar provisions but are less comprehensive)	Introduced in House on June 12, 2018	Increases filing requirement dollar thresholds for SARs and CTRs Requires Treasury Secretary to review SAR and CTR requirements and propose changes to reduce burdens Requires Treasury Secretary to issue rules permitting SAR sharing with foreign branches and affiliates Creates FinCEN no-action letter procedure Permits Section 314(b) sharing in connection with any specified unlawful activity Expands Treasury role in coordinating BSA/AML policy and examinations 18-month safe harbor for liability of violation of CDD Rule
FinCEN Improvement Act of 2018 (H.R. 6411)	Introduced in House on July 17, 2018 Passed by House on September 12, 2018	FinCEN must work with tribal law enforcement agencies, protect against terrorism regardless of origin and coordinate internationally on matters involving emerging technology and virtual currency
Nicaragua Human Rights and Anticorruption Act of 2018 (S. 3233)	Introduced in Senate on July 18, 2018 Reported to the full Senate by the Senate Committee on Foreign Relations on October 3, 2018	Imposes sanctions on the Government of Nicaragua or any person acting on its behalf

AMERICAS

New York

Ian Cuillerier
Partner, New York
T +1 212 819 8713
E icuillerier@whitecase.com

Glen Cuccinello
Counsel, New York
T +1 212 819 8239
E glen.cuccinello@whitecase.com

Virginia Romano
Partner, New York
T +1 212 819 8601
E virginia.romano@whitecase.com

Paul Saltzman
Partner, New York
T +1 212 819 8258
E paul.saltzman@whitecase.com

Edward So
Partner, New York
T +1 212 819 7006
E edward.so@whitecase.com

Duane Wall
Partner of Counsel, New York
T +1 202 626 3599
E duane.wall@whitecase.com

Francis Zou
Partner, New York
T +1 212 819 8733
E francis.zou@whitecase.com

Washington, DC

Steve Chabinsky
Partner, Washington, DC
T +1 202 626 3587
E steven.chabinsky@whitecase.com

Nicole Erb
Partner, Washington, DC
T +1 202 626 3694
E nicole.erb@whitecase.com

Shamita Etienne-Cummings
Partner, Washington, DC
T +1 202 626 3695
E shamita.etienne@whitecase.com

Will Giles
Counsel, Washington, DC
T +1 202 637 6281
E will.giles@whitecase.com

Jeremy Kuester
Counsel, Washington, DC
T +1 202 637 6284
E jeremy.kuester@whitecase.com

Helen Lee
Counsel, Washington, DC
T +202 626 6531
E helen.lee@whitecase.com

Kevin Petrasic
Partner, Washington, DC
T +1 202 626 3671
E kevin.petrasic@whitecase.com

Benjamin Saul
Partner, Washington, DC
T +1 202 626 3665
E benjamin.saul@whitecase.com

Pratin Vallabhaneni
Partner, Washington, DC
T +1 202 626 3596
E prat.vallabhaneni@whitecase.com

EMEA

Berlin

Dr. Henning Berger
Partner, Berlin
T +49 30 880911 540
E henning.berger@whitecase.com

Frankfurt

Dr. Dennis Heuer
Partner, Frankfurt
T +49 69 29994 1576
E dennis.heuer@whitecase.com

Matthias Kasch
Partner, Frankfurt
T +49 69 29994 1219
E matthias.kasch@whitecase.com

Hamburg

Dr. Carsten Loesing
Partner, Hamburg
T +49 40 35005 265
E carsten.loesing@whitecase.com

Helsinki

Tanja Törnkvist
Partner, Helsinki
T +358 9 228 64 351
E tanja.tornkvist@whitecase.com

Istanbul

Asli Basgoz
Partner, Istanbul
T +90 212 354 2013
E asli.basgoz@whitecase.com

London

Laura Durrant
Partner, London
T +44 20 7532 2225
E laura.durrant@whitecase.com

Patrick Sarch
Partner, London
T +44 20 7532 2286
E patrick.sarch@whitecase.com

Julia Smithers Excell
Partner, London
T +44 20 7532 2229
E julia.smithers.excell@whitecase.com

Gavin Weir
Partner, London
T +44 20 7532 2113
E gavin.weir@whitecase.com

Stuart Willey
Partner, London
T +44 20 7532 1508
E stuart.willey@whitecase.com

Ingrid York
Partner, London
T +44 20 7532 1441
E iyork@whitecase.com

Madrid

Yoko Takagi
Partner, Madrid
T +34 91 7876 320
E yoko.takagi@whitecase.com

Milan

Iacopo Canino
Partner, Milan
T +39 0200688 340
E iacopo.canino@whitecase.com

Paris

Grégoire Karila
Partner, Paris
T +33 1 55 04 58 40
E gregoire.karila@whitecase.com

Thomas Le Vert
Partner, Paris
T +33 1 55 04 15 67
E thomas.levert@whitecase.com

Jean-Pierre Picca
Partner, Paris
T +33 1 55 04 58 30
E jeanpierre.picca@whitecase.com

Stockholm

Carl Hugo Parment
Partner, Stockholm
T +46 8 506 32 341
E carlhugo.parment@whitecase.com

Warsaw

Tomasz Ostrowski
Partner, Warsaw
T +48 22 50 50 123
E tostrowski@whitecase.com

Marcin Studniarek
Partner, Warsaw
T +48 22 50 50 132
E marcin.studniarek@whitecase.com

1 Deputy Attorney General Rod Rosenstein, remarks as prepared for delivery to the New York City Bar White Collar Crime Institute (May 9, 2018), *available* here.

2 Remarks of FinCEN Director Kenneth A. Blanco as prepared for delivery at the 2018 Chicago-Kent Block (Legal) Tech Conference (Aug. 9, 2018), *available* here; remarks of US Department of the Treasury Under Secretary Sigal Mandelker Speech before the Securities Industry and Financial Markets Association Anti-Money Laundering & Financial Crimes Conference (Feb. 13, 2018), *available* here; Federal Reserve Governor Lael Brainard, remarks as prepared for delivery at the Decoding Digital Currency Conference, San Francisco, CA (May 15, 2018), *available* here; Testimony of SEC Chairman Jay Clayton before the Senate Banking Committee (Feb. 6, 2018), *available* here; remarks of US Department of the Treasury Under Secretary Sigal Mandelker before the ABA/ABA Financial Crimes Enforcement Conference (Dec. 3, 2018), *available* here.

3 Treasury, Press Release, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses (Nov. 28, 2018), *available* here.

4 Treasury, National Strategy for Combating Terrorist and Other Illicit Financing (2018), *available* here.

5 Treasury, National Money Laundering Risk Assessment (2018), *available* here; National Terrorist Financing Risk Assessment (2018), *available* here; National Proliferation Financing Risk Assessment (2018), *available* here.

6 US sanctions often prohibit transactions by non-US persons involving sanctioned countries or blocked parties if the transactions have a direct or indirect connection to the United States or a US person. For example, a non-US person can be deemed to have violated US sanctions even by engaging in a transaction outside the United States that involves only non-US persons if the transaction is denominated in US dollars or even if there is a remote US nexus like involvement in a US bankruptcy proceeding where property involved in a sanctioned transaction is under the jurisdiction of the US bankruptcy court.

7 White House, Presidential Memoranda, Ceasing US Participation in the JCPOA and Taking Additional Action to Counter Iran's Malign Influence and Deny Iran All Paths to a Nuclear Weapon (May 8, 2018), *available* here; Treasury, Press Release, US Government Fully Re-Imposes Sanctions on the Iranian Regime As Part of Unprecedented US Economic Pressure Campaign (Nov. 5, 2018), *available* here.

8 OFAC, Frequently Asked Questions Related to the "Snap-back" of Iranian sanctions in November 2018 (Nov. 5, 2018), *available* here.

9 OFAC, Publication of Updates to OFAC's Specially Designated Nationals and Blocked Persons List and 13599 List Removals (Nov. 5, 2018), *available* here.

10 OFAC, Final Rule, Iranian Transactions and Sanctions Regulations (Nov. 5, 2018), *available* here.

11 OFAC, Frequently Asked Questions, Frequently Asked Questions Regarding Executive Order of August 6, 2018, "Reimposing Certain Sanctions With Respect to Iran," *available* here.

12 OFAC, Press Release, Treasury Designates Russian Oligarchs, Officials, and Entities in Response to Worldwide Malign Activity (Apr. 6, 2018), *available* here.

13 OFAC, Press Release, Treasury Releases CAATSA Reports, Including Senior Foreign Political Figures and Oligarchs in the Russian Federation (Jan. 29, 2018), *available* here.

14 OFAC, Ukraine Related Sanctions Regulations General License 12, Authorizing Certain Activities Necessary to Maintenance or Wind Down of Operations or Existing Contracts (Apr. 6, 2018), *available* here; OFAC, Ukraine Related Sanctions Regulations General License 13, Authorizing Certain Transactions Necessary to Divest or Transfer Debt, Equity, or Other Holdings in Certain Blocked Persons (Apr. 6, 2018), *available* here.

15 For the most recent extension, *see* OFAC, Press Release, OFAC Extends Expiration Date of General Licenses Related to EN+, RUSAL, and GAZ (Dec. 7, 2018), *available* here.

16 Executive Order 13849, Authorizing the Implementation of Certain Sanctions Set Forth in the Countering America's Adversaries Through Sanctions Act (Sept. 20, 2018), *available* here.

17 OFAC, Specially Designated Nationals List Update, CAATSA – Russia-related Designations (Sept. 20, 2018), *available* here.

18 State Department, Press Release, CAATSA Section 231: "Addition of 33 Entities and Individuals to the List of Specified Persons and Imposition of Sanctions on the Equipment Development Department" (Sept. 20, 2018), *available* here.

19 OFAC, Press Release, OFAC Notifies Congress of Intent to Delist En+, Rusal, and EuroSibEnergo (Dec. 19, 2018), *available* here.

20 S.J.Res.2, Joint Resolution Disapproving the President's proposal to take an action relating to the application of certain sanctions with respect to the Russian Federation (Jan. 4, 2019), *available* here.

21 OFAC, Press Release, Treasury Targets Russian Operatives over Election Interference, World Anti-Doping Agency Hacking, and Other Malign Activities (Dec. 19, 2018), *available* here.

[22] Executive Order 13827, Taking Additional Steps to Address the Situation in Venezuela (Mar. 19, 2018), *available* here.

[23] Executive Order 13835, Prohibiting Certain Additional Transactions with Respect to Venezuela (May 21, 2018), *available* here.

[24] Executive Order 13850, Blocking Property of Additional Persons Contributing to the Situation in Venezuela (Nov. 1, 2018), *available* here.

[25] OFAC, Venezuela Sanctions, *available* here.

[26] Executive Order 13827, Taking Additional Steps to Address the Situation in Venezuela (Mar. 19, 2018), *available* here.

[27] OFAC, Frequently Asked Questions, Executive Order 13827 "Taking Additional Steps to Deal with the Situation in Venezuela," (Mar. 19, 2018) *available* here.

[28] OFAC, Press Release, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses (Nov. 28, 2018), *available* here.

[29] OFAC, Questions on Virtual Currency (Nov. 28, 2018), *available* here.

[30] Executive Order 13851, Blocking Property of Certain Persons Contributing to the Situation in Nicaragua (Nov. 27, 2018), *available* here.

[31] OFAC, Department of State, US Coast Guard, North Korea Sanctions Advisory, Sanctions Risks Related to North Korea's Shipping Practices (Feb. 23, 2018), *available* here.

[32] Treasury, US Department of State, and US Department of Homeland Security, North Korea Sanctions & Enforcement Actions Advisory, Risks for Businesses with Supply Chain Links to North Korea (July 23, 2018), *available* here.

[33] OFAC, Reissuance of North Korea Sanctions Regulations (Mar. 1, 2018), *available* here; OFAC, Final Rule, North Korea Sanctions Regulations (Mar. 5, 2018), *available* here.

[34] OFAC, North Korea Sanctions, *available* here.

[35] OFAC, Advisory to the Maritime Petroleum Shipping Community, Sanctions Risks Related to Shipping Petroleum to Syria (Nov. 20, 2018), *available* here.

[36] Executive Order 13848, Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election (Sept. 12, 2018), *available* here.

[37] State Department, Press Release, State Department Updates the Cuba Restricted List (Nov. 14, 2018), *available* here.

[38] OFAC, Removal of the Sudanese Sanctions Regulations and the Amendment of the Terrorism List Government Sanctions Regulations (June 29, 2018), *available* here.

[39] Remarks of US Department of the Treasury Under Secretary Sigal Mandelker before the ABA/ABA Financial Crimes Enforcement Conference (Dec. 3, 2018), *available* here.

[40] OFAC, Enforcement Information for December 20, 2018 (Dec. 20, 2018), *available* here.

[41] OFAC, Enforcement Information for December 12, 2018 (Dec. 12, 2018), *available* here; OFAC, Settlement Agreement (Dec. 12, 2018), *available* here.

[42] OFAC, Enforcement Information for November 27, 2018 (Nov. 27, 2018), *available* here.

[43] OFAC, Settlement Agreement (Nov. 19, 2018), *available* here.

[44] OFAC, Settlement Agreement (Oct. 5, 2018), *available* here; OFAC, Enforcement Information for October 5, 2018 (Oct. 5, 2018), *available* here.

[45] OFAC, Enforcement Information for September 13, 2018 (Sept. 13, 2018), *available* here.

[46] OFAC, Enforcement Information for June 6, 2018 (June 6, 2018), *available* here.

[47] FinCEN, Final Rule, Customer Due Diligence Requirements for Financial Institutions (May 11, 2016), *available* here.

[48] FinCEN, Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions, FIN-2018-G001 (Apr. 3, 2018), *available* here.

[49] FinCEN, Ruling: Premium Finance Cash Refunds and Beneficial Ownership Requirements for Legal Entity Customers, FIN-2018-R001 (May 11, 2018), *available* here.

[50] FinCEN, Ruling: Exceptive Relief from Beneficial Ownership Requirements for Legal Entity Customers of Rollovers, Renewals, Modifications, and Extensions of Certain Accounts, FIN-2018-R004 (Sept. 7, 2018), *available* here.

[51] Federal Reserve, FDIC, NCUA, OCC, FinCEN, Order granting an exemption from customer identification program requirements implementing section 326 of the USA PATRIOT Act, 31 USC § 5318(l), for loans extended by banks (and their subsidiaries) subject to the jurisdiction of the Federal Banking Agencies to commercial customers to facilitate purchases of property and casualty insurance policies (Sept. 28, 2018), *available* here.

[52] Federal Reserve, FDIC, FinCEN, NCUA and OCC, Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing (Dec. 3, 2018), *available* here.

[53] Federal Reserve, FDIC, FinCEN, NCUA and OCC, Interagency Statement on Sharing Bank Secrecy Act Resources (Oct. 3, 2018), *available* here.

[54] FinCEN, Advisory on Human Rights Abuses Enabled by Corrupt Senior Foreign Political Figures and their Financial Facilitators, FIN-2018-A003 (June 12, 2018), *available* here.

[55] FinCEN, Advisory to Financial Institutions on the Risk of Proceeds of Corruption from Nicaragua, FIN-2018-A005 (Oct. 4, 2018), *available* here.

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

[57] Remarks of FinCEN Director Kenneth A. Blanco at the 2018 Chicago-Kent Block (Legal) Tech Conference.

[58] Remarks of FinCEN Director Kenneth A. Blanco, remarks as prepared for delivery at the 11th Annual Las Vegas Anti-Money Laundering Conference and Expo (Aug. 14, 2018), *available* here.

[59] Remarks of US Department of the Treasury Under Secretary Sigal Mandelker before the Securities Industry and Financial Markets Association Anti-Money Laundering & Financial Crimes Conference.

[60] Remarks of US Department of the Treasury Under Secretary Sigal Mandelker before the ABA/ABA Financial Crimes Enforcement Conference.

[61] FinCEN, Geographic Targeting Order (Nov. 15, 2018), *available* here.

[62] FinCEN, Press Release (Dec. 17, 2018), *available* here; FinCEN, Assessment of Civil Money Penalty, Number 2018-03 (Dec. 11, 2018), *available* here.

[63] FinCEN, Assessment of Civil Money Penalty, Number 2018-02 (May 3, 2018), *available* here.

[64] Press Release, FinCEN (Feb. 15, 2018), *available* here; Press Release, DOJ (Feb. 15, 2018), *available* here; Press Release (Feb. 15, 2018), *available* here; Press Release, Federal Reserve (Feb. 15, 2018), *available* here.

[65] DOJ, Deferred Prosecution Agreement (Feb. 12, 2018), *available* here.

[66] OCC Consent Order for a Civil Money Penalty (Feb. 13, 2018), *available* here.

[67] Federal Reserve, Order to Cease and Desist and Order of Assessment of a Civil Money Penalty Issued Upon Consent (Feb. 14, 2018), *available* here.

[68] FinCEN, Assessment of Civil Money Penalty (Feb. 15, 2018), *available* here.

[69] The FinCEN penalty was a total of US$185 million, with US$115 million satisfied by the DOJ forfeiture.

[70] FinCEN, Press Release (Feb. 13, 2018), *available* here; FinCEN, Notice of Proposed Rulemaking (Feb. 13, 2018), *available* here.

[71] ECB, Press Release (Feb. 24, 2018), *available* here.

[72] Deputy Attorney General Rod Rosenstein, remarks as prepared for delivery to the New York City Bar White Collar Crime Institute.

[73] Federal Reserve, FDIC and OCC, Policy Statement on Interagency Notification of Formal Enforcement Actions (June 12, 2018), *available* here.

[74] Press Release, DOJ (Nov. 19, 2018), *available* here.

[75] DOJ, Press Release (Feb. 7, 2018), *available* here; Plea Agreement (S.D. Cal. Feb. 5, 2018), *available* here.

[76] OCC, Consent Order for a Civil Money Penalty (Feb. 6, 2018), *available* here.

[77] OCC, Notice of Charges for Order of Prohibition and Notice of Assessment of a Civil Monetary Penalty (Apr. 16, 2018), *available* here.

[78] OCC, Semiannual Risk Perspective (Fall 2018), *available* here.

[79] OCC, Fiscal Year 2019 Bank Supervision Operating Plan, OCC Committee on Bank Supervision, *available* here.

[80] Testimony of Joseph M. Otting, Comptroller of the Currency, before the House Financial Services Committee (June 13, 2018), *available* here; Testimony of Joseph M. Otting before the Senate Banking Committee (June 14, 2018), *available* here.

[81] OCC, Press Release (Oct. 23, 2018), *available* here.

[82] OCC, Consent Order, (July 10, 2015), *available* here.

[83] OCC, Consent Order (Oct. 23, 2018), *available* here.

[84] OCC, Consent Order (Sept. 12, 2018), *available* here.

[85] OCC, Consent Orders (June 21, 2018), *available* here and here.

[86] OCC, Press Release (Feb. 27, 2017), *available* here; OCC, Consent Order for a Civil Money Penalty (Feb. 14, 2017), *available* here.

[87] OCC, Consent Order (Apr. 10, 2018), *available* here.

[88] OCC, Consent Order (Apr. 16, 2018), *available* here.

[89] OCC, Consent Order (Mar. 5, 2018), *available* here.

[90] OCC, Consent Order (Feb. 5, 2018), *available* here.

[91] OCC, Consent Order (Mar. 7, 2018), *available* here.

[92] OCC, Consent Order (Apr. 26, 2018), *available* here; OCC, Consent Order (Feb. 6, 2018), *available* here.

[93] OCC, Consent Order for a Civil Money Penalty (Apr. 24, 2018), *available* here.

[94] OCC, Consent Order (Feb. 28, 2018), *available* here; OCC, Consent Order (Feb. 12, 2018), *available* here.

[95] Remarks of Federal Reserve Governor Lael Brainard.

[96] Federal Reserve, Press Release (Nov. 19, 2018), *available* here.

[97] Federal Reserve, Press Release (Jan. 17, 2018), *available* here.

[98] Federal Reserve and Illinois Department of Financial and Professional Regulation, Order to Cease and Desist and Order of Assessment of a Civil Money Penalty Issued Upon Consent (Jan. 17, 2018), *available* here.

[99] Federal Reserve Bank of Kansas City and Oklahoma State Banking Department, Written Agreement (Oct. 22, 2018), *available* here.

[100] Federal Reserve Bank of New York, Written Agreement (July 2, 2018), *available* here.

[101] Federal Reserve, Cease and Desist Order Issued Upon Consent (Mar. 12, 2018), *available* here.

[102] Remarks by Jelena McWilliams, Chairman, FDIC, at the Federal Reserve Bank of Philadelphia Fintech and the New Financial Landscape Conference in Philadelphia, Pennsylvania (Nov. 13, 2018), *available* here.

[103] *Cal. Pac. Bank v. FDIC*, 885 F.3d 560 (9th Cir. 2018).

[104] *Id.* at 571.

[105] Federal Reserve, FDIC, NCUA, OCC, Interagency Statement Clarifying the Role of Supervisory Guidance (Sept. 11, 2018), *available* here.

[106] FDIC, Consent Order, FDIC-18-0128b (Sept. 24, 2018), *available* here.

[107] FDIC, Consent Order, FDIC-18-0061b (Apr. 26, 2018), *available* here.

[108] Testimony of SEC Chairman Jay Clayton before the Senate Banking Committee.

[109] SEC, Press Release (Dec. 17, 2018), *available* here; SEC Order, File No. 3-18931 (Dec. 17, 2018), *available* here.

[110] SEC, Litigation Release No. 24189 (July 9, 2018), *available* here; SEC Complaint, No. 18-cv-3942 (N.D. Cal. July 9, 2018), *available* here.

[111] *United States SEC v. Alpine Secs. Corp.*, 308 F. Supp. 3d 775 (S.D.N.Y. Mar. 30, 2018); SEC, Litigation Release No. 23853, SEC Charges Brokerage Firm with Failing to Comply with Anti-Money Laundering Laws (June 5, 2017), *available* here.

[112] FinCEN, The SAR Activity Review: Trends, Tips & Issues, Issue 10 (May 2006), *available* here.

[113] SEC, Press Release, SEC Charges Brokerage Firms and AML Officer With Anti-Money Laundering Violations (May 16, 2018), *available* here.

[114] SEC, Administrative Proceeding File No. 3-18486 (May 16, 2018), *available* here.

[115] SEC, Administrative Proceeding File No. 3-18488 (May 16, 2018), *available* here.

[116] SEC, Administrative Proceeding File No. 3-18487 (May 16, 2018), *available* here.

[117] Financial Industry Regulation Authority Letter of Acceptance, Waiver and Consent No. 2015045550801 (May 16, 2018), *available* here.

[118] SEC, Press Release, Broker-Dealer Admits It Failed to File SARs (Mar. 28, 2018), *available* here.

[119] SEC, Administrative Proceeding File No. 3-18412 (Mar. 28, 2018), *available* here.

[120] Financial Industry Regulation Authority Letter of Acceptance, Waiver and Consent No. 20130387509 (Mar. 28, 2018), *available* here.

[121] SEC, Administrative Proceeding File No. 3-18413 (Mar. 28, 2018), *available* here; SEC, Administrative Proceeding File No. 3-18414 (July 6, 2018), *available* here.

[122] FINRA, Press Release (Dec. 26, 2018) *available* here.

[123] FINRA, Press Release (Dec. 17, 2018), *available* here.

[124] Financial Industry Regulation Authority Letter of Acceptance, Waiver and Consent No. 2014039400901 (Aug. 3, 2018), *available* here.

[125] Financial Industry Regulation Authority Letter of Acceptance, Waiver and Consent No. 2015046020002 (May 22, 2018), *available* here.

[126] Financial Industry Regulation Authority Letter of Acceptance, Waiver and Consent No. 2016052628901 (Apr. 10, 2018), *available* here.

[127] Financial Industry Regulation Authority Letter of Acceptance, Waiver and Consent No. 2017052146901 (Mar. 28, 2018), *available* here.

[128] Financial Industry Regulation Authority Letter of Acceptance, Waiver and Consent No. 20160476768-01 (Jan. 2, 2018), *available* here.

[129] CFTC, Press Release, CFTC Charges Trading Platform with Illegal Transactions Margined in Bitcoin, Failing to Implement Procedures to Prevent Money-Laundering, and Failing to Register with the CFTC (Sept. 27, 2018), *available* here.

[130] CFTC Complaint (D.D.C. Sept. 27, 2018), *available* here.

[131] DFS, Press Release (Oct. 10, 2018), *available* here.

[132] DFS, Consent Order (Oct. 10, 2018), *available* here.

[133] DFS, Press Release (Jan. 4, 2018), *available* here.

[134] DOJ, Deferred Prosecution Agreement, 1:17-cr-00011-CCC (M.D. Pa., Jan. 19, 2017), *available* here; Federal Trade Commission, Press Release (Jan. 19, 2017), *available* here; FinCEN, Press Release (Jan. 19, 2017), *available* here.

[135] Hearing information available here and here.

[136] Testimony of Grovetta N. Gardineer, Senior Deputy Comptroller for Compliance and Community Affairs, OCC, before the Senate Banking Committee (Nov. 29, 2018), *available* here.

[137] Testimony of Joseph M. Otting.

[138] Testimony of Kenneth A. Blanco, Director, FinCEN, before the Senate Banking Committee (Nov. 29, 2018), *available* here; testimony of Steven M. D'Antuono, Section Chief, Criminal Investigation Division, Federal Bureau of Investigation, DOJ (Nov. 29, 2018), *available* here.

[139] Testimony of Acting Deputy Assistant Attorney General, Criminal Division, M. Kendall before the Senate Judiciary Committee (Feb. 6, 2018), *available* here.

[140] Testimony of Grovetta Gardineer.

[141] Testimony of Grovetta Gardineer.