WILMERHALE

JULY 25, 2019

Anti-Money Laundering and Sanctions:

Trends and Developments Emerging Under the Trump Administration

By David S. Cohen, Franca Harris Gutierrez, Sharon Cohen Levin, Ronald I. Meltzer, Jeremy Dresner, David M. Horn, Zachary Goldman, Michael Romais and Semira Nikou

TABLE OF CONTENTS

I. Executive Summary

Bank Secrecy Act/anti-money laundering (BSA/AML) and sanctions matters continue to be a core focus of regulators, law enforcement agencies, policymakers and Congress, and the story of the Obama and Trump Administrations on AML and sanctions is one of general continuity. Policymakers are turning to sanctions with increasing frequency and launching programs that are increasingly complex, and regulatory and enforcement agencies are devoting significant resources and attention to AML. Congress continues to debate BSA reform, while the Treasury Department and federal banking regulators have encouraged financial institutions to use technology to support BSA compliance, in the hope of making the process more effective and efficient.

As Congress, the executive branch and regulators all continue to focus a great deal of attention on AML and sanctions issues, the expectations of financial institutions to prevent financial crime are growing. Sanctions regulations are becoming more numerous, are reaching more deeply into securities markets and are branching into new areas of technology—such as cryptocurrency. Simultaneously, the AML regime's push toward greater transparency in a number of contexts, from virtual currency regulation to beneficial ownership reform, means that financial institutions will shoulder greater responsibility for knowing their customers and their customers' activities. Strict distinctions among different categories of financial crime are starting to collapse, as an increasing number of sanctions programs and FinCEN advisories focus on issues such as corruption and misappropriation of assets by politically exposed persons (PEPs).

From the perspective of financial institutions, the need to take an increasingly integrated and coherent approach within individual institutions and the need to consider risk in a global context are paramount.[1] The fact that sanctions programs are increasingly focused on corruption means that financial institutions will need to understand their exposure to PEP clients, particularly in areas characterized by high geopolitical risk, as these individuals are more likely to be exposed to financial sanctions. Financial institutions must keep a close eye on the changing geopolitical landscape and map crisis areas to their client base to ensure their risk management program remains aligned with their risk appetite. All this means that the components of a financial institution's AML, sanctions, and anti-bribery and corruption compliance efforts must collaborate closely to proactively identify and mitigate risk. It also means that institutions must take a global view, understanding how different components of their organizations interact with each other, where the seams in their controls may be, and where conflicting legal regimes (whether involving a blocking statute, data privacy law or other legal measures) hinder the institution from taking an enterprise-wide approach to managing financial crimes compliance risk.

This report reviews recent trends and developments in the BSA/AML and sanctions regulatory landscape from 2017 to the first half of 2019. It will first describe recent developments in AML and sanctions law and policy, and then will describe recent enforcement actions that shape companies' obligations with respect to AML and sanctions. We hope it is useful in developing a richer understanding of the current financial crime risk management landscape.

II. BSA/AML Regulatory Trends and Developments

Throughout 2017 and 2018 and into 2019, the US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and other federal and state regulators have been active with respect to AML and BSA regulation and enforcement. FinCEN Director Ken Blanco and Under Secretary of the Treasury for Terrorism and Financial Intelligence Sigal Mandelker have generally adopted an approach consistent with that of their predecessors. Broadly,

FinCEN and other regulators continue to focus on issues where lack of transparency and intermediation, especially in the correspondent banking context, pose risks to the integrity of the financial system.

Beneficial ownership continues to be a focus of both regulators and Congress, and the entry into force of the new Customer Due Diligence (CDD) Rule[2] in May 2018 was the most significant recent development. FinCEN's broadening of Geographic Targeting Orders (GTOs) that require disclosure of beneficial ownership in certain situations[3] and its continued focus on beneficial ownership at the company formation stage[4] are key developments in recent years. These efforts complement those of the Financial Action Task Force (FATF) to call attention to the relationship between concealment of beneficial ownership and financial crime,[5] and the European Union's Fourth Anti-Money Laundering Directive, which mandates the creation of beneficial ownership registries.[6]

Transaction monitoring and suspicious activity reporting continued to be important areas of both regulatory action and enforcement. Initiatives such as the FinCEN Exchange, which was launched in December 2017 to enhance public/private collaboration to address financial crime, and interagency guidance FinCEN released with the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), the board of governors of the Federal Reserve, and the National Credit Union Administration (NCUA), which focused on the use of novel technologies to identify and report financial crime, illustrate FinCEN's focus on these issues. As will be seen below in the section describing recent enforcement actions, failures in transaction monitoring and suspicious activity reporting remain a priority focus for regulatory agencies.

Individual accountability at financial institutions for AML and sanctions compliance matters also remains an area of focus. Pursuant to the New York State Department of Financial Services (NYDFS)'s new "Part 504" rule, bank officials must certify that the institution they lead complies with the requirements of the rule, and regulators have started to pursue enforcement actions against individual executives in instances of systemic AML/sanctions compliance failures.

A. Changes in the Risk Environment

1. Cryptocurrencies

In 2018 and 2019, FinCEN and the Department of the Treasury's Office of Foreign Assets Control (OFAC) made several announcements clarifying how existing financial crimes regulations extend to different components of the virtual currency ecosystem. OFAC's guidance focused on the application of its general sanctions compliance obligations to virtual currency (and at the same time imposed sanctions on Venezuela's national cryptocurrency, the Petro), and on ways to implement obligations to block virtual currency owned by persons subject to sanctions. FinCEN's 2018 guidance, embodied in a letter to Senator Ron Wyden (D-OR), focused on the regulatory status of initial coin offerings (ICOs). ICOs are a way for businesses to raise money, without selling equity or raising debt, by issuing tokens that can later be used or resold. The money raised through the ICO is often used to develop the product or service that the startup plans to offer.

On March 6, 2018, FinCEN released a letter that it had sent to Senator Wyden on February 13, 2018, articulating its view of how the BSA and associated regulations apply to ICOs, building on cryptocurrency guidance the agency has issued in a variety of mechanisms since 2013.[7] According to FinCEN, businesses issuing an ICO may be money transmitters subject to the BSA, depending on the facts and circumstances and whether the business is already BSA-regulated (some companies issuing tokens are classified as broker-dealers under the SEC's regulations, in which

case the BSA obligations applicable to broker-dealers would apply). The FinCEN letter has broad implications for any company that has issued an ICO, is considering doing so, or plans to invest in a company that may issue an ICO, requiring them to adopt AML programs, register with FinCEN as a money services business (MSB), file Suspicious Activity Reports (SARs) when appropriate, and potentially also obtain state-issued money transmitter licenses.

In May 2019, FinCEN released comprehensive guidance on convertible virtual currencies (CVCs). The guidance did not itself establish any new regulatory expectations or requirements. It did, however, consolidate and explain FinCEN's previous rules, interpretations, and guidance in a single document and apply them to a range of common cryptocurrency business models. The guidance is detailed and nuanced, and will substantially assist the cryptocurrency community in meeting its AML program obligations. It is also broadly consistent with guidance the Financial Action Task Force released in June 2019 that explicated how its traditional recommendations apply to the cryptocurrency context. The FATF clearly articulated its view that Virtual Asset Service Providers (VASPs) must be subject to regulation and that the preventive measures and other recommendations that apply to regulated financial institutions (including the funds travel rule) should apply to VASPs as well.

Other regulatory agencies, including the SEC and the Commodity Futures Trading Commission (CFTC), have also been active recently in virtual currency regulation and enforcement in matters subject to their jurisdiction. AML and economic sanctions laws effectuate national security goals and impose compliance requirements for individuals and businesses. Taken together, FinCEN's and OFAC's pronouncements represent increased oversight of virtual currency in the financial crimes space while clarifying how businesses may meet their compliance obligations.

2. Marijuana

The myriad—and conflicting—state, federal and international laws governing the burgeoning marijuana industry have created a complicated legal landscape for financial institutions. In the United States, most states have legalized some form of marijuana use, but the manufacture, sale and distribution of marijuana nevertheless remain illegal under federal law. As a result, in providing financial products and services to US marijuana-related businesses (MRBs), a financial institution could risk violating the Controlled Substances Act (CSA), 21 U.S.C. § 841. Moreover, engaging in or facilitating transactions that contain proceeds from US marijuana sales could create liability under the money laundering laws.

Further complicating matters, in October 2018 Canada became the first major economy to legalize recreational marijuana. Because US narcotics laws generally do not apply to activity that is legal abroad, providing financial products and services to Canadian MRBs would not violate the CSA or implicate US money laundering laws. However, that is not the case in many European countries. The European Union recently passed a law expanding the extraterritorial scope of member countries' money laundering laws with respect to certain narcotics-related offenses. These laws could now criminalize the transfer of funds from activity that is legal in the foreign country (e.g., marijuana sales in Canada) if that activity would be illegal in the home country.

Below we discuss the fragmented legal and regulatory landscape governing the marijuana industry as well as notable recent developments and their implications for global financial institutions.

US Narcotics Laws

In the United States, 46 states have legalized marijuana for medical and/or recreational use in some form. Medical marijuana is used to control seizures, ease glaucoma and combat the loss of appetite caused by chemotherapy,

among other purposes. Notwithstanding these developments, the manufacture, sale or distribution of marijuana for any purpose continues to be a violation of the CSA, even in states that have legalized its use at the state level. As a result, businesses that manufacture, sell or distribute marijuana in the United States are generally operating in violation of federal law.

The federal government, however, has issued directives that create uncertainty regarding the likelihood of marijuana-related prosecutions. Department of Justice (DOJ) officials in the Obama Administration issued several memoranda, known as the "Cole memoranda," deprioritizing federal criminal prosecutions involving state-regulated marijuana businesses based on a set of eight priority factors.[8] On January 4, 2018, former Attorney General Jefferson Sessions rescinded that guidance and instructed federal prosecutors to determine "which marijuana activities to prosecute" based on the "well-established principles that govern all federal prosecutions."[9] Practically, this means that federal marijuana enforcement priorities will be determined by individual US attorneys' offices. Although Attorney General Sessions' memorandum did not alter the status of marijuana under federal law—marijuana commerce remained illegal even after the Cole memoranda were issued—the rescission of the Cole memoranda increased the risk of prosecution for marijuana-related commerce. Attorney General William Barr has not yet decided whether to formally reinstate the Cole memoranda, but he has announced that he "do[es] not intend to go after parties who have complied with state law in reliance on the Cole memorandum."[10] The risk of prosecution with respect to medical marijuana is much lower because Congress has—through the Rohrabacher-Blumenauer Amendment—limited the DOJ's ability to use federal funds to enforce the CSA with respect to state-legalized medical marijuana businesses.[11]

The 2018 Farm Bill, Industrial Hemp and CBD

Industrial hemp and products derived from hemp, such as cannabidiol (CBD), create yet another source of uncertainty. In December, Congress passed and the President signed the long-awaited 2018 Farm Bill, which removes industrial hemp from the CSA's definition of marijuana and expands legal cultivation of industrial hemp.[12] CBD and other extracts derived from industrial hemp are no longer Schedule I drugs under the CSA.

The cultivation of industrial hemp and the manufacture and sale of CBD products are, however, still subject to state laws and regulations as well as Food and Drug Administration (FDA) regulation. Although some states had legalized hemp and CBD prior to the 2018 Farm Bill, industrial hemp and CBD products remain illegal (at least for now) at the state level in many states. Other states regulate CBD as a form of medical marijuana and allow its use by patients with prescriptions. And it remains to be seen how state regulation of industrial hemp and CBD may change in response to the 2018 Farm Bill.

Additionally, the FDA's approach to regulating CBD is not yet clear. The FDA has indicated that it may regulate CBD as a pharmaceutical drug (subject to the FDA drug-approval process) rather than as a dietary supplement.[13] And the FDA recently approved a childhood epilepsy drug, Epidiolex, whose active ingredient is CBD. The FDA has also issued warning letters addressed to CBD manufacturers and retailers that claim unproven health benefits from CBD, but it has not yet brought enforcement actions against CBD manufacturers.

US Money Laundering Laws

The risk of providing products or services to MRBs is not limited to narcotics laws. The US money laundering laws make it a crime to conduct a financial transaction with proceeds of "specified unlawful activity," provided that a defendant has the requisite knowledge and/or intent. See 18 U.S.C. §§ 1956, 1957. It is also a crime to transport,

transmit or transfer funds internationally for the purpose of promoting a specified unlawful activity, even if the funds are derived from a legitimate source. See 18 U.S.C. § 1956(a)(2).

In the context of marijuana commerce, federal, state and foreign narcotics offenses constitute specified unlawful activity. As a result, if an entity engages in a financial transaction knowing that the property involved represents the proceeds of some unlawful activity (e.g., US marijuana sales or foreign marijuana sales in other countries where marijuana remains illegal) and intends to promote the carrying on of unlawful activity, it may violate US money laundering laws. If a transaction exceeds $10,000, intent to promote the underlying activity is not required. See 18 U.S.C. § 1957. The government need only establish that the entity knowingly engaged in a monetary transaction in property derived from specified unlawful activity with a value greater than $10,000.

Implications for Financial Institutions in the United States

The complicated legal status of marijuana in the United States has potentially serious implications for financial institutions. A financial institution that provides products or services directly to a US MRB could be viewed as conspiring to violate or aiding and abetting a violation of the CSA because such services promote or facilitate the US MRB's business. The potential money laundering risk arises where the financial institution receives or transfers funds from a US MRB that it knows are derived from the sale of marijuana. The money laundering risk is greater for transactions that exceed $10,000 because specific intent to promote the underlying criminal activity is not required; the government need only prove that the transaction contained crime proceeds and that the financial institution had knowledge of or was willfully blind to that fact.

The money laundering risk is not limited to direct transactions with US MRBs. There may also be risk in providing products and/or services to businesses that support US MRBs, such as companies that manufacture fertilizer and packaging materials or even provide accounting or legal services. Businesses that support US MRBs may engage in transactions with funds that contain proceeds from US marijuana sales (i.e., crime proceeds), and the receipt or transfer of such funds by a financial institution could expose a financial institution to liability under US money laundering laws. The risk of providing products or services to such supporting businesses is lower than that of providing products and services directly to US MRBs, but financial institutions can further mitigate their risk by obtaining representations and warranties from supporting businesses to ensure that they are not transacting with crime proceeds.[14]

The risk also differs based on the products or services provided (e.g., consumer banking services, initial public offerings, secondary-market trading, and research and analysis). Products and services that are material (i.e., necessary) to a US MRB's business create a greater risk that a financial institution could be viewed as aiding and abetting or conspiring to violate the CSA or promoting illegal marijuana sales in violation of US AML laws. Activities that are further attenuated from the underlying marijuana sales—e.g., secondary-market trading of securities—make it less likely that a financial institution would have the requisite knowledge and/or intent to violate US narcotics or money laundering laws.

In fact, regulatory guidance suggests that financial institutions may provide certain banking services related to MRBs. In 2014, FinCEN issued guidance based on the Cole memoranda that was designed to help banks reconcile the tension between state and federal narcotics laws. The FinCEN guidance created a three-tiered SAR filing system for marijuana-related activity. Notably, the FinCEN guidance does not prohibit financial institutions from providing banking services to state-licensed MRBs. Rather, FinCEN issued the "guidance [to] clarif[y] how financial institutions

can provide services to marijuana-related businesses consistent with their BSA obligations."[15] FinCEN has not revised the guidance following the repeal of the Cole memoranda.

Moreover, some states have encouraged the financial services industry to provide banking services to state-authorized MRBs. For example, New York Governor Andrew Cuomo directed the NYDFS to encourage New York State-chartered banks and credit unions to provide banking services to New York's medical marijuana and hemp businesses.[16] Several members of Congress have introduced legislation to enable state-licensed US MRBs to engage in relationships with banks and other financial institutions,[17] and many have advocated for US MRBs to have access to the banking system.[18]

Canada Legalizes Recreational Marijuana

Canadian MRBs, however, do not pose these same risks under US law. Canada legalized recreational marijuana on October 17, 2018, becoming the world's largest marketplace for legal marijuana. Each of Canada's provinces and territories is responsible for establishing its own rules governing how marijuana may be sold and where it may be consumed, but as a general matter, individuals 18 years and older may now consume marijuana, possess up to 30 grams of marijuana in public, and grow up to four marijuana plants at home. Some provinces, such as British Columbia, have elected to operate government-run marijuana stores, while others have granted licenses to private distributors.

Because the manufacture, distribution and sale of marijuana in Canada are now legal, MRBs that operate exclusively in Canada with no nexus to the United States are no longer engaged in specified unlawful activity—a predicate offense—under US money laundering laws. Accordingly, providing the same products and services that could implicate US narcotics or money laundering laws if provided to a US MRB would not violate US law if provided to a Canadian MRB. That is not necessarily the case under European law.

European Countries Expand the Scope of Their Money Laundering Laws

On October 23, 2018, the European Parliament and the European Council signed the Directive on Countering Money Laundering by Criminal Law (the "Directive"),[19] which broadens the scope of extraterritorial activity that may serve as a predicate for a money laundering offense in EU member countries. Currently, the laws of some EU member countries, such as Germany, provide that extraterritorial activity is generally not a basis for a money laundering conviction unless the activity is illegal both in the country where the activity takes place and in the EU member country. These laws apply what is known as the "double criminality criterion," meaning that the activity has to be a crime in both relevant countries to constitute a predicate offense. The Directive prohibits EU member countries from applying the double criminality criterion in cases of illicit trafficking in narcotic drugs and psychotropic substances (including the cultivation of cannabis). The elimination of the double criminality criterion means that proceeds from legal marijuana sales in Canada, which would be illegal if they occurred in the EU member country, could provide the basis for a money laundering conviction in the EU. EU member countries will be required to implement the Directive by December 3, 2020.

The United Kingdom's money laundering law similarly provides that persons or institutions that receive payments derived from legal marijuana sales abroad commit a criminal offense, provided that they know or suspect the funds were derived from the sale of marijuana. In the United Kingdom, it is illegal to possess, grow or sell marijuana, and the Proceeds of Crime Act (POCA) defines "criminal property" by reference to whether the predicate activity is lawful

in the United Kingdom (not where the activity occurred).[20] Although there is a statutory exemption to POCA for certain predicate acts that are legal where they occurred, that exemption does not apply to marijuana possession, cultivation or sales, given the prison sentences permissible for such crimes.

As explained above, because the manufacture, distribution and sale of marijuana in Canada are now legal, MRBs that operate exclusively in Canada with no nexus to the United States are not acting in violation of US narcotics or money laundering laws. Providing products and services to Canadian MRBs could, however, provide the predicate for a money laundering violation in EU Member States.

Summary

In sum, the risk of violating US narcotics or money laundering laws by providing products or services to businesses involved in marijuana commerce depends on a number of factors, including (but not limited to)

- whether the business is engaged in the manufacture, sale or distribution of recreational or medical marijuana in the United States;
- whether a foreign business operates in or has a nexus to the United States or operates solely in a jurisdiction, such as Canada, where marijuana is legal; and
- whether the business provides products or services to MRBs and/or receives funds that may be derived from US marijuana sales.

Financial institutions should be aware of and develop policies and procedures to mitigate these risks. Because different jurisdictions take different approaches to criminalizing activities involving MRBs, financial institutions should centralize risk-management decision making around marijuana-related issues with a knowledgeable group of legal, compliance and risk management personnel.

3. Treasury Publishes National Illicit Finance Strategy and National Money Laundering Risk Assessment

On December 20, 2018, the US Department of the Treasury released the National Strategy for Combating Terrorist and Other Illicit Financing, pursuant to Sections 261 and 262 of the Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA).[21] In connection with this issuance, the Treasury also released the 2018 National Money Laundering Risk Assessment (NMLRA), along with corresponding risk assessments for terrorist financing and proliferation financing.[22] Although casinos and gambling were not discussed in detail, the NMLRA provides a window into Treasury's thinking about certain money laundering risks.

Treasury estimated that domestic financial crime (excluding tax evasion) generates approximately $300 billion of proceeds for potential laundering each year.[23] The most significant areas of vulnerability in money laundering activity in the United States include (1) misuse of cash, (2) complicit individuals and financial services employees, and (3) lax compliance at financial institutions.

Six principal threats were identified in the NMLRA related to money laundering to the United States:

- ***Fraud.*** The bulk of illicit proceeds are generated by fraud (predominantly bank fraud, consumer fraud, healthcare fraud, securities fraud and tax refund fraud), as well as by cyber-enabled crimes (credit card fraud, business email compromise, and consumer scams like romance and lottery schemes).

- *Drug Trafficking*. Mexico is the primary pathway for most illegal drugs entering the United States. Common typologies for the repatriation of cash generated from drug sales include (1) pooling proceeds into a single account whose funds are then wired outside the United States to Mexico; (2) bulk cash smuggling of proceeds back into Mexico; or (3) trade-based money laundering (TBML), both witting and unwitting. The rise of China as the most significant global supplier of fentanyl and other synthetic opiates has changed the nature of synthetic drug trafficking, as law enforcement has identified complex schemes using aliases, cryptocurrency, offshore accounts and encrypted communications to facilitate laundering of funds internationally through third parties. Drug trafficking in marijuana, cocaine, heroin and synthetic opioids, methamphetamine, and synthetic psychoactive drugs (including MDMA/ecstasy and synthetic cannabis) all pose significant risk of money laundering.
- *Human Smuggling*. Increased US border security has driven up human smuggling fees. Human smuggling continues, with the average fee to smuggle someone into the United States from Mexico and Central America averaging $4,000. In general, human smuggling involves transporting individuals who have consented to their travel.
- *Human Trafficking*. Human trafficking, by contrast, involves movement of non-consenting persons. Cash is the most common form of payment in this $32 billion annual industry. Recently the DOJ included in charges against an advertising website accused of facilitating prostitution and money laundering that the site facilitated human trafficking by misrepresenting the nature of the business to credit card companies and routing payments through shell companies.
- *Corruption.* Though domestic corruption persists as a threat within the United States, "offenses involving foreign corruption can have a significant, negative impact on the US financial system, including possibly skewing markets. By some estimates, the proceeds of corruption equal two percent of US gross domestic product. The proliferation of corruption abroad can destabilize countries—creating economic and human rights refugees—waste US aid and other financial support from donors, and pose national security challenges to the United States."[24]
- *Transnational Criminal Organizations (TCOs)*. African, Asian, Mexican and Colombian, and Eurasian TCOs each are identified as using a wide range of typologies to facilitate laundering of the illicit proceeds of their criminal activity.

The NMLRA identified cash use as the most critical vulnerability related to money laundering: "U.S. currency remains a significant money laundering vulnerability because its use is often anonymous, despite reporting requirements for financial institutions, individuals, and persons engaged in a trade or business. The Federal Reserve Board (FRB) estimates that between one-half and two-thirds of the value of all U.S. currency in circulation is held abroad. This widespread use of U.S. currency internationally makes it difficult for authorities to know when someone is accumulating illicit cash or merely attempting to protect their life savings. Although identifying the illicit use of currency is difficult, the required reporting domestically, including SARs, provides FinCEN and law enforcement with useful indicators for criminal investigations and trend analysis."[25]

The principal risks and vulnerabilities related to use of US currency are:

- *Bulk Cash Smuggling.* Though it remains one of the main methods Mexican drug cartels use to move illicit drug proceeds across the southwest US border to Mexico, there has been a steady decrease in the number of bulk cash seizures throughout the United States since 2013, potentially indicating that TCOs are increasingly using other, more discreet methods of moving illicit money, such as TBML, or that law enforcement is targeting other money laundering activities away from the borders.
- *Structuring.* Evasion of reporting and record-keeping requirements remains a significant risk, as individuals committing illicit activity (e.g., healthcare fraud, drug trafficking, identify theft) continue to structure cash withdrawals and deposits in the hopes of avoiding Currency Transaction Reports (CTRs) or internally set thresholds to avoid detection of their crimes.
- *Funnel Accounts.* Criminal actors will use a single bank account to collect or pool deposits from various locations and individuals to facilitate transactions in illicit activity; this is a common typology seen in transactions related to human smuggling and human trafficking.
- *Virtual Currency.* Virtual currencies not only have become the payment of choice for the purchase of illicit drugs and goods on the dark web, or in response to ransomware attacks, but also are now used as a money laundering vehicle to further layer transactions and hide the origins of dirty money.
- *Misuse of Legal Entities*. "Bad actors consistently use shell companies to disguise criminal proceeds, and U.S. law enforcement agencies have had no systematic way to obtain information on the beneficial owners of legal entities."[26] The new CDD Rule (effective May 2018), which requires covered financial institutions in the United States to collect and verify the personal information of the beneficial owners who own and/or control companies when those companies open accounts, will make it harder for criminals to circumvent the law through opaque corporate structures.
- *Complicit Merchants, Professionals and Financial Services Employees.* Criminal organizations often will look for potential accomplices with placement and access to the US financial system to facilitate their money laundering activity.
    - *Merchants.* Overall improved compliance by financial institutions related to cash reporting requirements and AML laws has led to an increase in alternative mechanisms of moving illicit funds, such as TBML, not only via traditional South American Black Market Peso Exchange schemes, but also involving Chinese suppliers of synthetic opioids or Peruvian drug traffickers purchasing gold illegally mined and then sold to US refineries.
    - *Attorneys.* Attorneys can facilitate laundering of criminal proceeds either intentionally (by means of misuse of their Interest on Lawyers Trust Account, particularly seen in drug trafficking cases) or unwittingly (such as by helping criminal clients establish legal entities, open bank accounts and engage in other "transactional" activities).
    - *Real Estate Professionals*. Illicit activity has been identified involving borrowers (who, as part of a money laundering scheme, commit bank fraud by falsifying loan documents to secure a mortgage or refinance a property, and then pay the loan off with illicit proceeds) and industry insiders who commit and/or facilitate mortgage fraud.

- *Financial Services Employees.* Risks involving financial institutions involve not just employees who serve as accomplices to facilitate money laundering but also criminals who purchase or obtain control of foreign or domestic institutions to further their criminal schemes. At-risk employees include bankers, MSB operators, broker-dealers and precious metals dealers.

- *Compliance Deficiencies.* Lax compliance with BSA, AML and sanctions requirements by banks, retailers, casinos, foreign currency exchangers, financial advisors and broker-dealers creates an environment that allows money laundering to continue undetected and uninterrupted.

4. Prepaid Cards

Reports indicate that the recent trial of Sinaloa cartel leader Joaquin "El Chapo" Guzman has placed renewed law enforcement on the use of prepaid cards to launder money.[27] In particular, there may be increased pressure on FinCEN to finalize a 2011 proposed rule that would require persons to declare when they are moving out of the country $10,000 or more of prepaid cards, in the same way one must declare currency or traveler's checks. A related potential measure would allow law enforcement to seize prepaid cards totaling in excess of $10,000 if they are mailed cross-border, in the same way law enforcement can seize traveler's checks.

B. Changes in Regulation

1. FinCEN Customer Due Diligence Rule Implementation Update

CDD Compliance

FinCEN's CDD Rule requires covered financial institutions to establish and maintain written procedures reasonably designed to identify and verify the identities of beneficial owners for new accounts opened by legal entity customers, unless an exemption or exclusion applies.[28] Compliance was mandatory by May 11, 2018.

The rule applies to covered financial institutions—including banks, broker-dealers, mutual funds, futures commissions merchants, and commodities introducing brokers—and requires them to "look through" the nominal account holder to identify the natural persons (i.e., the beneficial owners) who own or control, directly or indirectly, certain legal entity customers and verify such information.[29] Financial institutions must also comply with FinCEN's establishment of a "fifth pillar" in the AML program requirement, which mandates that these institutions implement risk-based procedures for conducting customer due diligence.[30]

AML compliance personnel throughout the industry have developed processes to help their institutions meet CDD requirements, including (i) a CDD working group to review these issues; (ii) a review of policies and procedures by internal and/or external counsel; (iii) preparation of new training materials for employees; and (iv) an evaluation of how CDD information may be leveraged to satisfy other obligations, such as sanctions and tax compliance and AML reporting.

Beneficial Ownership

The beneficial ownership requirement applies to accounts opened at a covered financial institution by certain legal entity customers. The requirement applies only to "accounts" opened after the May 11, 2018, compliance date. For preexisting accounts, covered financial institutions must obtain beneficial ownership information when they learn in the course of their normal monitoring that the beneficial owner of a legal entity customer may have changed, or if they

identify a risk factor that militates in favor of collecting such information. (See below for further discussion on monitoring.)

Legal entity customers whose new accounts are subject to the rule include corporations, limited liability companies and partnerships, and other similar domestic or foreign business entities—but *not* non-statutory trusts. There are several exclusions to the definition of a legal entity customer. Some key exclusions include banks, bank holding companies, SEC- and CFTC- registered entities, and entities listed on the New York, American or Nasdaq stock exchanges.

A "beneficial owner" is a natural person who satisfies the requirements of either the ownership prong or the control prong of the CDD Rule.[31] FinCEN emphasized in the final rule that the financial institutions can generally rely upon the legal entity customer's identification of the beneficial owners.[32]

Ownership Prong

Under the ownership prong, a covered financial institution must identify each individual who owns, directly or indirectly, 25 percent or more of the equity interests in the legal entity customer.[33] If the beneficial owner under the ownership prong is an entity excluded from the definition of a legal entity customer, no beneficial owner need be identified with respect to that excluded entity. If no individual owns 25 percent or more of the equity interests, the covered financial institution would identify a beneficial owner under the control prong only.

Control Prong

Under the control prong, a covered financial institution must identify a single individual with significant responsibility to control, manage or direct the legal entity customer.[34] A legal entity customer must always designate an individual under the control prong, but it can use an individual already designated under the ownership prong if that is factually accurate. FinCEN said in the final rule that the control prong is designed to ensure that the financial institution has a record of at least one natural person associated with the legal entity customer.

Certain legal entity customers, such as non-excluded pooled investment vehicles and domestic nonprofit organizations, are subject only to the control prong.

Identification and Verification Process

Covered financial institutions must verify beneficial owners identified pursuant to the rule. Identification must occur at the time the new account is opened, and may be accomplished by having the customer fill out a standard Certification Form or by obtaining by another means the information required by the Certification Form.[35] Pursuant to either method, the individual opening the account on behalf of the legal entity customer must certify that the information provided on the form is true and accurate to the best of his or her knowledge.

Covered financial institutions may rely on the beneficial ownership information provided by their customers but must verify the identity of the beneficial owners.[36] The verification procedures must be risk-based and must, at a minimum, contain the elements required for verifying the identity of customers pursuant to the Customer Identification Program (CIP) requirements, except that documentation may be provided through photocopies rather than original documents. Like CIP requirements, to which all covered financial institutions are already subject, verification must be completed within a reasonable time after the account is opened. Covered financial institutions may legally rely on other financial institutions to fulfill beneficial ownership obligations under the same conditions that apply to CIP reliance.[37]

FinCEN expects covered financial institutions to use the collected beneficial ownership information in other areas of compliance, such as sanctions, other AML filing requirements, and tax reporting, investigations and compliance.[38]

A Note on Intermediated Accounts

If an intermediary is the customer and the financial institution has no CIP obligation with respect to the intermediary's underlying clients pursuant to existing guidance, then the financial institution should treat the intermediary, and not the intermediary's underlying clients, as its legal entity customer.

CDD Procedures to Implement the Fifth Pillar of the AML Program Requirement

In addition to the beneficial ownership requirement, the CDD Rule requires covered financial institutions to establish risk-based CDD procedures to understand the "nature and purpose of the customer relationship," to conduct ongoing monitoring to identify and report suspicious transactions, and to update customer information. These elements of the CDD Rule apply to all customers of covered financial institutions, including those customers that are exempted from the beneficial ownership requirement.

The CDD Rule states that ongoing monitoring is conducted to identify and report suspicious transactions. FinCEN's expectation is for financial institutions to conduct a "monitoring-triggered" update of customer information when they detect, during the course of their normal monitoring, information relevant to assessing or reevaluating the risk of a customer relationship. However, FinCEN did not specify which triggers should be used.

This aspect of CDD should require less additional activity for compliance (at least in theory) because, as FinCEN asserted in the rulemaking process, this so-called fifth pillar merely formalizes prior practices that were necessary in order for financial institutions to meet their suspicious activity reporting obligations.

<u>CDD Rule FAQs</u>

In April 2018, FinCEN issued much-anticipated frequently asked questions (CDD Rule FAQs) that provide additional guidance to financial institutions relating to the implementation of the CDD Rule.[39] In general, the FAQs clarify certain issues that have caused implementation challenges for financial institutions and provide greater detail for those seeking to comply with the CDD Rule.

The FAQ topics generally include identification, collection and verification of beneficial ownership information; the accounts subject to the beneficial ownership requirements; customers and accounts excluded from the beneficial ownership requirements; CTR filing with respect to beneficial owners; and ongoing customer monitoring.

Fifth Pillar Requirements

FAQ 37 states that "[f]inancial institutions must implement risk-based procedures as part of their AML program to demonstrate an understanding of the nature and purpose of customer relationships to develop customer risk profiles."[40] Customer risk profiles should include "the information gathered about a customer at account opening," which is "used to develop a baseline against which customer activity can be assessed for suspicious activity reporting."[41] If account activity changes relative to the baseline of the original nature and purpose of the account, risk-based ongoing monitoring may identify a need to update customer information, such as beneficial ownership.[42]

Updating Beneficial Ownership Information

As a general matter, the FAQs make clear that the CDD Rule establishes a minimum standard—a 25 percent ownership interest in the legal entity customer—of beneficial ownership information that financial institutions must collect and verify. However, financial institutions may choose to collect and verify beneficial ownership information at a lower ownership threshold than the rule requires.[43] FinCEN also states that "[t]here may be circumstances where a financial institution may determine" that collecting information at a lower threshold "may be warranted."[44]

Application of the Rule and Relationship With Ongoing Monitoring

The CDD Rule only applies to new accounts opened after its May 11, 2018, effective date.[45] The FAQs make clear that there is no affirmative obligation to obtain beneficial ownership information from customers with accounts opened prior to May 11, 2018, nor is there an affirmative requirement to periodically update or solicit such information for any account.

A financial institution must, however, update existing beneficial ownership information for any client when—in the course of normal monitoring relevant to assess or reassess the customer's overall risk profile—the financial institution becomes aware of information about the customer or account that includes a possible change of beneficial ownership information.[46] Financial institutions must also update beneficial ownership information for an existing client that opens a new account, although the financial institution may be able to rely on a customer certification in certain circumstances.

Reasonable Reliance on Information Provided by Customers

FinCEN emphasized throughout the FAQs that financial institutions may rely on information provided by customers when such reliance is reasonable—i.e., when the financial institution has "no knowledge of facts that would reasonably call into question the reliability of such information."[47] For example, financial institutions do not need to independently investigate a legal entity customer's ownership structure, and they may instead reasonably rely on information provided by the customer.[48] Financial institutions may also rely on the information provided by the legal entity customer to determine whether the legal entity is excluded from the definition of a legal entity customer, provided the institution has no knowledge of facts that indicate the contrary.[49]

Interplay Between CDD and CIP

Under the CDD Rule, financial institutions are required to verify beneficial ownership according to risk-based procedures that contain, at a minimum, the same elements institutions use to verify customer identity under the CIP rules.[50] However, the CDD and existing CIP procedures do not need to be identical. Financial institutions may use the same documentary and nondocumentary methods of verification as those for CIP. Unlike CIP, the CDD Rule permits some variances, such as allowing photocopies and reproductions of documents.[51]

Existing Customers

The requirement to collect and verify beneficial ownership information applies to every new account opening, although FinCEN's FAQs have softened somewhat the steps financial institutions must take for existing customers.[52] For existing customers subject to CIP, financial institutions may rely on information obtained through CIP to fulfill the

identification and verification requirements of the CDD Rule, provided that a representative of the customer "certifies or confirms (verbally or in writing) the accuracy of the pre-existing CIP information."[53] Similarly, if a customer opens multiple accounts at a financial institution, simultaneously or not, the financial institution may rely on the information already obtained from the customer, provided the customer "certifies or confirms (verbally or in writing) that such information is up to date and accurate at the time each subsequent account is opened and the financial institution has no knowledge of facts that would reasonably call into question the reliability of such information."[54]

Foreign Customers

FinCEN included a number of FAQs about foreign customers.[55] For example, although companies traded on US stock exchanges are excluded from the definition of a legal entity customer, companies traded on foreign exchanges are not excluded, so financial institutions must collect and maintain beneficial ownership information about such customers.[56] Furthermore, financial institutions may not take a "risk-based approach" to collecting the required beneficial ownership information from legal entity customers listed on foreign exchanges.[57] Institutions may, however, rely on the public disclosures of such entities as they may with other legal entity customers (whether listed or not), "absent any reason to believe such information is inaccurate or not up-to-date."[58]

A foreign financial institution (FFI) is excluded from the definition of a legal entity customer if its foreign regulator collects and maintains beneficial ownership information about the FFI.[59] If the foreign regulator does not collect such information, however, covered financial institutions must do so.[60] Consistent with a general theme in the CDD Rule, financial institutions may rely on the representations of the FFI as to whether this exclusion applies to that FFI, provided that the institution does not have knowledge of facts that would reasonably call into question the reliability of such representations.[61]

Absent reliance on a reasonable representation from the FFI, FinCEN suggests that financial institutions should contact the relevant foreign regulator "or use other reliable means" to determine whether the foreign regulator maintains beneficial ownership information.[62] The US government will not maintain a list of non-US jurisdictions where regulators maintain beneficial ownership information for FFIs they regulate or supervise.[63] Financial institutions are not required to research the specific transparency requirements a foreign regulator may impose and compare them to US AML requirements—rather, the inquiry is simply whether a foreign regulator for the FFI collects and maintains information on the beneficial owner(s) of the regulated institution.[64]

Securities Industry

Two of the FinCEN FAQs discuss the opening of subaccounts and pooled investment vehicles.

First, FinCEN clarified that the beneficial ownership requirement does not apply when financial institutions open additional accounts or subaccounts for a legal entity customer for the institution's own record-keeping or operational purposes (such as to accommodate trading strategies); rather, it applies when an account is opened at the customer's request.[65]

Second, FinCEN stated that, in general, financial institutions are not required to "look through" a pooled investment vehicle to identify beneficial ownership information. However, financial institutions are required to collect beneficial

ownership information about the pooled investment vehicle under the "control prong" of the rule, i.e., about "an individual with significant responsibility to control, manage, or direct the vehicle."[66]

CTR Reporting Requirements

The CDD Rule does not change existing CTR reporting requirements.[67] "[C]overed financial institutions should presume that different businesses that share a common owner are operating separately and independently from each other and from the common owner."[68] Thus, FinCEN does not expect transactions across commonly owned legal entity customers to be aggregated absent indications that the businesses are not operating independently (e.g., same staff or location, or accounts of one business are repeatedly used to pay the expenses of another business).

Financial institutions are also not required to list beneficial owners of a trust or estate account when completing a CTR. A financial institution must list a beneficial owner in Part 1 of the CTR only if the institution has knowledge that the transaction or transactions requiring the filing are made on behalf of the beneficial owner and result in either cash in or cash out totaling more than $10,000 during any one business day.[69]

2. FinCEN Expands GTOs

In November 2018, FinCEN issued revised GTOs covering counties in a dozen major US metropolitan areas: Boston, Chicago, Dallas-Fort Worth, Honolulu, Las Vegas, Los Angeles, Miami, New York City, San Antonio, San Diego, San Francisco and Seattle.[70] The GTOs require title insurance companies to report non-mortgage cash real estate transactions in which the purchase was made by cash, check, wire or virtual currency above the $300,000 reporting threshold for each covered city (significantly lower than some of the previous thresholds).

GTOs were initially promulgated in 2016 and applied only to Manhattan (for purchases over $3 million) and Miami-Dade County (for purchases over $1 million). The GTOs have steadily expanded to apply to more jurisdictions and lower transaction thresholds and are consistent with the general theme of federal financial regulators promulgating measures designed to increase transparency in financial transactions as a means to clamp down on money laundering.

3. New York Department of Financial Services "Rule 504"

NYDFS Rule 504 imposes three principal requirements on NYDFS-regulated institutions: (1) implementation of an AML transaction monitoring program; (2) implementation of a watch-list filtering program; and (3) a certification requirement. The certification requirement reflects a continuing trend by NYDFS and federal regulators toward holding executives individually accountable for an institution's perceived AML and sanctions program failures.

- *Transaction Monitoring Program*. The rule requires regulated institutions to maintain a reasonably designed transaction monitoring program to monitor for potential violations of the BSA and to comply with suspicious activity reporting obligations. The program can be either manual or automated and should be based on the institution's risk assessment.
- *Filtering Program*. Regulated institutions are required to maintain a manual or automatic filtering program reasonably designed to interdict transactions prohibited by OFAC sanctions programs. The filtering must be based on the institution's risk assessment, and it must include the attributes specified in the regulation, to the extent they are applicable.

- *Compliance Certification*. The rule requires regulated institutions to adopt either an annual board resolution, signed by each director, or a senior officer "compliance finding" (included as "Attachment A" in the rule) to certify compliance. The certification must state that the financial institution's systems comply with the substantive and subjective requirements for AML transaction monitoring and filtering programs, not simply that they are reasonably designed to detect money laundering and to block sanctioned transactions.

April 15, 2018, was the due date for the first annual certifications of compliance with NYDFS Rule 504 AML transaction monitoring and filtering program requirements.[71]

FAQs About the Rule

In October 2017, NYDFS issued five FAQs regarding the rule for regulated institutions as they prepared to submit certifications for the first time in April 2018.[72]

- First, the "compliance finding" in the rule directs the board or senior officers to certify the date the institution came into compliance with the rule. NYDFS clarified that regulated institutions should use April 15 of the given year as the "as of" date for their transaction monitoring and filtering program certification.[73]
- Second, the NYDFS stated clearly that a regulated institution may not submit a compliance finding if it is in the midst of adapting its systems to come into compliance with the rule. A regulated institution "may not submit a certification" under the rule "unless the Regulated Institution is in compliance with the requirements of Part 504 as of the effective date of the certification."[74]
- Third, in response to a question about whether a regulated institution should send additional documentation with the certification to prove compliance, NYDFS said that explanatory material was not required. However, the NYDFS noted that regulated institutions are expected to retain documents and records necessary to support the certification in the event the NYDFS asks for them. And, to the extent that a regulated institution has identified areas, systems and processes that require improvement, it should document efforts to ameliorate deficiencies and maintain those documents for inspection during an examination, under the rule.[75]
- Fourth, in response to a question about whether NYDFS will require a pre-implementation test for systems a regulated institution used prior to the rule, NYDFS clarified that it will not require a full, end-to-end testing of the systems that an institution operated before April 15, 2018. But NYDFS noted that the rule requires regulated institutions to review and periodically update their systems and programs "at risk-based intervals."[76] Accordingly, NYDFS expects regulated institutions to conduct periodic, risk-based testing of their systems to support their AML programs.[77]
- Finally, the rule requires each transaction monitoring and filtering program to have qualified personnel or outside consultants to conduct the design, implementation and validation of the transaction monitoring and filtering programs.[78] The NYDFS clarified in its FAQs that it does not require a regulated institution to conduct a vendor selection process for the systems that were engaged prior to the effective date of the regulation, although it does require an institution to conduct a vendor selection process when hiring a new vendor to implement the transaction monitoring and filtering program. Accordingly, the guidance appears to alleviate the concern for regulated institutions to conduct and document vendor selection processes on all

existing vendors prior to April 15, 2018. However, in the same FAQ, NYDFS seems to complicate the picture, noting that the rule requires regulated institutions to engage "qualified" personnel or outside consultants for such purposes, and encourages entities to "have processes in place to confirm that the personnel and vendors it has engaged to execute its transaction monitoring and filtering program are qualified and competent."[79]

C. Significant Regulatory Guidance

1. Federal Regulators' Joint Statements Contemplate Modern Approaches to AML Compliance

In late 2018, regulators endorsed the use of cutting-edge technology and collaborative structures to help banks meet their BSA/AML obligations, while still reiterating that institutions' core regulatory responsibilities remain unchanged. While these statements from regulators are significant, there is a lot that is still unknown about how these statements will translate into examinations and regulatory expectations.

On October 3, 2018, federal regulators (FinCEN, the FRB, the FDIC, the NCUA, and the OCC) issued a joint statement describing instances in which banks might seek to enter into collaborative arrangements and share resources to manage BSA/AML obligations more efficiently and effectively.[80] The statement highlighted several possible benefits of such arrangements, including that banks might elect to (i) share personnel and resources to conduct internal-controls functions, such as developing and reviewing BSA/AML policies and monitoring processes; (ii) use personnel at a partner bank to conduct the required independent BSA/AML compliance testing; or (iii) share the cost of hiring qualified BSA/AML trainers among several banks. However, the statement also highlighted possible pitfalls of doing so: It may not be appropriate for banks to share a BSA compliance officer, and any collaborative relationships should be formalized by a contract with adequate protections for each institution's confidential information. Additionally, even under collaborative arrangements, each bank remains responsible for ensuring its own BSA/AML compliance.

On December 3, 2018, the same group of regulators issued another joint statement encouraging banks to consider and implement "innovative efforts to combat money laundering and terrorist financing" through the deployment of novel technologies.[81] Although the regulators stated that they would not require particular methods or technologies, and would not penalize banks that maintained effective compliance programs that do not make use of these tools, they encouraged banks to tap into "private sector innovation" and committed to "continued engagement with the private sector" in pursuit of more effective solutions—for instance, through FinCEN's BSA Advisory Group and FinCEN's new "innovation initiative." As examples of innovative approaches already being pursued, the regulators specifically highlighted "internal financial intelligence units" and the use of artificial intelligence and digital identity technologies. Critically, the regulators clarified that they will not automatically assume that a bank's existing process is deficient if the bank's innovative pilot program detects suspicious activity that went undetected by the existing process. This reassurance is vital to encouraging banks' experimentation with novel and sophisticated approaches to detecting illicit activity.

Taken together, these statements demonstrate willingness on the part of federal regulators to consider how banks may use new technologies in BSA compliance activities to lower costs without increasing risk.

2. FinCEN Exchange

Consistent with the move toward innovation and collaboration, FinCEN announced the creation of the "FinCEN Exchange," a new voluntary platform to facilitate information sharing between the government and industry on topics related to AML and other financial crime issues.[82] The program represents a significant step forward on two related priority areas for FinCEN: information sharing and public-private partnerships. The press release publicizing the creation of the FinCEN Exchange also touted the benefits of 314(b) sharing, an example of wholly private sector information sharing.

In a speech announcing the creation of the FinCEN Exchange, Treasury Under Secretary for Terrorism and Financial Intelligence Sigal Mandelker cited industry appetite for increased "outreach, discussion, and information" as a primary motivation for the new initiative.[83] In recent years, there have been repeated calls to strengthen these areas—particularly in light of the success of the United Kingdom's Joint Money Laundering Intelligence Taskforce, which has received accolades from financial services industry participants, government and law enforcement alike.

Although channels such as the Bank Secrecy Act Advisory Group already exist for the industry to provide feedback to FinCEN, the FinCEN Exchange will provide a new and more regularized mechanism to do so. In addition to being an opportunity for the industry to obtain information from the government to help identify and prioritize risks so industry can "channel[] resources toward high-priority targets[,]" the exchange will serve as another forum that will underscore the industry's significant AML efforts.[84]

Details About the FinCEN Exchange

The FinCEN Exchange convenes briefings among FinCEN, law enforcement and financial institutions to exchange targeted information on priority illicit finance threats, such as specific money laundering methods and typologies. Participation in the program is strictly voluntary and does not introduce any new regulatory requirements. It is unclear which financial institutions will participate in the FinCEN Exchange, or how those institutions will be selected; it is possible that the program will be invitation-only, at least in the near term.

Endorsement of 314(b) Sharing

The press release announcing the exchange also encouraged "314(b)" sharing among financial institutions.[85] Section 314(b) of the USA PATRIOT Act provides financial institutions and associations of financial institutions a safe harbor from civil liability to their customers for sharing "information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist or money laundering activities."[86] Financial institutions share information under that provision to facilitate investigations of potential money laundering or terrorist financing activity and the creation of more complete SARs to law enforcement.

In addition to traditional bilateral 314(b) sharing, Mandelker said the government is "highly encouraged" by bank efforts to form "consortia to share information more dynamically" under Section 314(b), adding that "these groups of financial institutions have provided substantial insight into illicit finance threats that otherwise may be invisible to a single institution."[87]

3. FinCEN Advisories

FinCEN has issued a number of other advisories, with a focus on public corruption, potentially fraudulent activity related to disaster relief efforts, and the FATF update to its list of jurisdictions with AML deficiencies. FinCEN

advisories are also increasingly linked to sanctions targets such as Venezuela, increasing the imperative for the different components of financial institutions focused on AML and sanctions to collaborate in the effort to detect and prevent financial crime.

- On September 6, 2017, FinCEN issued an advisory alerting financial institutions to the possibility that certain South Sudanese senior political figures could be using the US financial system to hide proceeds of public corruption.[88] FinCEN reports that, according to the Department of State, various forms of corruption in South Sudan have increased since the beginning of the South Sudanese Civil War in December 2013, including abuse of position and use of shell companies, abuse of government contracting, and abuse of military procurement and payrolls. The alert highlighted individuals and companies who have been sanctioned by OFAC and the United Nations, and reminded financial institutions of due diligence and SAR filing obligations with respect to South Sudan.
- On September 20, 2017, FinCEN issued an advisory alerting financial institutions of widespread public corruption and money laundering in Venezuela, and warning that Venezuelan government agencies and bodies, including state-owned entities, appear vulnerable.[89] The advisory suggests that financial institutions take "risk-based steps to identify and limit any exposure they may have to funds and other assets associated with Venezuelan public corruption."[90] It identifies several red flags to assist financial institutions in identifying suspicious activity, including the use of state-owned entities and government contracts, wire transfers from shell companies, and transactions for the purchase of real estate, particularly in South Florida and Houston. FinCEN updated this advisory on May 3, 2019, with typologies used in connection with Venezuelan public corruption and money laundering, and attendant red flags.[91]
- On October 31, 2017, FinCEN issued an advisory regarding potentially fraudulent activity related to disaster relief efforts.[92] The advisory warns financial institutions to pay particular attention to benefits fraud, charities fraud and cyber-related fraud.
- FinCEN issued advisories on April 3, 2017,[93] October 31, 2018,[94] and March 8, 2019,[95] focused on FATF's update to its list of jurisdictions with strategic anti-money laundering and countering the financing of terrorism (AML/CFT) deficiencies, and cautioned financial institutions to consider the changes when reviewing their policies and procedures. Notably, in 2017, FATF added Ethiopia to the list due to a lack of effective implementation of its AML/CFT framework. In 2018, FATF added the Bahamas, Botswana and Ghana to the list. In addition, the advisories highlighted that the Democratic People's Republic of Korea (DPRK) is subject to FATF's call for its members to apply countermeasures to protect the international financial system from AML/CFT risks stemming from the DPRK. In 2018, FATF also advised financial institutions to apply enhanced due diligence in connection with Iran. Finally, in 2019, FATF "reaffirm[ed] its 25 February 2011 call on its members and urges all jurisdictions to advise their financial institutions to give special attention to business relationships and transactions with the DPRK, including DPRK companies, financial institutions, and those acting on their behalf."
- FinCEN issued an advisory on June 12, 2018, highlighting the connection between "corrupt senior foreign political figures and their enabling of human rights abuses."[96] The advisory warns US financial institutions to be wary of the possibility that such individuals might use US "financial facilitators" to "move or hide illicit proceeds," thereby exposing those institutions to regulatory risk. The advisory lists several red flags that

may help institutions identify such behavior—including, for example, the use of third parties, family members, shell companies or other means of concealing ownership; transactions involving government contracts that are directed to shell companies or companies operating in an unrelated line of business; and invoices relating to government contracts that include substantially above-market prices, overly simple documentation, a lack of details or some combination of the above. Advisories like this put a premium on the ability of financial institutions to identify customers who are PEPs so that they may take appropriate risk management steps with respect to those accounts.

- On October 4, 2018, FinCEN issued an advisory warning financial institutions of an "increasing risk" that funds tied to political corruption in Nicaragua might enter the US financial system.[97] FinCEN noted that the US government has "strongly condemned" the violence, corruption and human rights abuses associated with the regime of Nicaragua's president, Daniel Ortega, and that "senior members of the Ortega regime" might accordingly be seeking to move assets out of the country. FinCEN referred financial institutions to its June 12 advisory and requested that institutions file SARs when their monitoring processes detected activity potentially associated with the Ortega regime or any other misuse of Nicaraguan public funds.
- On October 11, 2018, FinCEN issued an advisory concerning the AML/CFT risks posed by certain transactions related to Iran.[98] Iran's government, FinCEN explained, has long exploited and abused the global financial system, often in an effort to support the regime's "nefarious activities" or to fund terrorist groups in Iran and other Middle East countries. Many of Iran's abuses have involved officials of the Central Bank of Iran using "exchange houses," shell companies and/or virtual currencies to procure cash, technology and/or services. FinCEN advised banks to be particularly attentive to red flags of this sort and to conduct additional monitoring and inquiries to detect illicit Iran-linked activity—particularly in light of the US government's reimposition of sanctions on Iran.

4. Public Response to Tax Regularization Program Inquiry

In February 2018, FinCEN released its response to an inquiry from the Florida Bankers Association regarding whether a bank must file a SAR upon a customer's inquiry into, or participation in, a tax regularization program, which affords taxpayers an opportunity to become current on their taxes.[99] FinCEN stated that a mere customer inquiry does not on its own constitute a suspicious transaction or activity for the purposes of the SAR rules. Additionally, the inquiry about or participation in such a program, independent of other factors, does not give a financial institution notice of past activity that would require the filing of a SAR, because individuals could choose to participate in a tax regularization program for a number of legitimate reasons. Although FinCEN stated that there is no SAR filing obligation, a financial institution may choose, as a part of its overall risk assessment, to undertake a review of the customer and related account activity in light of the customer's inquiry about or participation in such a program.

5. SEC and FINRA Examination Priorities

In early 2019, the SEC and Financial Industry Regulatory Authority (FINRA) announced their examination priorities for the year. FINRA also published a report on its exam findings from 2018.[100] AML continues to be a priority for both regulators. The SEC's stated priorities for 2019 were similar to those from the past several years. They included examining whether broker-dealers are "meeting their SAR filing obligations, implementing all elements of their AML program, and robustly and timely conducting independent tests of their AML program."[101]

FINRA, too, stated its intention to focus on AML in 2019. The regulator emphasized its continued interest in examining firms' compliance with the CDD Rule as well as a focus on data integrity in connection with suspicious activity monitoring systems and "the decisions associated with changes to those systems."[102] FINRA also identified AML compliance as an area of focus in connection with digital assets.[103]

In its 2018 Examination Findings Report, FINRA identified "challenges" it observed in broker-dealers' AML compliance, including new challenges it observed, as well as challenges it has observed in the past.[104] The three principal new challenges are (i) "questionable" or unknown ownership status of foreign legal entity accounts (including seemingly unrelated accounts with shared interests, indicating potential overlapping beneficial ownership); (ii) no documentation of investigations of potentially suspicious activity; and (iii) irregular and undocumented 314(a) searches. The challenges present in past years include issues with the overall adequacy of certain firms' AML programs; difficulties allocating AML monitoring responsibilities, especially in respect of trade monitoring; data integrity in AML automated surveillance systems (especially in connection with "suspense accounts" for foreign currency transactions); sufficiency of firm resources for AML programs; and independent testing of AML monitoring programs.

D. Congress

After years of calls from industry, Congress has considered multiple serious AML reforms in recent years to modernize financial institutions' BSA requirements. Four bills merit specific discussion. First, in 2016, the Counter Terrorism and Illicit Finance Act (H.R. 6068) was introduced by Reps. Steve Pearce (R-NM) and Blaine Luetkemeyer (R-MO). Among other things, the bill would (i) raise CTR and SAR thresholds; (ii) increase information sharing; (iii) provide for a FinCEN "no-action letter" program; and (iv) promote the use of technological innovations. The bill was reportedly scuttled because of a provision that would have required corporations to disclose their beneficial owners at the time of company formation. The provision had gained the support of the Delaware secretary of state, an important stakeholder for corporate formations in the United States, but it was ultimately removed from the bill, reportedly because it may burden companies during incorporation.

Second, Rep. Maxine Waters (D-CA), the chairwoman of the House Financial Services committee, released a draft bill proposing sweeping changes to AML safeguards. According to a memo produced by the House Financial Services Committee regarding the bill, it would impose stricter rules on art and real estate transactions, strengthen whistleblower protections, increase damages for BSA offenders, allow FinCEN to offer more competitive salaries for hiring purposes, permit banks to share SARs with foreign affiliates, and mandate the appointment of a civil liberties and privacy officer at the Treasury Department.[105]

Third, Rep. Carolyn Maloney (D-NY) reintroduced a bill she first authored in 2017, titled the Corporate Transparency Act. The bill, if passed, would require corporations and LLCs to disclose their beneficial owners to FinCEN to ensure sanctioned persons cannot evade rules banning their beneficial interest by assisting law enforcement agencies and banks in policing their customers.

Finally, Rep. Stephen Lynch (D-MA) introduced the Kleptocracy Asset Recovery Rewards Act (H.R. 389). The act creates discretionary monetary rewards to incentivize individuals to tell the government about any information that assists the government in rooting out corruption.

III. Sanctions Regulatory Trends and Developments

Sanctions continue to play a central role in US foreign policy and national security. Like his predecessors, President Trump has issued a series of executive orders establishing or expanding sanctions against such disparate targets as Nicaragua and Iran and for election interference. At the same time, President Trump has also, notably, withdrawn the United States from the Joint Comprehensive Plan of Action (JCPOA), the multilateral agreement in which the United States had committed to certain sanctions relief for Iran in exchange for Iranian commitments to constrain its nuclear program. Meanwhile, in summer 2017, Congress significantly escalated US sanctions against Russia, creating a range of new sanctions authorities that expose non-US companies to severe consequences; the Trump Administration has been slowly implementing several of those authorities.

In a sharp departure from the efforts of both the Bush and Obama Administrations to pursue harmonized, multilateral sanctions strategies, US sanctions have become more unilateral, leading to a divergence in sanctions between the United States, on the one hand, and those of the EU, Canada, Switzerland, Japan and other countries. This conflict of law presents global companies with a fast-changing and complex set of sanctions-related risks. We expect this trend to further accelerate throughout 2019, especially as the United States seeks to use sanctions to pressure Iran, North Korea and Venezuela in a wide range of circumstances. Additional sanctions pressure may also come as a result of congressional oversight and legislation, including possible additional designations of Russian targets.

It remains essential for financial services firms and others to take account of the key developments in US sanctions enacted since the beginning of the Trump Administration. New sanctions create new risks—and new opportunities—and successfully navigating this area of law requires careful attention and strategic planning.

A. Russia

In 2017 Congress led the effort to ratchet up US sanctions against Russia by passing the Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA). President Trump signed the bill into law on August 2, 2017, and, since that time, members of Congress have been consistently pressing for executive action to implement CAATSA's new sanctions authorities, in spite of an often-reluctant chief executive (the Treasury Department appears somewhat more willing). As discussed further below, the United States also took steps to trigger the imposition of new sanctions against Russia under the Chemical and Biological Weapons Control and Warfare Elimination Act of 1991 (CBW Act).

CAATSA

CAATSA codified existing US sanctions against Russia that the United States had imposed after the Russian invasion of Ukraine in 2014 and requires that the President submit notices or reports to Congress in a variety of circumstances, including any action to relax certain measures. This codification and the requirement for presidential coordination with Congress prior to any change to the sanctions cover those sanctions established by past statutes (in addition to those established under CAATSA) as well as executive orders issued by President Obama concerning Russia, Ukraine and cyber-enabled attacks connected to Russia. CAATSA thus constrains presidential discretion to terminate or waive the applicability of sanctions, and generally expands Congress's authority over the imposition, suspension or removal of sanctions against Russia.

CAATSA also established new "secondary sanctions," i.e., sanctions authorities that may be used against non-US companies even when the underlying transaction giving rise to the sanctions does not involve any US person or have

any US nexus. For example, the President may impose five or more measures from a sanctions "menu" against any person who "knowingly" engages in certain transactions tied to Russia's ability to construct energy export pipelines; in the "unjust" privatization of state-owned assets; in Syria's acquisition or development of WMD and certain conventional weapons; or with certain persons in the Russian intelligence or defense sectors. The President may also impose blocking sanctions against any person or government that knowingly engages in or provides financial services in support of the Russian government's actions to undermine cybersecurity. CAATSA also authorizes the imposition of sanctions against financial institutions and others who knowingly facilitate significant transactions for or on behalf of a Russian previously added to OFAC's Specially Designated Nationals and Blocked Persons (SDN) List or members of their family.

CAATSA tightened US sectoral sanctions against Russia by further limiting the authorized tenor of "new debt" of certain Russian banking and energy sector firms in which persons subject to US jurisdiction may deal and by expanding the breadth of sanctions targeting certain energy projects (deepwater, Arctic offshore and shale) connected to Russian energy firms. CAATSA also tightened two prior statutory authorities targeting Russian crude oil projects and Russian corruption.

In addition to the Trump Administration implementing several administrative requirements of CAATSA, the President issued E.O. 13849 on September 20, 2018, delegating authority to the Secretary of the Treasury and other administration officials to implement CAATSA's sanctions menus.[106] The executive order was accompanied by the Administration's first use of CAATSA's new secondary sanctions authorities; OFAC[107] and the State Department[108] imposed sanctions on a Chinese entity and its director for engaging in significant transactions with Russia's primary arms export company, which is on the State Department's List of Specified Persons in the defense and intelligence sectors of Russia.[109]

CAATSA also required that the Treasury Department publish a list of so-called oligarchs based on their net worth and closeness to the "Russian regime."[110] In January 2018 the Treasury Department published that list, and the public version was a list of the wealthiest Russians based on media reports. OFAC was quick to inform the public that this was not a "sanctions" list, and Secretary of the Treasury Steve Mnuchin stated at the time that actual sanctions would follow in some circumstances. As discussed below, OFAC's SDN designations of April 6, 2018, included several individuals who had appeared on the "oligarchs" list.

For additional information, refer to our Client Alert: President Expected to Sign New Sanctions Bill to Constrain Presidential Authority While Expanding "Sanctions Toolkit" for Russia, Iran and North Korea.

SDN Designations

On April 6, 2018, OFAC added several Russian government officials, oligarchs and companies that they own—including major companies in the energy and manufacturing sectors—to the SDN List. In recognition of the difficulty that many US and non-US companies faced in disentangling their business dealings from those of the newly designated SDNs, OFAC published a series of FAQs[111] and issued several iterations of general licenses authorizing the "wind down" of such business,[112] notably with Rusal plc, EN+ Group plc and JSC EuroSibEnergo, the businesses owned by Russian billionaire Oleg Deripaska. After months of engagement between the designated entities and the Treasury Department to work out an arrangement by which Deripaska would reduce his ownership in these entities below 50 percent so as to remove Rusal, EN+ and EuroSibEnergo from sanctions, OFAC notified Congress of its

intent to terminate sanctions on these entities,[113] though Deripaska himself remains an SDN. The agreement to remove Rusal and EN+ from the SDN List involves unprecedented levels of involvement by OFAC in the selection of corporate officials and governance of a non-US company. On January 27, 2019, following a failed effort in the US Senate to prevent the delisting, OFAC lifted sanctions on the entities.

CBW Act

On August 6, 2018, the State Department determined, pursuant to the CBW Act, that in March 2018 the Russian government had used a chemical weapon in the United Kingdom to poison former Russian military intelligence officer Sergei Skripal and his daughter. The CBW Act requires the imposition of certain sanctions "forthwith" following such a determination, and another set of sanctions three months later unless the United States determines that the Russian government is no longer using chemical weapons, that it has provided reasonable assurances that it will not in the future use such weapons, and that on-site inspections or other reliable means can be used to verify compliance.

The State Department formally announced the imposition of CBW Act sanctions on August 27, 2018.[114] This initial tranche of sanctions included a general prohibition on foreign assistance, suspension of sales of defense articles or services, denial of credit or other financial assistance by the US government, and a prohibition of exports of national security–sensitive goods and technology. But the State Department concurrently invoked the national security waiver authority available under the CBW Act to waive the prohibition on foreign assistance and sanctions on exports/reexports related to space flight and civil aviation, exports/reexports destined for wholly owned US subsidiaries operating in Russia, exports/reexports destined for commercial end uses and users in Russia, and deemed exports/reexports to Russian nationals.[115]

On November 6, 2018, the State Department informed Congress that it "could not certify that [the] Russian Federation met the conditions required" by the CBW Act and intends "to proceed in accordance with the terms of the CBW Act, which directs the implementation of additional sanctions."[116] However, the State Department has not, to date, imposed the second tranche of sanctions despite the statutory deadline for such sanctions having passed.

Looking Ahead

On September 12, 2018, President Trump issued E.O. 13848, "Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election,"[117] which declares the threat of foreign interference in US elections to be a "national emergency" and authorizes sanctions on non-US persons found responsible in such future election meddling.[118] On December 21, 2018, Director of National Intelligence Dan Coats issued a statement under E.O. 13848 advising that "Russia, and other foreign countries, including China and Iran, conducted influence activities and messaging campaigns targeted at the United States to promote their strategic interests" during the 2018 midterm election campaign, but that the intelligence community, per normal practice, "did not make an assessment of the impact that these activities had on the outcome of the 2018 election."[119] It has yet to be seen whether anyone will be designated for interference with the November 2018 US midterm elections, but it seems unlikely that sanctions under this authority will be forthcoming.

Congressional leaders also renewed their interest in further escalating the US sanctions against Russia following President Trump's controversial meeting with Russian President Vladimir Putin in Helsinki in July 2018. There had been several bills in the previous Congress that, if enacted, would have resulted in significant new sanctions on Russian financial and business activity. Notably, these included the Defending Elections from Threats by Establishing

Redlines Act (DETER Act) (S. 2313, H.R. 4884) and the Defending American Security from Kremlin Aggression Act of 2018 (DASKAA) (S. 3336). The bills proposed broad sanctions on Russia. For example, DASKAA's targets include investments in Russian energy projects and transactions in Russian sovereign debt, and the DETER Act seeks to penalize Russian interference in US elections and to block the property of all persons on the Department of the Treasury's oligarchs list.

While it appears unlikely that these bills or successors in the new Congress will become law in the near future, it is possible that OFAC will impose sanctions on additional Russian oligarchs (similar to the April 2018 designations), particularly if additional Russian efforts to influence the 2018 election are subsequently uncovered, if there are additional Russian efforts to undermine Ukraine's sovereignty, or if there are other acts of Russian aggression. New oligarch sanctions may also come about more organically, as a consequence of OFAC continuing to work on implementing Russian sanctions programs that have already been adopted.

B. Iran

On May 8, 2018, President Trump announced that the United States was withdrawing from the July 2015 Joint Comprehensive Plan of Action (JCPOA) that had been agreed to by Iran, the United States, the other four permanent members of the United Nations Security Council (Russia, China, the United Kingdom and France) and Germany.[120] The withdrawal was not unexpected, as the President had repeatedly criticized the agreement and had threatened withdrawal unless the agreement was renegotiated.

Under the JCPOA, the United States had waived the application of most of its secondary sanctions targeting Iran, thereby removing many of the risks that had impeded non-US companies from pursuing commercial opportunities in or with Iran, even when such activities had no US nexus and did not violate EU (or other non-US) sanctions requirements. The US and the EU also had removed a significant number of individuals and entities from the restricted party lists on which they appeared, including many of Iran's largest state-owned banks, the National Iranian Oil Company (NIOC), the Islamic Republic of Iran Shipping Lines, and Iran's national air carrier, Iran Air, among others.

With the withdrawal from the JCPOA, however, the US secondary sanctions that had previously been waived have been reimposed following two wind-down periods ending on August 7 and November 5, 2018.

The secondary sanctions reimposed on August 7 target the purchase or acquisition of US dollar banknotes by the Government of Iran; Iran's trade in gold and other precious metals; the sale, supply or transfer to Iran of (1) graphite, (2) raw or semifinished metals such as aluminum and steel, (3) coal, and (4) software for integrating industrial processes; the purchase of, subscription to or facilitation of the issuance of Iranian sovereign debt; and Iran's automotive sectors.

The secondary sanctions reimposed on November 5, in turn, include those targeting the provision of specialized financial messaging services to Iranian financial institutions, the provision of underwriting services or insurance, and the Iranian shipping sector. The United States also reimposed secondary sanctions targeting the purchase of petroleum or petrochemical products from Iran, designed to reduce exports of Iranian crude oil. OFAC also added more than 700 individuals and entities to the SDN List on November 5, covering "hundreds of targets previously granted sanctions relief under the JCPOA, as well as more than 300 new designations."[121] More generally, the Trump Administration has designated a large number of Iranian targets under existing sanctions programs.

To ease implementation burdens, at the same time that the secondary oil sanctions went into effect, the Administration granted significant reduction exceptions (SREs) for an initial six-month period to eight jurisdictions determined by the Secretary of State to have significantly reduced their oil imports from Iran: China, India, Japan, Italy, Greece, South Korea, Turkey and Taiwan; after six months, the SREs may be renewed. Others seeking an exemption, including the European Union,[122] were not granted an SRE.[123] Pursuant to the SRE, individuals and entities in countries subject to the SRE could continue to pay for petroleum and petroleum products imported from Iran. But in April 2019, the United States announced that it would not reissue the waivers, which were set to expire by the end of May 2019.

The US withdrawal from the JCPOA had an impact not only on secondary sanctions but on "primary" sanctions as well. On June 27, 2018, OFAC revoked two general licenses that had, pursuant to the JCPOA, authorized certain activities by persons subject to US jurisdiction. General License H had allowed foreign-incorporated subsidiaries of US companies to engage in certain activities in or with Iran, while General License I had authorized certain transactions concerning commercial aircraft.

The United States' withdrawal from the JCPOA has had and will continue to have significant implications for companies whose business activities involving Iran had been effectively authorized by US sanctions waivers and licensing since January 2016. Global companies may face significant challenges due to the divergence between the United States and its major trading partners, particularly in Europe and Asia, when it comes to Iran sanctions. This is especially true for banks and other financial services firms, many of which are electing to "de-risk" when it comes to Iran even if particular transactions may be lawful.

Further complicating compliance risk for European companies, the EU has recently reactivated its so-called 1996 Blocking Statute intended to penalize EU companies that comply with certain US sanctions on Iran that are inconsistent with the EU's commitments under the JCPOA. That said, the EU has not initiated any enforcement actions pursuant to the Blocking Statute despite the fact that some EU companies have already abandoned trade and investment opportunities in Iran, apparently due to reimposed US sanctions.

In an effort to moderate the impact of the reinstated US secondary sanctions, the EU, Germany, France, Britain, Russia and China have agreed to set up a special purpose vehicle (SPV) for non-US trade with Iran. The SPV, now called the Instrument in Support of Trade Exchanges, or INSTEX, was conceived of as a means to enable European companies to bypass US sanctions targeting Iran's oil and financial sectors. INSTEX will reportedly be based in Paris and will be initially used to sell only food, medicine and medical devices to Iran, but could expand its scope in the future.[124] In April 2019, Iran also announced that it has established a Special Trade and Finance Institute (STFI), similar to INSTEX, to facilitate EU-Iran trade. However, the extent to which either INSTEX or STFI will be of practical use is still unclear. US officials have suggested that the SPV will not be an effective tool to overcome ongoing sanctions risks presented by US actions to implement JCPOA withdrawal and that the United States "will aggressively pursue" those entities involved in transactions intended to evade applicable US sanctions.[125] This is in large measure because the SPV cannot insulate companies that participate in it from the reach of secondary sanctions, which do not depend on the presence of a jurisdictional nexus to the United States for their imposition.

In 2019, the United States further tightened sanctions on Iran through additional SDN designations of Iranian persons and entities, notably Iran's largest petrochemical holding group, Persian Gulf Petrochemical Industries Company. On

April 8, President Trump also announced that Iran's Islamic Revolutionary Guard Corps (IRGC), including its external special operations arm the Quds Force, would be designated as a Foreign Terrorist Organization (FTO).[126] While the designation will likely have limited practical implications—because the IRGC was previously designated under multiple sanctions authorities—the move marks the first time the United States has designated a part of another country's government as an FTO.

For additional information, refer to our Client Alert: US Reimposes Final Tranche of Iran-Related Sanctions and our Client Alert: US Reimposes First Tranche of Iran-Related Sanctions.

Looking Ahead

President Trump and members of his administration have insisted that the United States will aggressively enforce US sanctions authorities against Iran. However, the United States used secondary sanctions relatively sparingly during the Obama Administration, and each application of these sanctions raises challenging geopolitical questions for the United States. Nevertheless, we expect that the Administration will be eager to identify an opportunity to impose secondary sanctions against a non-US entity in order to demonstrate its aggressive enforcement posture. This course of action could result in drastic consequences for banks and other companies that continue to pursue opportunities in Iran, even when their business there has no US nexus. The December 2018 arrest of Meng Wanzhou, the chief financial officer of the Chinese company Huawei Technologies, which reportedly arose in connection with Meng's role in misleading two international banks about Huawei's business in Iran through an affiliated Hong Kong company, demonstrates the expansive reach of US sanctions as well as the willingness of the United States to enforce the sanctions amid high political stakes.

C. Cuba

There have been notable changes to US sanctions on Cuba in 2019, with particular impact on the tourism industry. These changes come after a quiet year in 2018, following an active 2017 in which President Trump partially reversed some of the liberalization of US-Cuba trade and travel that had occurred during the Obama Administration.

On June 16, 2017, President Trump issued a National Security Presidential Memorandum directing the Treasury Secretary and the Secretary of Commerce to adjust regulations regarding transactions with Cuba,[127] which they have done. The new rules prohibit direct financial transactions with entities that the State Department determines are closely connected to the Cuban military or intelligence services.[128] The State Department has published (and since updated) a new list, the Cuba Restricted List, that originally included 180 entities. Many of these entities are connected to the Cuban tourism industry.[129] On November 14, 2018, the Department of State added another 26 entities—including 16 hotels owned by the Cuban military—to the list.[130] The principal consequence of this prohibition is that persons subject to US jurisdiction will need to undertake additional diligence to ensure that they do not engage in *new* commercial engagements with entities listed by the State Department, including the Cuban military monopoly Grupo de Administración Empresarial S.A. Businesses may proceed with existing commercial transactions with a listed entity if their transactions were agreed to before the entity was added to the Cuba Restricted List (i.e., prior to November 9, 2017).[131]

On June 4, 2019, OFAC and the Department of Commerce's Bureau of Industry and Security (BIS) jointly announced additional restrictions involving Cuba.[132] Effective June 5, BIS amended License Exception Aircraft, Vessels and Spacecraft to remove the authorization for the export or reexport to Cuba of most noncommercial aircraft and all

passenger and recreational vessels on temporary sojourn. OFAC also amended the Cuban Assets Control Regulations to note that the export of relevant vessels or aircraft providing carrier services requires separate authorization from BIS. Notably, BIS and OFAC did not issue a concurrent general license authorizing vessels and aircraft operators to "wind down" any such transactions with Cuba.

Additionally, the new regulations now remove one of the 12 general licenses for travel to Cuba established during the Obama Administration.[133] In 2018, OFAC had limited the general license for "people to people" travel for individuals traveling to Cuba for educational exchange activities, but the 2019 changes altogether remove this general license (subject to a grandfathering provision for travel-related transactions conducted prior to June 5).

For additional information, refer to our Client Alert: The US Revises Commercial and Travel Sanctions Against Cuba.

D. North Korea

Despite a summit in Singapore between President Trump and North Korean leader Kim Jong Un on June 12, 2018, after which the President tweeted that "[t]here is no longer a Nuclear Threat from North Korea" and signaled that the United States may begin lifting sanctions even before North Korea completely denuclearizes, the United States has not eased sanctions against North Korea. In fact, the United States in 2018–19 increased sanctions pressure against North Korea, including under several key executive and legislative measures, even as others in the international community—most notably China—appear to have eased off on pressure following the Singapore summit.

In September 2017, President Trump issued E.O. 13810 to expand OFAC's authority to impose sanctions against North Korean entities, as well as non-North Korean entities that do business with North Korea.[134] The measure was quite expansive, including sectoral sanctions and status-based sanctions, drawing heavily from the architecture of US sanctions programs against Russia and Iran.

The sectoral sanctions provide for "blocking" sanctions against any person operating in targeted North Korean sectors—e.g., construction, energy, financial services, fishing, information technology, manufacturing, medical, mining, textiles or transportation, or engaging in any "significant" trade with North Korea. E.O. 13810 also authorizes the Secretary of the Treasury to block the funds of any North Korean person and authorizes secondary sanctions against non-US banks that transact business with designated North Korean entities.

Throughout 2018–19, OFAC issued several rounds of designations against individuals and entities pursuant to E.O. 13810.[135] The designations have included dozens of banks, financial representatives, shipping and trading companies, and vessels, and include persons and entities from North Korea, China, Russia, Taiwan, Singapore and Libya.

Additionally, Section 321(b) of CAATSA amends the North Korea Sanctions and Policy Enhancement Act of 2016 to further tighten preexisting restrictions under US law with respect to imported goods derived from forced labor. Section 321(b) creates a rebuttable presumption that significant goods, wares, merchandise and articles mined, produced or manufactured wholly or in part by North Korean nationals or North Korean citizens *anywhere* in the world are forced-labor goods, and therefore prohibited from importation.[136] This provision, and its related guidance (see below), indicate that US Customs and Border Protection may renew its focus on enforcing the US ban on imports derived from forced labor.

OFAC has also issued several advisories concerning risks associated with North Korea. A February 2018 advisory concerned deceptive practices used by North Korea to evade sanctions in the shipping industry, including obfuscating

the identity of vessels, the goods being shipped, or the origin or destination of cargo.[137] And, in July 2018, OFAC issued an advisory addressing the risks for businesses with supply chain links to North Korea, noting, for example, the heightened risks associated with subcontracting and consignment firms that may rely on North Korean factories; mislabeled goods, services and technology that North Korean exporters may use to disguise their provenance; joint ventures in China and elsewhere involving North Korean firms; raw materials sold by North Korean exporters at below-market prices to intermediaries; and North Korean information technology services that are disguised through front companies. The advisory also addresses the heightened risk for North Korean overseas labor, and identifies a list of countries where North Korean workers are known to be present (accompanied by an annex identifying the industrial sectors in those countries in which North Korean workers are known to be employed).[138] These advisories, which also include recommendations for due diligence best practices and a summary of the consequences for violating US sanctions, demonstrate that enforcement of US sanctions against North Korea are a priority for OFAC and the Trump Administration.

For additional details, refer to our Client Alert: Trump Administration Imposes Broad New Sanctions Against North Korea and Client Alert: President Expected to Sign New Sanctions Bill to Constrain Presidential Authority While Expanding "Sanctions Toolkit" for Russia, Iran, and North Korea.

Looking Ahead

While OFAC continues to implement existing sanctions authorities, the President's messaging after the July 2018 summit with North Korea sends a mixed signal to US and non-US companies alike. South Korea is reportedly considering lifting its trade embargo on North Korea,[139] as elements within the South Korean government favor trade liberalization between the two countries. And China has largely ignored or resisted efforts by the Trump Administration to discourage its commercial and financial relationship with North Korea. These and other related geopolitical considerations may complicate the use of US secondary sanctions authorities and may also, eventually, force the United States to adopt a more permissive posture vis-à-vis North Korea.

E. Sudan

On June 29, 2018, OFAC formally terminated the Sudanese Sanctions Regulations, though sanctions remain against individuals and entities in Darfur and South Sudan.[140] Certain US export restrictions remain in place, so banks and other US companies should continue to proceed cautiously when considering transactions involving Sudan.

F. Venezuela

The United States has continued to expand sanctions on Venezuela in response to the escalating political and humanitarian crisis there. On August 24, 2017, President Trump issued E.O. 13808 to expand US sanctions against the Government of Venezuela and state-owned oil company Petroleos de Venezuela S.A. (PdVSA).[141] The United States has further expanded sanctions on Venezuela several times since then. These measures primarily target the Venezuelan government's access to capital markets and ability to engage in corrupt practices, and have created a challenging compliance environment for investment banks, custodial banks, broker-dealers and other financial services firms.

E.O. 13808 includes prohibitions on all transactions related to dealings in "new" debt of PdVSA with a maturity of greater than 90 days, and with the Government of Venezuela (other than PdVSA) in "new" debt with a maturity of greater than 30 days or new equity.[142] Dealings in any new debt beyond the applicable tenor are prohibited under the

sanctions.[143] However, OFAC also issued four general licenses accompanying the sanctions. The general licenses authorize transactions related to certain previously issued bonds, transactions dealing with only CITGO Holding Inc. and its subsidiaries, and transactions related to the export or reexport of certain agricultural commodities, medicine, medical devices and replacement parts.

In March 2018, President Trump issued E.O. 13835, which prohibits certain transactions involving the collateralization of debt owned by the Government of Venezuela. Specifically, it prohibits all transactions by a US person or occurring within the United States related to the purchase of any debt owed to the Government of Venezuela, including accounts receivable; any debt owed to the Government of Venezuela, including accounts receivable, that is pledged as collateral after May 21, 2018; and the sale, transfer, assignment or pledge as collateral of any equity interest in any entity of which the Government of Venezuela owns a 50 percent or greater interest, directly or indirectly.

President Trump also issued E.O. 13827 in March 2018 to impose the first US sanctions against a digital currency. The measure prohibits dealings in digital currency issued by, for or on behalf of the Government of Venezuela, including the "Petro," which had just been issued.

Then, on November 1, 2018, the President issued E.O. 13850, authorizing sanctions against persons determined to operate in Venezuela's gold sector and "in any other sector of the Venezuelan economy as may be determined by the Secretary of the Treasury, in consultation with the Secretary of State," as well as those complicit in the Venezuela government's corrupt or deceptive practices (the immediate family members of such persons will also be subject to sanctions). The sanctions are designed to target the Venezuelan government's "rampant corruption" and the ability of those who "operate corruptly" in the gold or other identified sectors to raise funds.[144]

More recently, on January 28, 2019, OFAC added PdVSA to the SDN List in an attempt to further isolate what it labeled a "vehicle for corruption" and the "primary source of Venezuela's income and foreign currency." The dramatic escalation of sanctions, which followed Venezuelan opposition leader Juan Guaidó's declaration as interim president of Venezuela and US recognition of his legitimacy, was accompanied by a series of general licenses intended to relieve some of the burden on US companies that had existing interests in Venezuela, as well as on US financial services firms, investors and others who had been dealing in PdVSA-linked securities. Secretary Mnuchin stated that sanctions relief for PdVSA will occur "through the expeditious transfer of control to the Interim President or a subsequent, democratically elected government."[145] Until that time, US persons with interests in Venezuela or who deal in PdVSA-linked securities must ensure that they can meet the requirements of the general licenses, which have been revised and reissued several times already since January 28.

In another significant move, OFAC designated Banco Central de Venezuela (the Central Bank of Venezuela) in April 2019, pursuant to E.O. 13850, for operating in Venezuela's financial sector of the Venezuelan economy, and it also simultaneously designated the director of Banco Central de Venezuela, Iliana Josefa Ruzza Terán. OFAC also amended existing general licenses and issued two new general licenses to allow certain transactions with Banco Central de Venezuela, including to allow US companies to wind down their contracts with the banks (expired on May 16, 2019). For additional details, refer to our Client Alert: US Sanctions PdVSA to Increase Pressure on Maduro Regime.

Looking Ahead

The Venezuela sanctions program has grown to become one of OFAC's most active sanctions programs. As the political and humanitarian crisis in Venezuela continues, we can expect OFAC to continue designating SDNs and

enforcing Venezuela-related sanctions. As President Trump has indicated, the "toughest" sanctions on Venezuela may be yet to come.[146]

G. Cyber-Related Sanctions

In 2018 and into 2019, OFAC took steps to enforce US sanctions in the digital currencies space. Notably, on November 28, 2018, the Treasury Department sanctioned two Iran-based individuals for exchanging bitcoin into Iranian rials on behalf of malicious cyber actors involved in the SamSam ransomware scheme.[147] Beyond the significance of the designations themselves, OFAC included the digital currency addresses used in the conversion by the designated Iranian individuals in their respective entries on the SDN List, marking the first time it has done so. Non-US persons engaging in certain transactions with the designated individuals—whether through traditional means or with cryptocurrency—may now be subject to secondary sanctions. OFAC concurrently issued two FAQs, adding to the growing list of OFAC FAQs pertaining to virtual currency, that clarified compliance obligations for cryptocurrency custodians.[148]

Looking Ahead

OFAC FAQs indicate that it will expect the same level and manner of compliance for transactions involving digital currencies as for traditional fiat currencies. However, while the FAQs have clarified some important questions about how persons subject to US jurisdiction can implement their existing obligations with respect to blocked property, a number of important questions remain outstanding (e.g., how to implement compliance obligations under jurisdictional sanctions programs, and how to link digital currency addresses with real-world identities), which will continue to complicate compliance.

H. Nicaragua

In response to Nicaragua's state-sponsored violence against protestors in 2018, President Trump issued E.O. 13851, "Blocking Property of Certain Persons Contributing to the Situation in Nicaragua," on November 27, 2018, which authorizes blocking sanctions on persons determined to be responsible for or complicit in serious human rights abuses in Nicaragua or actions that undermine Nicaragua's democratic process or threaten its peace, security, or stability, and persons engaging in deceptive practices on behalf of the Nicaraguan government.[149] E.O. 13851 also authorizes the Secretary of the Treasury, in consultation with the Secretary of State, to sanction anyone (including current officials) who has served as a public official in Nicaragua since January 10, 2007. OFAC concurrently added Nicaragua's vice president and national security advisor—two of Nicaraguan president Daniel Ortega's closest associates—to the SDN List. On April 17, 2019, OFAC also designated several additional individuals, including Laureano Ortega Murillo, the son of President Ortega.[150] As a result, all persons subject to US jurisdiction are prohibited from dealing with these individuals.

Looking Ahead

This is a new sanctions program, and it is another example of sanctions focused on grave human rights abuses. The events in Nicaragua should be watched closely because the program could expand in the absence of political reforms or in response to additional instances of antidemocratic activity by the Nicaraguan government.

I. Global Magnitsky Sanctions

In December 2017, President Trump issued E.O. 13818 to implement 2016's Global Magnitsky Human Rights Accountability Act authorizing the President to impose sanctions against human rights abusers and those who facilitate government corruption.[151] The new Global Magnitsky sanctions target corruption by current and former government officials anywhere in the world, whereas previously sanctions related to government corruption targeted only such conduct in a limited set of countries. This means that companies must consider human rights and anti-corruption compliance risks more expansively than ever before, as OFAC now has the authority to impose sanctions that reach commercial and financial relationships in every jurisdiction based on the conduct of foreign government officials.

OFAC designated dozens of individuals and entities under this authority during 2018. These include 17 individuals from Saudi Arabia who played a role in the killing of Saudi journalist Jamal Khashoggi.[152] OFAC designated these individuals approximately a month after a bipartisan group of US senators wrote a letter to President Trump calling for an investigation of the matter.[153] OFAC also designated Turkey's Minister of Justice and Minister of Interior pursuant to E.O. 13818 in response to Turkey's detention of Pastor Andrew Brunson,[154] but "de-listed" the officials[155] after Brunson's release.

Looking Ahead

OFAC will likely continue to use Global Magnitsky designations as an important foreign policy tool. We also expect that Congress will continue to play an active role in human rights–based sanctions, including, potentially, additional sanctions against the Kingdom of Saudi Arabia. In particular, the Trump Administration's defiance of Congress's request to investigate and report back on the Khashoggi assassination pursuant to the Global Magnitsky Act may lead to additional congressional action.

For additional details, refer to our Client Alert: Global Magnitsky Sanctions Target Human Rights Abusers and Government Corruption Around the World.

J. Virtual Currency

On March 19, 2018, OFAC issued guidance in the form of FAQs regarding the application of economic sanctions laws to virtual currency. These FAQs were released contemporaneously with E.O. 13827, which was issued by President Trump to prohibit US persons from transacting with virtual currency, including the newly issued Petro, issued by, for or on behalf of the Government of Venezuela.[156] OFAC's FAQs similarly described how existing sanctions compliance obligations apply to cryptocurrency. In subsequent guidance published in November 2018, OFAC further clarified how virtual currency custodians subject to US jurisdiction can implement their obligations to block cryptocurrency in which sanctioned persons have an interest.[157] At the same time, on November 28, OFAC added virtual currency addresses to the identifying information it published for two Iranian hackers subject to sanctions under the cybersecurity sanctions program.[158] This was the first time OFAC did so, and the inclusion of the sanctioned persons' virtual currency addresses will help companies implement their sanctions compliance obligations with respect to cryptocurrency.

IV. Enforcement

The Trump Administration has focused on enforcement of AML and sanctions cases, with various agencies seeking to increase both the number of actions and the size of the penalties. In **AML enforcement**, cases have successfully obtained larger and more expansive relief, some of which included *significant corporate fines* (including a single

penalty of $528 million for US Bank), *heightened individual penalties* (including six-figure fines and industry bans), *culpability for acts by foreign affiliates* (Deutsche Bank), the *unwinding of US operations* (Habib Bank) and *guilty pleas* for impeding an investigation (Rabobank). Similarly, OFAC has expanded **sanctions enforcement** in several interesting ways, including larger *volume and penalties*, obtaining 18 penalties or settlements cases in the first half of 2019 totaling nearly $1.3 billion. OFAC's primary focus on Iran has expanded to include actions involving Cuba, Ukraine and Syria. OFAC has also imposed a number of penalties on nonfinancial services companies, such as oil and gas, telecommunications, industrial tools, healthcare, retail, automotive, and international logistics. Recently published enforcement guidelines and public statements that accompanied OFAC enforcement actions provide much more detailed factual findings for the industry to use to improve compliance practices. The large numbers of fines and enforcement actions demonstrate the increased financial (and other) risk that institutions face in AML and sanctions actions, as well as the Administration's commitment to remaining active in this space.

A. AML Enforcement

AML enforcement continues to be a priority for regulators, with financial institutions of many types and sizes facing scrutiny from a number of federal agencies and state regulators. Regulators have brought notable public actions against individuals, some of the nation's largest banks, a significant broker-dealer, a large MSB and other firms. The substantive allegations brought against financial institutions vary widely, and include willful failures to maintain an AML program, violations of past cease and desist orders, and stiff penalties for historical conduct. And a wide group of US regulators, including the OCC, the Fed, the FDIC, FinCEN, the SEC, FINRA and NYDFS, in addition to the DOJ, continue to pursue AML violations. Financial institutions may be—and recently have been—forced to defend against parallel actions from multiple regulators. Below we discuss several trends and developments observed in the Trump Administration.

- Individual liability for compliance officers is increasing, with hefty financial and career impacts. The first-ever civil suit against a compliance officer resulted in a $250,000 fine and a three-year employment injunction (MoneyGram);[159] the DOJ entered into a deferred prosecution agreement (DPA) with an individual for allegedly "aiding and abetting" the company's illegal actions (Rabobank);[160] an executive received a six-month suspension and a $20,000 fine (C.L. King & Associates Inc.);[161] and a branch manager received a two-month suspension and a $5,000 fine (Revere Securities LLC).[162]
- Recent enforcement actions underscore that regulators and law enforcement closely scrutinize financial institutions' conduct during examinations. For example, Rabobank pled guilty to a felony conspiracy charge for impeding an OCC investigation and concealing deficiencies in its AML program.
- In addition to the continued enforcement focus on the US operations of foreign banks, the Trump Administration's recent enforcement actions highlight that banks should carefully consider the totality of available information about their customers, and that potential AML issues lurk in foreign affiliates. Furthermore, the year's actions emphasize risks in connection with foreign correspondent banking and US dollar clearing.
- The NYDFS continues to be an aggressive enforcer in the AML space. Most notably, a NYDFS enforcement action led Habib Bank to unwind its New York operations. Substantively, the NYDFS focused on transaction monitoring, a trend that is likely to continue as Part 504 obligations take effect.

- MSBs continue to be a major risk area. In addition to the Western Union enforcement action, FinCEN took its first action against a foreign-located cryptocurrency exchange, BTC-e, in 2017. And Merchants Bank of California faced enforcement actions for AML failures in connection with MSB clients.
- Regulator-imposed monitorships remain a key feature of the AML remedial toolkit, with Deutsche Bank AG and Western Union (along with ZTE Corporation in the sanctions and export controls space) each receiving monitorships in connection with their recent enforcement actions. However, the imposition of monitorships is not the outcome for all AML enforcement actions. In 2017 and 2018, US Bank, Rabobank, Citibank and Mega Bank were all subject to significant enforcement actions that did not require a monitor.
- AML enforcement continued in the securities industry. The SEC and FINRA remain focused on AML issues, especially in microcap trading, continuing the trend from the past few years.

1. Continuing Risks of Individual Liability for Compliance Officers

The Trump Administration has continued to bring high-profile actions against individuals for BSA compliance failures. Perhaps most notable was the first-ever civil suit settlement for an AML program violation, reached by the government in May 2017 against an individual compliance officer. FinCEN and the US Attorney's Office for the Southern District of New York alleged **Thomas Haider**, former chief compliance officer for MoneyGram International Inc., had violated the BSA, which resulted in stiff penalties. As part of that settlement, Haider agreed to a three-year injunction barring him from performing a compliance function for any money transmitter and to pay $250,000 (less than the $1 million FinCEN sought in its complaint, but still the largest amount sought by FinCEN against an individual).[163] The settlement followed on MoneyGram's November 2012 DPA with the DOJ, in which MoneyGram agreed to forfeit $100 million and admitted to willfully failing to maintain an effective AML program in violation of 31 U.S.C. § 5318(h).

The *Haider* case signals two important shifts in enforcement against individuals. First, the settlement delineates examples of what actions, or failures to act, the government views as particularly egregious. For example, the government required Haider to accept responsibility for failing to (i) direct the termination of MoneyGram outlets that were involved in fraud schemes; (ii) establish a policy for terminating outlets that presented a high risk of fraud; and (iii) structure MoneyGram's AML program to properly use information from the Fraud Department to file SARs. Second, *Haider* signals important implications for other individuals in the financial industry with compliance responsibilities, including the tension between entity and individual liability under the BSA. In this case, Haider had argued that he could not be held liable under § 5318(h) of the BSA, because that section's requirement to establish an AML program applies only to financial institutions, rather than individuals.[164] The district court rejected that argument, holding that FinCEN could proceed under the BSA's general civil penalty provision in § 5321(a), which permits FinCEN to assess civil penalties against a "partner, director, officer, or employee" of a financial institution for willful violations of the BSA. The court's analysis of this issue was not detailed, and its reasoning—which arguably expanded the substantive requirements of the BSA based on the civil penalty provision—was not free from doubt. This was likely to have been a significant issue on appeal, but the settlement means that the issue will have to be decided in a future case.

In addition to the *Haider* settlement, there were a number of other regulatory actions involving individual liability under the BSA. For example, former **Rabobank** AML monitoring and investigations manager George Martin entered into a DPA with the DOJ for "aiding and abetting" Rabobank's AML violations.[165]

Regulators continue to pursue actions against individuals employed at institutions recently subject to enforcement actions, as illustrated by the above actions. The OCC took a similar tack in the wake of the Merchants Bank and Gibraltar enforcement actions from 2017 and 2016, respectively.

- The OCC pursued actions against several **Merchants Bank** directors and officers for "reckless unsafe or unsound practices," breach of fiduciary duties, and violations of "regulations and orders" under 12 U.S.C. § 1813(v): Daniel Roberts, former chairman of the board, president and CEO ($175,000 fine); Rodrigo Garza, former executive vice president and director ($70,000 fine); and Jane Chu, former executive vice president and CFO ($35,000 fine). The OCC also pursued actions against three other individuals for § 1813(v) violations only: Philip Scot, chairman of the board ($20,000 fine); Susan Cavano, chief banking officer and former COO ($5,000 fine); and Janice Hall, former director ($5,000 fine).[166] The actions stemmed from the failure of Merchants' directors to abide by the terms of OCC consent orders entered into in 2010 and 2014.
- The OCC pursued actions against officers of **Gibraltar Private Bank and Trust Co.** for "reckless unsafe or unsound practices": William VanDresser, former executive vice president and managing director of wealth management ($35,000 fine), and Elden LeGaux, former senior vice president and director of wealth management operations ($15,000 fine).[167] Both VanDresser and LeGaux were involved in a recommendation that Gibraltar's BSA committee open wealth-management accounts for a new client who the officers knew, or should have known, had family ties to a high-risk client that the committee had previously declined for compliance reasons. The OCC also pursued an action against Charles Sanders, the chief compliance and risk officer ($2,500 fine), for failing to file SARs on a set of accounts for a client later convicted for his role in a Ponzi scheme.[168]

OCC also fined **Dirceu Magalhaes**, former private banking senior manager at the Miami Federal Branch of the **Royal Bank of Canada**, $100,000 for failing to file SARs, in violation of 31 U.S.C. § 5318(g) and 12 C.F.R. § 21.11.[169] In 2013, he had facilitated Brazil-US transactions, through an informal network, for clients and others, evading record-keeping and compliance restrictions on such transactions. He gained approximately $15,000 from his work facilitating the transactions and took steps to conceal his involvement from his employer.

In addition, a September 2017 FINRA hearing panel found that broker-dealer **C.L. King & Associates Inc.** and its AML compliance officer, **Gregg Alan Miller**, had failed to implement an AML program reasonably designed to monitor risks associated with the liquidation of billions of shares of penny stocks by two of its customers, in violation of NASD Rule 3011(a) and FINRA Rules 3310(a) and 2010. The FINRA panel pointed out that both Miller and the firm had little experience with penny stocks and, as a result, "they did not adopt an AML program that would reasonably ensure that they even understood what red flags to look for."[170] Miller was suspended in a principal capacity for six months and fined $20,000.

Finally, another FINRA case suggests that even branch-level officers may be held liable for AML program failures. In September 2017, **Revere Securities LLC** and **Kurt Alfred Hurst**, a branch manager for the firm, submitted to FINRA a Letter of Acceptance, Waiver and Consent in connection with the firm's alleged failure to establish and implement policies to detect and report suspicious activity involving the deposit and liquidation of millions of shares of microcap stocks, in violation of FINRA Rules 3310(a) and 2010.[171] As a result, Hurst was suspended for two months from acting in all principal capacities with any FINRA-registered firm and was fined $5,000.

a) DOJ Charges FinCEN Employee With Unlawful Disclosure of SARs

The US Attorney's Office for the Southern District of New York (SDNY) recently charged a former FinCEN employee with leaking SARs to a member of the media. The case is a sharp reminder to financial institutions, and their employees and agents, of the importance of SAR confidentiality, and serves as a useful opportunity for all institutions that file SARs to review their SAR confidentiality programs for consistency with federal law and FinCEN guidance.

SDNY Case Summary

On October 17, 2018, SDNY charged Natalie Mayflower Sours Edwards with unauthorized disclosure of SARs and conspiracy to make unauthorized disclosure of SARs. According to the complaint, a press release and surrounding news reports, Edwards disclosed "numerous" SARs to a BuzzFeed News reporter, who published the content of those SARs in a number of articles.[172] The SARs in question pertained to, among other things, Paul Manafort, Richard Gates, the Russian Embassy, Maria Butina and Prevezon Alexander. Edwards saved the SARs—and a number of other sensitive government documents, including FinCEN internal emails, nonpublic memoranda and intelligence assessments—to a flash drive and transmitted them to the reporter.

Background and Legal Authority

SARs are a key law enforcement tool in detecting, preventing and prosecuting money laundering, terrorist financing and other illegal activity. The BSA requires a financial institution to file a SAR with FinCEN when that financial institution detects a known or suspected violation of federal law or a suspicious transaction related to money laundering, terrorist financing or a violation of the BSA.[173] The purpose of a SAR is to assist law enforcement in fighting crime, so SARs and information that might reveal the existence of a SAR are subject to strict confidentiality rules so as not to tip off criminals.

Financial institutions and their current and former directors, officers, employees, agents and contractors are prohibited from disclosing SARs, or any information that would reveal the existence of a SAR, except in very limited circumstances.[174] Material that could reveal the existence of a SAR can include email correspondence and verbal disclosures, as well as any acknowledgement that a SAR exists. FinCEN takes the position that documents stating that a SAR has not been filed should also be kept confidential.

As the recent SDNY case makes clear, the unauthorized disclosure of a SAR is a violation of federal law. Financial institutions and their current and former directors, officers, employees, agents and contractors could be subject to civil and criminal penalties for the unauthorized disclosure of a SAR.[175] There can be criminal penalties of up to $250,000 and/or imprisonment not to exceed five years, and civil penalties of up to $100,000 for each violation.[176]

Financial institutions could also be liable for civil money penalties resulting from AML program deficiencies (internal controls, training, etc.) that led to the SAR disclosure. Such penalties could be up to $25,000 per day for each day the violation continues.[177]

Importance of SAR Confidentiality Program

Although the alleged conduct in the SDNY case was especially egregious, particularly because the suspect in question was an employee of the US government, the case underscores how seriously FinCEN and the DOJ take SAR confidentiality. Financial institutions—and all SAR filers—should carefully review their SAR confidentiality programs.

FinCEN most saliently reminded financial institutions of their SAR confidentiality obligations in a 2012 advisory.[178] That advisory underscored the importance of training staff on SAR handling and confidentiality. While each institution's SAR confidentiality program may be slightly different, FinCEN highlighted a number of risk-based measures financial institutions could consider implementing to enhance SAR confidentiality, such as

- limiting access on a "need to know" basis;
- restricting areas for reviewing SARs;
- logging access to SARs;
- using cover sheets for SARs or information that reveals the existence of a SAR; or
- providing electronic notices that highlight confidentiality concerns before a person may access or disseminate the information.[179]

Financial institutions should consider these measures anew in light of the facts of the recent case. The advisory also directs institutions that become aware of unauthorized disclosure of a SAR to immediately contact FinCEN's Office of Chief Counsel, and consider whether they are also required to contact their federal regulator, as prescribed by the applicable SAR rule. Financial institutions should consider developing a SAR disclosure response plan that includes these measures and, in certain circumstances, conferring with outside counsel.

SARs in Civil Litigation

In addition to broad advice about maintaining an effective SAR program, FinCEN has provided more specific guidance to financial institutions about how to handle certain situations that may arise in dealing with SARs. For example, FinCEN has provided guidance to financial institutions about how to approach a civil subpoena that seeks production of a SAR.[180] If the subpoena does not specifically seek production of a SAR, the recipient should object on the basis that some responsive material contains confidential supervisory information.[181] If the subpoena specifically seeks a SAR, the financial institution is to send the issuer of the subpoena a written objection pointing out the SAR confidentiality regulations.[182] Financial institutions should also be mindful not to reveal the existence of a SAR during the course of the litigation; in pleadings or a privilege log, for example, FinCEN directs financial institutions to generically refer to "nonpublic supervisory information" or something similar.[183]

2. Federal Court Rules on SAR Filing Case

On December 11, 2018, the SEC won partial summary judgment in an enforcement suit against clearing broker Alpine Securities Corporation in the Southern District of New York.[184] The SEC alleged that Alpine had violated Rule 17a-8,[185] which obligates broker-dealers to comply with regulations promulgated under the BSA. Specifically, it claimed that Alpine had committed thousands of violations by failing to file complete SARs when required to do so.[186] The detailed, 100-page opinion authored by Judge Denise Cote provides a rare glimpse into a court's analysis of a financial institution's SARs filing, or lack thereof.

Judge Cote first held that the SEC has independent authority to require broker-dealers to file SARs, as well as enforcement authority over those reporting obligations.[187] Alpine also contended that the SEC could not bring claims that rely on guidance from FinCEN because such guidance contained mere suggestions, as opposed to rules of law. Judge Cote acknowledged that "while FinCEN guidance is informative and useful, its role in this action can be overstated." She held instead that Alpine's violations arose from its failure to comply with Section 1023.320, the regulation that dictates when SARs must be filed,[188] and the SAR Form instructions, which "have the force of law, having been issued as FinCEN regulations following a notice and comment period."[189] But the court then explained

that the FinCEN guidance cited by the SEC "give[s] content to a broker-dealer's obligation to file SARs." And throughout the rest of the opinion, Judge Cote used FinCEN guidance in explaining Alpine's missteps.

At its core, the opinion stands for the proposition that financial institutions should ensure they digest the government's instructions in connection with SAR filing obligations, especially with respect to identified potential red flags for suspicious activity and ensuring that SAR narratives are complete.

SEC's Claims and Standard of Review

The SEC ultimately alleged four categories of Alpine's SARs (or lack thereof) that violated the regulations: (1) SARs with deficient narrative explanations, (2) failure to file certain SARs, (3) late-filed SARs and (4) failure to maintain proper supporting files. To win summary judgment, the SEC was required to demonstrate that no question of fact existed as to these violations on Alpine's part—the court denied summary judgment for specific reports as to which Alpine raised a question of fact or on which the SEC's "presentation [was] deficient."[190] In effect, the SEC was saying that Alpine was required to file these SARs as a matter of law. However, the court explained that Alpine's failures overall were "stark," and elaborated that "[g]iven the sheer number of lapses at issue in this case, there is no basis to conclude that a broker-dealer that reasonably attempts to follow the requirements of Section 1023.320 will be at risk."[191]

SAR Filing Obligations

As a preliminary matter, the court explained that Alpine's duty to file a SAR is triggered when a transaction involves (i) a large deposit of low-priced securities (LPS) and (ii) either the presence of one of six red flags or the involvement of a certain customer.[192] Once the duty is triggered, the broker is required to include a "clear, complete and chronological narrative" in the SAR.[193] The court gave an overview of the more than 1,500 transactions that the SEC alleged had deficient narratives, based on the six red flags outlined below. Alpine's failure to include and sufficiently describe these categories of information resulted in deficient narratives for many transactions. The six red flags were "derived from the SAR Form and its instructions, as well as FinCEN and other guidance interpreting Section 1023.320."[194]

In addition, the court found, another 295 SAR narratives omitted basic customer information, identified in FinCEN's SAR Narrative Guidance as the essential elements: who, what, when, where, why and how. [195] These elements can and often do encompass information that, if omitted, raises one of the six red flags. Here, the Court agreed that many SARs failed to include basic customer information, but it did not grant summary judgment on SARs that did not include a statement that Alpine considered the transaction suspicious, as these were not clearly required filings.[196] In other words, the court held that if a financial institution considers a transaction suspicious, then the SAR is mandatory, not voluntary.

As a specific matter, the case should encourage financial institutions to incorporate into their transaction monitoring and SAR investigative units the capacity to identify such red flags in connection with LPS (identified below). As a general matter, and more importantly, the opinion should cause all financial institutions to go back to basics and review closely FinCEN documents—especially FinCEN's SAR Form, SAR Instructions and SAR Narrative Guidance; various issues of the SAR Activity Review; and FinCEN's myriad guidance documents—to ensure the entity is adhering to FinCEN's prescriptions about SAR content and completeness and identifying appropriate red flags.

Continued Monitoring

The court addressed the second category of claims next: SARs on which Alpine reported a large deposit of LPS but did not subsequently file SARs reflecting the sales following those deposits.[197] The SEC won summary judgment that Alpine violated the law by failing to file these SARs, but the court held that a decision on the question of how many SARs should have been filed would require a fact-intensive inquiry.[198] Although the court's reasoning was limited to the relatively narrow factual situation of large LPS deposits followed by LPS sales, financial institutions should use this as an opportunity to consider their procedures around continuing to monitor customers about which they have previously filed SARs, especially with respect to whether a continuing activity SAR may be warranted.

Late-Filed SARs

The court denied summary judgment to the SEC on late-filed SARs. The SEC had failed to establish that Alpine was obligated to file the 251 reports that were filed over six months after the date of initial detection.[199] The case underscores that regulators are focused on ensuring the timely filing of SARs.

Inadequate Support Files

Finally, the SEC won summary judgment on the nearly 500 SARs for which Alpine had maintained inadequate support files.[200] Alpine was unable to locate any supporting material for a number of SARs and provided no evidence to the contrary.[201] Most notably, the court held that a SAR narrative is deficient if it omits evidence of red flags present in SAR support files.[202] This indicates that filers should be cautious not only to maintain fulsome supporting files but also to ensure that the SAR narratives based on those files adequately reflect all red flags present in the files.

LPS Red Flags

As noted above, a financial institution's duty to file a SAR is triggered when a transaction involves (i) a large deposit of LPS and (ii) the presence of one of six red flags (related litigation, shell companies or derogatory history, stock promotion, unverified issuers, low trading volume, or foreign involvement). Going forward, all financial institutions that handle LPS should ensure they are able to adequately monitor for such red flags.

3. Banking Cases

a) Department of Justice Continues to Prioritize AML Cases

In February 2018, **Rabobank** pled guilty to a felony conspiracy charge brought by the DOJ for concealing deficiencies in its AML program during an OCC examination in 2012. In pleading guilty, Rabobank admitted to unlawfully impeding the OCC's ability to regulate and examine the bank's operations.[203] Additionally, the DOJ found that Rabobank's AML program deficiencies allowed hundreds of millions of dollars in "untraceable cash" from Mexico and elsewhere to be deposited at the bank and transferred without required notification to the government. Rabobank's policies and procedures were inadequate to cause investigation of these transactions, many of which occurred in branches near the Mexican border in California. Rabobank will forfeit nearly $369 million as a result of this action, which underscores the importance of forthrightness in interactions with regulators. In addition to the DOJ action, the OCC entered into a consent order with Rabobank for civil money penalties of $50 million, which will be credited toward the fine determined by the DOJ.[204] The subject of the consent order was AML and BSA deficiencies identified in a previous consent order from December 2013, which did not include a money penalty. The OCC found that since at least 2012 Rabobank failed to establish and maintain an adequate compliance program and failed to investigate potentially suspicious activity related to law enforcement subpoenas.

US Bank entered into a DPA with the SDNY, admitting criminal violations including willfully failing to maintain an effective AML program and willfully failing to file a SAR in relation to its former client Scott Tucker, who used his accounts at US Bank to launder proceeds from an illegal payday lending scheme.[205] The facts supporting US Bank's willful failure to maintain an effective AML program included maintaining caps on the number of alerts generated by a portion of its automated transaction monitoring system, in part because it did not have adequate staff to review those alerts; failing to hire additional investigators to review an adequate number of alerts; and excluding from presentations to the OCC references to resource limitations. The SDNY imposed a $528 million penalty, which was satisfied by a civil forfeiture of $453 million and payment of a $75 million civil money penalty to the OCC in connection with similar violations. The FRB and FinCEN also brought actions against US Bank, which were resolved by a $15 million civil money penalty paid to the FRB and a $185 million civil money penalty paid to FinCEN. The FinCEN action also covered separate currency transaction report violations, and $115 million of the total penalty was satisfied by US Bank's civil forfeiture.

Société Générale S.A. (SocGen) agreed to pay over $1.34 billion in penalties ($717 million in forfeiture to the DOJ, pursuant to a DPA, and penalties of $163 million to the Manhattan District Attorney's Office, $54 million to OFAC, $81 million to the Federal Reserve and $325 million to NYDFS) in connection with its failure to take sufficient steps, between 2003 and 2013, to ensure compliance with federal sanctions regulations and New York banking law.[206] Due to poor training of the relevant individuals, SocGen executed (in an improper, non-transparent manner) more than 9,000 outbound US dollar payments, valued at over $13 billion. The vast majority of the payments involved Iran; others involved Cuba, Sudan, Libya or Myanmar.

b) AML Actions by Federal Regulators

Federal regulators continued to be active in the AML enforcement space in 2017, with each of the OCC, the FRB, the FDIC and FinCEN bringing at least one significant action against a bank, with a continued focus on foreign banks. Although penalty amounts are down somewhat compared to earlier in the decade, the past year underscored that there is still significant risk for financial institutions of all sizes, and that all relevant federal regulators are committed to AML enforcement.

i) OCC

In March 2017, the OCC entered into a supervisory written agreement with **UBS** after finding UBS failed to maintain an effective BSA/AML compliance program.[207] The action emphasizes the importance of evaluating customer risk by examining the customer's whole relationship with the bank, a theme that is likely to become increasingly prominent now that the CDD Rule and NYDFS Rule 504 have been in effect for over a year. Both sets of rules highlight the importance of aggregating all available information about a client and integrating it into a holistic view of the customer's risk. If UBS's general manager or BSA officer leaves the bank, the agreement requires that replacement candidates be approved by the OCC.

In April 2018, the OCC and **Bank of China** (New York branch) entered into a consent order for a $12.5 million penalty related to the New York branch's violations of 12 C.F.R. §§ 21.11 and 21.21.[208] The OCC identified deficiencies in the branch's BSA/AML compliance programs that resulted in violations, including failures to file SARs, as well as deficiencies in the branch's compliance with OFAC.

In October 2018, the OCC assessed a $100 million civil penalty against **Capital One N.A. and Capital One Bank (USA) N.A.** for BSA/AML violations.[209] Capital One had failed to heed the terms of a 2015 OCC consent order and to timely fix the deficiencies OCC had identified in its compliance processes, which included (1) weaknesses in its compliance program and related controls; (2) deficiencies in its risk assessment, remote deposit capture, and correspondent banking processes; and (3) failure to file SARs. Capital One violated 12 C.F.R. §§ 21.11 and 21.21, subsequent to the 2015 OCC consent order, by failing to file SARs and by initiating wire transfers containing inadequate information.

ii) FRB

In May 2017, the FRB issued a $41 million penalty and cease and desist order against **Deutsche Bank AG, Deutsche Bank AG New York Branch, DB USA Corporation and Deutsche Bank Trust Company Americas** for "significant deficiencies" in Deutsche Bank's US risk management and BSA compliance that resulted in a failure to maintain an effective AML compliance program, and for deficient transaction monitoring capabilities.[210] The FRB found that Deutsche Bank's transaction monitoring deficiencies meant the bank could not properly assess AML risks for "billions of dollars in potentially suspicious transactions" processed for Deutsche Bank European affiliates, which themselves "failed to prove sufficiently accurate and complete information."[211] The action underscores the risk that lies in US dollar clearing and correspondent banking operations and, in particular, that AML compliance obligations are not diminished when the direct customer is a financial institution's own overseas affiliate. In addition to the civil money penalty, the order requires Deutsche Bank to submit and implement plans to improve compliance and reporting and hire independent third parties to (i) review Deutsche Bank's compliance program and (ii) conduct a look-back review of certain correspondent banking transactions.

In January 2018, the FRB issued a $29 million penalty against **Mega International Commercial Bank and its branches in New York, Chicago and Silicon Valley** for its deficient AML oversight and controls.[212] The cease and desist order addressed deficiencies in those branches, each of which was required to submit a written BSA/AML compliance program, a revised program for conducting customer due diligence, and an enhanced written program to ensure the identification and timely, accurate and complete reporting of all known or suspected violations of the law. In addition, the New York branch was required to engage an independent third party to conduct a look-back review of six months of past dollar clearing transaction activity to determine if suspicious activity was properly identified and reported. The New York branch was previously fined $180 million by the NYDFS in August 2016 and required to install an independent compliance monitor for violating New York's AML laws. It is also notable that the Illinois Department of Financial and Professional Regulation was also party to this action; this could presage stepped-up enforcement on the state level for jurisdictions in addition to New York, particularly as to branches of foreign banks.

Consistent with the federal enforcement approach, the North Carolina Office of the Commissioner of Banks was also involved in the FRB's January 2017 action against **BB&T Corporation**.[213] The consent order required the bank to address "significant deficiencies" in its AML compliance program. The agreement also required BB&T to submit a written plan for improvement of its compliance risk management program and to provide quarterly updates.

In March 2018, the Federal Reserve issued an enforcement action against the **Industrial and Commercial Bank of China and its New York branch (ICBC)** for failing to comply with federal and state laws relating to AML compliance, including the BSA, and the requirements of Regulation K to report suspicious activity and maintain an adequate BSA/AML compliance program. While this action set forth several requirements, no money penalties were

attached.[214] ICBC is required to submit a written plan to enhance oversight and compliance with BSA/AML requirements, customer due diligence, OFAC requirements, and SAR monitoring and reporting within 60 days of the order. Consistent with a key feature of recent FRB actions, ICBC is required to engage an independent third party to conduct a look-back review of a six-month period of the New York branch's US dollar clearing transactions.

Finally, in 2018, FRB reached agreements with the New York branches of **Hua Nan Commercial Bank Ltd. (Taiwan)** and **United Bank Limited (Pakistan)**, concluding FRB/NYDFS investigations that had identified significant deficiencies in each institution's risk management and BSA/AML compliance, including the regulations promulgated under the BSA (31 C.F.R. Chapter X) and the requirements of Regulation K. Each institution agreed to work with the FRB to devise a written plan to increase management oversight of BSA/AML compliance and to create a written plan for a comprehensive overhaul of its BSA/AML compliance program within 60 days of the agreement.

iii) FinCEN

In October 2017, FinCEN assessed a $2 million civil money penalty against **Lone Star National Bank** for willfully violating the BSA, highlighting that "[s]maller banks, just like the bigger ones, need to fully understand and follow . . . diligence requirements if they open up accounts for foreign banks."[215] FinCEN found that from 2010 until 2014, Lone Star failed to establish an AML program, conduct required due diligence on a foreign correspondent account, and report suspicious activity. In just two years, such failures allowed an FFI to introduce hundreds of millions of dollars in bulk cash shipments into the US financial system. Lone Star also had an inadequate system of monitoring and reporting suspicious activity, resulting in failure to file 173 SARs. Many of these deficiencies were highlighted in a March 2015 OCC consent order. FinCEN acknowledged the OCC action but noted it considered the penalties specifically applicable under FinCEN's Section 312 authority to require special due diligence for foreign correspondent accounts. FinCEN's penalty was partially satisfied by Lone Star's previous $1 million OCC fine; it also recognized Lone Star for the considerable resources it expended to promote compliance, noting Lone Star was no longer engaging in the "correspondent banking activities for which it was ill prepared."[216]

In February 2017, FinCEN assessed a $7 million civil penalty against **Merchants Bank of California,** a California-based community bank, for failing to establish an adequate AML compliance program, conduct due diligence on foreign correspondent accounts, and detect and report suspicious activity.[217] The bank provided banking services to MSBs, including check-cashers and money transmitters. FinCEN concluded that the bank did not adequately assess the money laundering risks presented by servicing the MSBs, and that the bank's leadership impeded the investigation and reporting of suspicious activity by threatening employees who attempted to report suspicious transactions in accounts affiliated with bank executives. In addition to FinCEN's order, the OCC imposed a $1 million penalty for AML compliance failures that led to violations of previous OCC consent orders.

iv) FDIC

The FDIC entered into a June 2017 consent order with **Shinhan Bank America**, an insured state bank in New York, requiring the bank to improve its BSA/AML compliance program.[218] The order did not allege specific violations, and the bank did not admit to or deny any charges. Among other things, the order required Shinhan's board to increase supervision and direction of the bank's BSA/AML compliance program, form a BSA/AML compliance committee, retain qualified management to oversee the program, and conduct a look-back review of transactions from December 1, 2015, through the date of the order.

c) The NYDFS Continues to Impose Substantial AML Penalties

The NYDFS has brought six significant enforcement actions since the start of 2017, totaling over $850 million in penalties. These actions highlight NYDFS's aggressive posture toward bringing AML enforcement actions, particularly against the US operations of foreign banks.

Most prominently, in September 2017, the NYDFS fined **Habib Bank** and its New York branch $225 million and ordered the bank to wind down its New York operations.[219] The order follows a series of prior compliance violations that resulted in a 2006 written agreement and a 2015 consent order. In connection with the most recent action, the NYDFS found that Habib Bank facilitated billions of dollars in transactions with Al Rajihi Bank—a large private Saudi bank with reported ties to al-Qaeda—without adequate AML and CFT controls or adequate customer due diligence. In addition, Habib Bank permitted to flow through New York at least 13,000 transactions that potentially omitted information necessary to screen for transactions with sanctioned countries. The bank also improperly used a "good guy" list—a list of customers who supposedly presented a low risk of illicit transactions—to allow at least $250 million in transactions to occur without any screening, including dealings by an identified terrorist, an international arms dealer and an Iranian oil tanker. It appears that customers were added to the good guy list in spite of indicia of financial crime risk. The NYDFS's investigation also found multiple instances where alerts generated by the branch's transaction monitoring system were improperly cleared. Although the facts in this matter were particularly egregious, the action makes clear that the NYDFS will continue to be an active enforcer and will, at times, even force the closure of a financial institution. One broader lesson is that financial institutions should scrutinize their use of "good guy" lists and install proper controls to ensure that careful consideration is given to any additions to such lists. Financial institutions should also take from this action that even "low risk" customers deserve some level of financial crime scrutiny.

As described above, **SocGen** agreed to pay over $1.34 billion in penalties, including $325 million to the NYDFS, in connection with regulatory violations that occurred between 2003 and 2013. NYDFS's investigation disclosed that SocGen had fundamental deficiencies in its policies and procedures governing SARs and flaws in its customer due diligence protocols. SocGen was found to have failed to maintain an effective and compliant AML program, in violation of 3 N.Y.C.R.R. § 116.2 and New York Banking Law § 200-c, and to have violated provisions of a 2009 agreement with the NYDFS to implement and maintain an effective BSA/AML compliance program and transaction monitoring system.

The NYDFS, which licenses and regulates money transmitters in New York, also brought an action and imposed a $60 million penalty against **Western Union** in January 2018 for failure to implement and maintain an effective AML compliance program between 2004 and 2012.[220] The NYDFS specifically cited illegal conduct by Western Union agents in connection with transactions to China. In considering the appropriate remedy, the NYDFS credited Western Union for its "significant remedial measures" and "substantial contributions to" and "cooperation with" law enforcement. It appears that the action relates to the conduct at issue in the federal action identified below.

In October 2018, despite strong cooperation with the NYDFS, the New York branch of **Mashreqbank PSC** was fined $40 million for identified deficiencies in the branch's BSA/AML program and in its OFAC compliance program and for violations of 3 N.Y.C.R.R. § 116.2 and New York Banking Law § 200-c. Mashreqbank, the oldest and largest private bank in the United Arab Emirates, cleared more than a million US dollar transactions from its New York branch in both 2016 and 2017, with an aggregate value of over $367 billion (2016) and $350 billion (2017). Many of the branch's clients are located in Southeast Asia, North Africa or the Middle East—all regions presenting a high risk for

illicit financial transactions and BSA/AML violations. The NYDFS found that the branch's BSA/AML and OFAC policies lacked detail, nuance or complexity, doing little more than citing standard language from applicable regulations. Further, transaction monitoring alerts were reviewed only once, by a single reviewer, who would then determine whether the alert should be closed or escalated, without adequate quality assurance reviews.

In January 2017, the NYDFS entered a consent order with **Deutsche Bank** in connection with the Russian "mirror trading" scheme.[221] The scheme reportedly allowed roughly $10 billion to be moved out of Russia, and it went undetected in the bank's Moscow, London and New York offices. According to the NYDFS, the scheme involved closely related parties making a series of offsetting stock trades that lacked economic purpose. Deutsche Bank cooperated with the investigation and agreed to pay $425 million in fines and hire an independent monitor for a two-year term. The NYDFS coordinated its investigation with the UK Financial Conduct Authority, which in parallel assessed a penalty equivalent to approximately $210 million.

The NYDFS entered into a November 2017 consent order with **NongHyup Bank** for $11 million based on a failure to maintain an effective AML program. Specifically, the NYDFS found that NongHyup failed to maintain an adequate transaction monitoring system, leading to potentially suspicious activity going undetected. Notably, the consent order states that the NYDFS recognized NongHyup's cooperation in the investigations and gave this conduct positive consideration.

4. Money Services Businesses

The Trump Administration has continued to focus on AML compliance in the MSB sector.

In November 2018, **MoneyGram International Inc.** agreed to extend a 2012 DPA and forfeit $125 million due to weaknesses in its AML program, resulting in a breach of the 2012 DPA.[222]

The 2012 DPA alleged that MoneyGram violated the BSA by willfully failing to maintain an AML program and that it aided and abetted wire fraud because it knew or should have known that its money transmission systems were being used to perpetrate consumer fraud.[223] These consumer fraud scams targeted the elderly and other vulnerable groups, promising cash prizes, promising items for sale or posing as relatives in urgent need of money, and the perpetrators required victims to send funds through MoneyGram's transfer systems. The 2012 DPA required enhancements to MoneyGram's AML and anti- fraud programs.

In the 2018 action, the DOJ alleged that during the course of the DPA, MoneyGram experienced significant weaknesses in its AML and anti-fraud program, inadequately disclosed weaknesses to the government, and failed to complete all the DPA's required compliance enhancements.[224] MoneyGram's failures included, among other things, failure to implement an effective transaction monitoring system, failure to investigate or terminate agents suspected of engaging in fraud or suspicious activity, and failure to investigate or terminate locations or agents that exhibited red flags such as high levels of consumer fraud complaints. As a result of these failures, MoneyGram processed at least $125 million in fraudulent transactions between April 2015 and October 2016.

Under the terms of the extended DPA, MoneyGram agreed to block certain fraud receivers and senders within two days of a consumer fraud complaint, to require individuals worldwide to provide government-issued identification to conduct any transaction, to monitor all transfers originating in the United States in its anti-fraud program, and to terminate, discipline or restrict agents processing a high volume of transactions related to reported fraudsters.

In a related case on the same day, MoneyGram settled Federal Trade Commission (FTC) allegations of unfair or deceptive acts and practices under consumer protection laws for the same acts or omissions, which violated a 2009 consent order.[225]

In January 2017, **Western Union** agreed to forfeit $586 million and enter into agreements with the DOJ, the FTC, several US attorneys' offices and FinCEN.[226] Western Union entered into a DPA and admitted to criminal violations including willfully failing to maintain an effective AML program and aiding and abetting wire fraud. According to the DPA, Western Union's agents repeatedly facilitated consumer fraud-related transactions, but Western Union failed to file SARs identifying these agents. Western Union also acquired FEXCO, knowing that FEXCO had an ineffective AML program and had contracted with other agents who facilitated consumer fraud. Despite this, Western Union did not remedy FEXCO's AML failures or terminate the high-fraud agents. As part of the FinCEN settlement, Western Union agreed to implement stricter AML/anti-fraud policies. The FTC's order required the appointment of an independent compliance auditor to assess compliance and issue periodic reports for three years. The penalty will be used to reimburse victims of the fraud.

FinCEN took its first action against a foreign-located MSB in July 2017, fining virtual currency exchange **BTC-e** $110 million for failing to register as an MSB, failing to implement an effective AML program, failing to file SARs and violating record-keeping requirements.[227] BTC-e's operator, Alexander Vinnick, was also fined $12 million. BTC-e was a virtual currency exchange but never registered as an MSB, even after FinCEN issued guidance in March 2013 indicating that an exchanger or administrator of virtual currency is an MSB under FinCEN's regulations.[228] BTC-e lacked effective AML policies: for example, it failed to collect and verify any customer information beyond a username, password and email address, and did not mitigate risks caused by certain anonymizing features. BTC-e also lacked monitoring procedures and took no action when users openly and explicitly discussed criminal conduct through the website's internal messaging system. FinCEN alleged that BTC-e "processed thousands of suspicious transactions without ever filing a single SAR."[229] According to FinCEN, BTC-e facilitated transactions involving a host of crimes, including ransomware, hacking, identity theft, fraud, public corruption and drug trafficking. In addition to the civil fines, Vinnick was indicted for allegedly laundering more than $4 billion in funds, among other crimes, and was arrested in Greece in 2017.[230]

In addition, in April 2019 FinCEN assessed a $35,350 civil money penalty against Eric Powers for willful violation of the BSA for failure to register an MSB, having no written policies or procedures, and failing to report suspicious transactions and currency transactions.[231] Powers was operating a "peer-to-peer exchanger of convertible virtual currency." Director Blanco said that this underscores that "[o]bligations under the BSA apply to money transmitters regardless of their size" and added that FinCEN will take action in connection with its virtual currency guidance. These concerns are even sharper since FinCEN issued additional virtual currency guidance in May 2019.

5. Securities Cases

a) Department of Justice Brings BSA Charges

In the first-ever criminal charges against a broker-dealer for BSA/AML violations, the DOJ charged **Central States Capital Markets LLC** with a felony violation of the BSA for its failure to file SARs related to "historically significant pay-day lending fraud."[232] Central States was found by the DOJ to have failed to follow its own written customer identification procedures and disregarded red flags known prior to and just after opening accounts for Scott Tucker. Tucker was convicted in 2017 of racketeering, wire fraud and money laundering as part of a massive payday lending

scheme, predicated on sham relationships with certain Native American tribes to conceal his ownership of various entities and gain protection from tribal sovereign immunity. During the account-opening process, Central States became aware of Tucker's fraud conviction from 1991, later found news reports indicating potentially suspicious activity via payday loan lending schemes related to Native American tribes, and subsequently learned of an FTC action against Tucker for unfair business practices. Despite all of this, Central States still facilitated 18 wire transfers totaling over $40 million related to Tucker and his businesses.

The identified deficiencies are especially egregious with some additional context provided by the DOJ (and the SEC, which in parallel action issued a cease and desist order and censure against Central States). Specifically, not only did Central States ignore the above-mentioned red flags, but also it (a) failed to review alerts generated by its AML transaction monitoring tool, (b) failed to customize the tool away from its default parameters, and (c) failed to assess whether the monitoring tool was tuned and properly utilized to monitor transactions for its client base and anticipated transactional patterns. Beyond these failings, perhaps most significantly, Central States did not file a SAR until long after Tucker was convicted at trial in 2017, despite much earlier producing documents in connection with the DOJ's criminal investigation and despite its awareness of the indictment against Tucker.

Broker-dealers can learn critical lessons from the case. Firms must actually follow internal policies and not ignore red flags. Additionally, it is not enough merely to acquire and activate a plug-and-play AML transaction monitoring tool; broker-dealers must modify their transaction monitoring solutions commensurate with their client population and anticipated activity (that is, must tailor their solutions to their risk). Finally, broker-dealers—even after finding out about an investigation or pending indictment—must immediately follow through with the filing of a SAR of potentially suspicious activity; waiting to do so until after criminal proceedings into the underlying conduct will likely result in adverse consequences.

b) FinCEN Takes Action Against UBS

In December 2018, FinCEN[233] (in parallel with the SEC[234] and FINRA[235]) assessed a $14.5 million civil money penalty against **UBS Financial Services Inc. (UBS)** for willfully violating both BSA-mandated AML program requirements and Section 312 of the USA PATRIOT Act, requiring ongoing due diligence on correspondent accounts for FFIs. In particular, FinCEN found that from 2004 until April 2017, UBS failed to (1) develop and implement an appropriate, risk-based AML program, and (2) perform periodic reviews of its correspondent accounts for FFIs. The AML program failed to adequately address certain risks associated with accounts that offer traditional brokerage and also banking-like services (e.g., wire transfers, checks and ATM withdrawals), and failed to adequately monitor foreign currency–denominated wire transfers conducted through commodities accounts and retail brokerage accounts. In addition, UBS failed to provide its AML compliance officer with adequate resources to ensure day-to-day compliance with the BSA. Such failures inhibited UBS from identifying various red flags indicative of suspicious activity, led to backlogs of alerts and decreased UBS's ability to file SARs in a timely manner. Though UBS discovered and attempted to remediate these issues in 2012, FinCEN found such remedial efforts inadequate.

In addition to consenting to a civil monetary penalty of $5 million with FinCEN, UBS also agreed to a cease and desist order, a censure, and a $5 million civil penalty with the SEC for failure to identify certain long-term patterns of suspicious activity. This failure resulted in UBS not filing SARs on some suspicious transactions, as required by Rule 17a-8 and Section 17(a) of the Securities Exchange Act of 1934.

Finally, UBS agreed to a censure and to pay a fine of $4.5 million to its self-regulatory organization, FINRA, for failing to establish and implement (1) AML programs reasonably designed to monitor certain high-risk transactions in customer accounts (i.e., currency wires) for potentially suspicious activity, and (2) a reasonably designed due diligence program for correspondent accounts. **UBS Securities LLC (UBSS)** also agreed to censure and to pay a fine of $500,000 to FINRA. FINRA found that UBSS failed to establish and implement AML programs reasonably designed to monitor penny stock transactions for potentially suspicious activity and, like UBS, failed to establish a reasonably designed due diligence program for correspondent accounts.

c) SEC Continues to Be an Active AML Enforcer

In May 2018, **Chardan Capital Markets LLC** agreed with the SEC to pay a $1 million penalty (and to accept a censure) to settle charges relating to Chardan's alleged failure to file SARs for suspicious penny stock transactions that occurred between October 2013 and June 2014. The SEC alleged that Chardan liquidated more than 12.5 billion penny stock shares for seven of its customers and did not file SARs, even though the transactions had several indicia of possible fraud—for example, similar trading patterns or sales in issuers that lacked either revenues or products. The SEC claimed that Chardan's actions violated both the Exchange Act and an SEC financial record-keeping and reporting rule. The SEC also alleged that Chardan's AML officer, Jerard Basmagy, was complicit in the illegal behavior. Like his employer, Basmagy settled the charges without admitting or denying the SEC's findings; he paid a penalty of $15,000 and agreed to industry and penny stock bars for at least three years.

Finally, in July 2018, **Charles Schwab & Co. Inc.** agreed with the SEC to pay a $2.8 million civil penalty to settle charges relating to Schwab's alleged failure to file SARs for suspicious transactions made in 2012 and 2013 by independent investment advisors whom Schwab had terminated from using Schwab as custodian for their client accounts.[236] Schwab failed to file SARs in certain instances where it suspected, or had reason to suspect, that the terminated advisor had engaged in a suspicious transaction. These instances included (1) transactions that possibly involved undisclosed self-dealing or conflicts of interest; (2) advisors who charged excessive advisory fees to their client accounts; (3) potentially fraudulent client account transactions; (4) advisors posing as one of their clients in the client's account to effect (or confirm) transactions; and (5) executing client trades, and/or collecting advisory fees, despite lacking the proper advisor registration. Schwab also failed to file SARs in certain instances where it suspected, or had reason to suspect, that the terminated advisor had misused client funds, but the client had not complained.

d) FINRA: Continued Enforcement in Microcap Trading

FINRA continued to focus on AML violations, especially those relating to microcap trading, issuing fines against several financial institutions. FINRA's actions in connection with microcap transactions also include a number of other violations.

Most notably, in December 2018, FINRA fined **Morgan Stanley Smith Barney LLC** $10 million for AML program failures over a five-year period. FINRA identified three key deficiencies: (i) Morgan Stanley's transaction monitoring system did not receive critical data, which weakened its monitoring of wire and foreign currency transfers, including those involving high-risk jurisdictions; (ii) failure to provide sufficient resources to review transaction monitoring alerts, resulting in incomplete or poorly documented investigations; and (iii) failure to reasonably monitor for suspicious activity deposits and trades in microcap securities.

In July 2017, FINRA fined broker-dealer **Spartan Securities Group Ltd.** $100,000 for AML program deficiencies that caused a failure to detect red flags and report eight instances of suspicious activity despite red flags such as customers maintaining bank accounts in tax havens, false or contradictory business representations, and large or unexplainable fluctuations in the prices of securities. FINRA criticized Spartan for reviewing clients' individual transactions in "silos" and failing to consider the context surrounding each transaction. FINRA censured and fined in April 2017 **Valdes & Moreno Inc.** $20,000 for failing to establish an effective AML compliance program to address issues related to microcap securities transactions. Among other violations, Valdes & Moreno allowed its president, CEO and CCO to conduct the "independent" test of the AML program.[237] FINRA took action in two other matters in September 2017, against **C.L. King & Associates Inc.**[238] and its AML compliance officer, and **Revere Securities LLC** and its branch manager (*see* infra).[239] FINRA also issued a censure and an $80,000 fine against **Alexander Capital LP** for failing to establish an effective AML program between February 2013 and March 2014.[240] Alexander Capital failed to detect and report potentially suspicious activity relating to transactions involving the liquidation of hundreds of millions of shares of microcap stocks.

In July 2017, FINRA censured and issued a $250,000 fine against **Electronic Transaction Clearing Inc. (ETC)** for failing to implement a compliant AML program between January 2013 and July 2015.[241] ETC is a clearing firm that provides high-volume execution and clearing services to broker-dealers, alternative trading systems, hedge funds, and other firms. Among a host of other problems, FINRA found that ETC failed to properly assess incidents of suspicious trading, failed to keep accurate books and records, and did not properly implement customer identification procedures.

6. Gaming

FinCEN only took one action against a gaming company in 2017 and 2018, which signals a trend that actions against gaming companies are down, perhaps reflecting FinCEN's view that the industry has made substantial strides in improving AML compliance efforts in the past few years. In 2017, FinCEN assessed an $8 million penalty against **Artichoke Joe's Casino (AJC)** for willful violations of AML laws, including failure to maintain an effective AML program and file SARs and CTRs.[242] The heart of the alleged deficiencies in AJC's AML program included failure to continually monitor customers on whom SARs were filed, conduct adequate due diligence on customers who pooled wagers anonymously, engage propositional players who observed suspicious transactions, and monitor transactions where loan sharks may have provided chips. AJC also allegedly failed to correct deficiencies identified in a 2011 independent test of its AML program and failed to conduct additional independent tests. In 2018, FinCEN issued a revised assessment of a civil monetary penalty, suspending $3 million of the 2017 penalty pending compliance with a set of undertakings identified in the release.

B. Sanctions Enforcement

OFAC indicated an aggressive enforcement posture in the first half of 2019, after a relatively quiet year in 2018. As of early June, OFAC reached settlements or issued penalties in more than 15 instances, with a total monetary value of nearly 1.3 billion.[243] The actions targeted violations of several sanctions regimes including for Iran, Cuba, Ukraine, Syria and North Korea. OFAC's April 2019 settlement with Standard Chartered Bank (which was part of a global settlement involving multiple regulatory authorities) for nearly $640 million was the largest of the year.[244]

The majority of OFAC's enforcement actions target violations of US sanctions against Iran, underscoring the priority that OFAC and the Trump Administration continue to place on sanctions that were reimposed following the US

withdrawal from the JCPOA. The enforcement pattern also illustrates OFAC's broad reach and signals that OFAC will look beyond financial institutions to those that do business with sanctioned jurisdictions and parties, if that business relies on the US financial system.

While notable 2018 and 2019 actions involved the financial sector, 2017 enforcement actions largely were focused on other types of firms. For example, OFAC's settlement with **ZTE Corporation** in March 2017 for $100,871,266 was the largest single penalty of the previous two years. Although sanctions have fluctuated in prior years—and in some periods, OFAC has reaped lower individual recoupments—the overall trend is toward stricter enforcement. For example: OFAC successfully prosecuted and achieved 16 penalties in 2017, up from nine in 2016 (almost the same as the 15 in 2015, but down from 23 in 2014). In those same years, the total annual penalties also moved around, with OFAC collecting its highest amount, $1.2 billion, in 2014, and its lowest, $21.6 million, in 2016.

Additionally, following a period in which OFAC enforcement actions against financial institutions seemed to be waning, OFAC may be renewing its focus on the activities of financial institutions, especially as international banks face difficult decisions about secondary sanctions risk in Iran, North Korea and Russia.

1. Focus on Iran

OFAC's increased focus on Iran post-JCPOA began in 2017 and has continued since. Nearly half of the enforcement actions taken in 2019 targeted violations of the Iranian Transactions and Sanctions Regulations (ITSR) or dealings with Iranian designated parties. OFAC also issued a finding of violation to State Street Bank and Trust Co. (SSBT) after SSBT processed pension payments to a plan participant who was a US citizen with a US bank account, but who resided Iran—though OFAC did not impose any monetary penalty for the violation.

OFAC's settlement with Stanley Black & Decker and its foreign subsidiary, Jiangsu Guoqiang Tools Co. Ltd. (GQ), was the largest (in terms of monetary amount) of Iran-related cases in 2019 (OFAC's settlements with UniCredit and SCB were far larger, but these enforcement actions implicated multiple sanctions programs in addition to Iran).[245] Stanley Black & Decker agreed to pay $1,869,144 on behalf of GQ for the latter's subsidiary's unauthorized export of various tools and related parts to Iran. Despite written agreements between Stanley Black & Decker and GQ, in which GQ's senior management executed attested that GQ would not engage in transactions with Iran, GQ continued to export goods to Iran.

OFAC's settlement with ZTE, which was part of a coordinated multiyear and multiagency effort, is also notable. In March 2017, OFAC announced its settlement with ZTE for over $100 million, the largest OFAC settlement ever with a nonfinancial institution. The ZTE settlement was part of a $1.2 billion settlement agreement with OFAC, the US Department of Commerce's Bureau of Industry and Security, and the DOJ arising from civil and criminal violations of the export control and sanctions laws. OFAC accused ZTE of a "multi-year and systemic practice of utilizing third-party companies to surreptitiously supply Iran with a substantial volume of U.S. origin goods," including controlled goods.

2. Expanded Reach

As the cases below illustrate, OFAC has demonstrated its expansive reach, exposing a broad range of activities and actors to potential sanctions violations.

a) ExxonMobil

In July 2017, OFAC penalized ExxonMobil and two of its subsidiaries $2 million for violating the Ukraine Related Sanctions Regulations (URSR). According to OFAC, the violation occurred when the presidents of ExxonMobil's US subsidiaries signed eight legal documents related to oil and gas projects in Russia with Rosneft OAO, on which Rosneft's CEO, Igor Sechin, was a signatory. While Rosneft property and property interests had not been blocked by OFAC, Sechin was on OFAC's SDN List, so US companies were prohibited from providing services to or receiving services from him. OFAC alleged that ExxonMobil "dealt in services of" Sechin and rejected ExxonMobil's argument that contracts executed by Sechin as Rosneft's representative rather than in his personal capacity. ExxonMobil defended this argument by citing a Treasury official who had stated that US persons would not be prohibited from participating in Rosneft's board meetings. In response, OFAC stated that ExxonMobil should have been on notice that its conduct potentially violated the regulations because, in addition to the "plain language" of the URSR that does not distinguish between "personal" and "professional," an FAQ under a different OFAC sanctions program and various official press statements spoke to the conduct at issue. The same day that OFAC issued its decision, ExxonMobil filed suit in federal court (the case is ongoing).[246]

b) CSE Global

Also in July 2017, OFAC announced a settlement with Singapore-based CSE Global Limited and its subsidiary CSE TransTel Pte. Ltd. for over $12 million. OFAC alleged that TransTel violated the ITSR and the International Emergency Economic Powers Act (IEEPA) by causing several banks to engage in unauthorized transactions. According to OFAC, TransTel contracted with multiple Iranian companies to deliver and install telecommunications equipment for energy projects in Iran. Top officials from both TransTel and CSE Global sent attestation letters to TransTel's Singapore bank stating that they would not route any Iran-related transactions through their US dollar accounts at the bank. But TransTel did initiate wire transfers from its account with the bank, and some of them were destined for Iranian parties that supplied goods or services for the energy projects in Iran. The fund transfers were processed through the United States. The case is one of the latest examples of a foreign company "causing" a US sanctions violation through its own acts or omissions.

3. Financial Institutions

a) Standard Chartered Bank

As part of a combined $1.1 billion global settlement involving multiple regulatory authorities,[247] SCB agreed to pay OFAC more than $639 million for apparent violations of various sanctions programs, including those applying to Iran, Cuba, Burma, Sudan and Syria. From 2009 to 2014, SCB processed thousands of transactions totaling nearly half a million dollars involving persons in Burma, Cuba, Iran, Sudan and Syria.[248] Most transactions concerned Iran-related customer accounts maintained by SCB's Dubai, UAE, branches ("SCB Dubai"), including accounts at SCB Dubai, held for a number of general trading companies and a petrochemical company.[249] SCB Dubai processed USD transactions to or through US financial institutions on behalf of these customers. SCB also processed online banking instructions for residents of comprehensively sanctioned countries.

b) SocGen

OFAC's settlement with Société Générale arose because of the bank's "processing of transactions to or through the United States or U.S. financial institutions in a manner that removed, omitted, obscured, or otherwise failed to include references to OFAC-sanctioned parties in the information sent to U.S. financial institutions that were involved in the

transactions."[250] The SocGen settlement was notable for several reasons. First, it continued a trend of global settlements of sanctions violations; here, the bank's settlement included not only OFAC but also the US Federal Reserve Bank, the New York County District Attorney's Office, the NYDFS and the US Attorney's Office for the Southern District of New York. Indeed, the state of New York continues to assert itself in major sanctions enforcement cases against financial institutions. Second, the total settlement of $1.34 billion was among the highest ever for a sanctions violation. Third, the bank's violations included those of multiple OFAC sanctions regimes—Sudan, Iran, Libya, Myanmar and North Korea—evidencing "the inadequacy of Société Générale's sanctions-related internal controls."[251] Fourth, the violations involved "stripping" data related to sanctions targets from financial messages, a practice that has been the predicate for sanctions enforcement actions against other banks for many years.

c) JPMorgan Chase Bank

OFAC's settlement with JPMorgan Chase Bank N.A. (JPMC) arose from JPMC's operation of a net settlement mechanism to resolve billings by various airlines on behalf of JPMC's client, a US entity with approximately 100 members, and a non-US entity and its more than 350 members. According to OFAC, JPMC processed transactions "that may have contained interests attributable to a sanctions-targeted party."[252] OFAC also noted that "JPMC does not appear to have had, prior to January 2012, a process to independently evaluate the participating member entities of the non-U.S. person entity for OFAC sanctions risk, despite receiving red flag notifications regarding OFAC-sanctioned members on at least three occasions." The settlement, for just over $5 million, illustrates the importance of onboarding due diligence especially as it relates to understanding "your customer's customer." OFAC also found that "JPMC staff members had actual knowledge of the individual members, including OFAC-sanctioned entities, involved in each transaction." JPMC's "enhanced employee training" and use of these violations "as a case study for training purposes" were a mitigating factor in OFAC's calculation of the penalty amount it sought.

4. Nonfinancial Institutions

While OFAC remains active in pursuing enforcement against financial services firms, the vast majority of its 2018–19 enforcement actions targeted nonfinancial institutions in the United States and abroad. The targeted nonfinancial institutions operate in a variety of sectors, including industrial goods, oil and gas, telecommunications, healthcare, retail, automotive, and international logistics.

5. Post-acquisition Liability

In several recent enforcement actions, OFAC has penalized a US parent company for the post-acquisition conduct of its foreign subsidiary involving Iran or Cuba (e.g., OFAC's enforcement actions against Stanley Black & Decker, Kollmorgen Corporation, and AppliChem GmbH). These actions indicate OFAC's expectations that US companies periodically and adequately audit or verify the activities of their foreign subsidiaries, even where these subsidiaries commit to refraining from conduct prohibited under US sanctions.

6. Compliance Programs

OFAC has repeatedly articulated an expectation that US and foreign companies develop and implement carefully tailored, risk-based sanctions compliance programs, and it has cited the lack of an adequate compliance program as an aggravating factor when calculating—and sometimes augmenting—the outcome of a violation. In May 2019, OFAC published its most detailed guidance to date on the essential components of a risk-based sanctions

compliance program.[253] In the dozen-pages-long document titled "A Framework for OFAC Compliance Commitments" ("Compliance Framework"), OFAC identified five overarching elements that are the pillars of an effective compliance program, though companies will likely vary in how they implement these expectations under the risk-based approach to sanctions compliance:

i. **Management Commitment**. A company's senior management should demonstrate and communicate its commitment to compliance. Ways to demonstrate such commitment include ensuring that compliance units are delegated sufficient authority, autonomy and resources, and promoting a "culture of compliance" throughout the organization.

ii. **Risk Assessment**. A compliance program should be tailored to the level of sanctions-specific risk posed, based on the company's activities, products and services, and customers, among other factors. The risk assessment should be conducted in a manner, and with a frequency, that adequately account for potential risks, and it should be based on a methodology for identifying, analyzing and addressing such risks.

iii. **Internal Controls**. Internal controls should be implemented to detect, escalate, report and record activities that are prohibited under US sanctions. OFAC has identified a range of specific elements or actions for ensuring that adequate controls are in place. These include implementing written sanctions, compliance-related policies and procedures; maintaining clear and effective internal controls pertaining to the company's ability to identify, interdict, escalate and report relevant transactions; enforcing the compliance policies and procedures; appointing personnel to integrate such policies and procedures; and conducting adequate record-keeping.

iv. **Testing and Auditing**. Periodic testing and audits should be conducted on specific elements of the compliance program and across the organization to identify and address any potential gaps. Specifically, the testing or audit should, inter alia, be a function that is accountable to the board, independent of the audited activities or functions, and has sufficient resources and authority within the organization. In addition, the risk assessment and sanctions program in general should be updated on a "periodic basis" to correct any potential weaknesses or deficiencies.

v. **Training**. Personnel and stakeholders should be provided sufficient and tailored sanctions-related training. This includes OFAC-related training with a scope and frequency that account for the company's risk profile and activities; at a minimum, all relevant employees should receive training at least once a year.

The settlement agreement followed recent indications by Department of the Treasury officials that future settlement agreements will be similarly specific in setting out the compliance commitments that OFAC will seek from each apparent violator. In a December 2018 speech at the American Bar Association, Under Secretary for Terrorism and Financial Intelligence Sigal Mandelker stated that "[t]o aid the compliance community in strengthening defenses against sanctions violations, OFAC will be outlining the hallmarks of an effective sanctions compliance program" in settlement agreements going forward.[254]

As the Compliance Framework and OFAC's past enforcement actions underscore, it is important for companies to harmonize their internal compliance programs with US sanctions laws in a way that accounts for the specific sanctions risks associated with their business.

ABOUT WILMERHALE'S AML AND ECONOMIC SANCTIONS COMPLIANCE AND ENFORCEMENT PRACTICE

WilmerHale's interdisciplinary AML and Economic Sanctions Compliance and Enforcement Group brings together leading practitioners to focus on our clients' most challenging AML- and economic sanctions–related regulatory, examination, and enforcement issues. The team has a wealth of knowledge and government experience at the forefront of AML and sanctions policy and enforcement. Our lawyers have worked in the US Department of Justice, US attorneys' offices, the US Department of the Treasury, the US Department of State, the Central Intelligence Agency and the National Security Agency, the Securities and Exchange Commission, the Office of the Comptroller of the Currency, the White House, and the US Congress. This depth of experience enables us to assist clients in anticipating and understanding the government's priorities, communicating with regulators and key stakeholders, and resolving the most challenging matters and law enforcement proceedings.

Regulatory: We advise financial institutions on a complex array of regulations issued by the Financial Crimes Enforcement Network, the Office of Foreign Assets Control, and state and federal banking and securities supervisors. We assist clients in preparing for and responding to regulatory examinations conducted by banking and securities regulators. Our attorneys draft regulatory comment letters and advise financial institutions and trade associations on the implications of forthcoming rulemakings. We also advocate for our clients regarding regulatory and statutory issues in Congress with key oversight and policymaking committees.

Compliance: We provide compliance training, advise on strategic and tactical compliance matters, and assist our clients in drafting policies and procedures to enhance their compliance programs. We help many US and non-US clients develop and implement internal policies and procedures to promote compliance with applicable AML and sanctions requirements, which often present complex challenges for financial institutions with global operations. Our advice includes corporate compliance programs, contractual assurances, technology control and vendor management plans, transaction and customer screening, and in-house training and compliance reviews.

Enforcement: We represent a diverse array of foreign and domestic financial institutions that have found themselves the targets of enforcement actions by federal and state regulators and of congressional inquiries. Our experience spans the life cycle of enforcement, from responding to initial formal and informal requests for information through negotiating and complying with consent orders. We also represent financial institutions in federal and state criminal investigations and frequently advise clients on matters involving voluntary self-disclosures of sanctions violations. Our attorneys have assisted financial and other institutions with their responses to nearly all of the major congressional inquiries regarding AML issues over the past two decades.

Transactional Counseling: AML and sanctions compliance issues arise in a variety of business transactions, including mergers and acquisitions, joint ventures, trade financing, and other specialized transactions. WilmerHale has extensive experience counseling financial firms on AML- and OFAC-related transactional issues. We work with colleagues in our Corporate Practice and Transactional Department to review and assess the risks associated with potential transactions, and advise on the allocation of risks and liabilities between the parties. Where appropriate, we design potential remediation.

FOR MORE INFORMATION ON AML AND SANCTIONS MATTERS, PLEASE CONTACT:

David S. Cohen **+1 202 663 6205** **david.cohen@wilmerhale.com**

Franca Harris Gutierrez **+1 202 663 6557** **franca.gutierrez@wilmerhale.com**

Sharon Cohen Levin **+1 212 230 8804** **sharon.levin@wilmerhale.com**

Ronald I. Meltzer **+1 202 663 6389** **ronald.meltzer@wilmerhale.com**

Jeremy Dresner **+1 202 663 6176** **jeremy.dresner@wilmerhale.com**

David M. Horn **+1 202 663 6749** **david.horn@wilmerhale.com**

Zachary Goldman **+1 212 295 6309** **zachary.goldman@wilmerhale.com**

Michael Romais **+1 202 663 6233** **michael.romais@wilmerhale.com**

Semira Nikou **+1 202 663 6511** **semira.nikou@wilmerhale.com**

Additional contributors included, Kenneth A. Brady, Michelle Nicole Diamond, Matthew F. Ferraro, Caryn Garvin, Lauren Ige, Kirsten Johansson, Pablo Lafuente, Jessica Lutkenhaus, Sheila E. Menz, and Russell Spivak.

---

[1] FinCEN, the Board of Governors of the Federal Reserve, the Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency recently issued a joint statement underscoring that their approach to examinations of financial institutions' AML compliance are themselves risk-based. The statement does not establish any new regulatory requirements. Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision (July 22, 2019), https://www.fincen.gov/sites/default/files/2019-07/Joint%20Statement%20on%20Risk-Focused%20Bank%20Secrecy%20Act-Anti-Money%20Laundering%20Supervision%20FINAL1.pdf.

[2] Codified at 31 C.F.R. § 1010.230.

[3] Press Release, FinCEN, *FinCEN Reissues Real Estate Geographic Targeting Orders and Expands Coverage to 12 Metropolitan Areas*, https://www.fincen.gov/news/news-releases/fincen-reissues-real-estate-geographic-targeting-orders-and-expands-coverage-12.

[4] Counter Terrorism and Illicit Finance Act, H.R. 6068, 115th Cong. § 10(a) (2018).

[5] FATF & Egmont Group, *Concealment of Beneficial Ownership* (July 2018), http://www.fatf-gafi.org/publications/methodsandtrends/documents/concealment-beneficial-ownership.html.

[6] Directive (EU) 2015/849, ch. III, 2015 O.J. (L 141) 73, http://data.europa.eu/eli/dir/2015/849/oj.

[7] Letter from Drew Maloney, Assistant Secretary of the Treasury for Legislative Affairs, to Senator Ron Wyden (Feb. 13, 2018), *available at* https://coincenter.org/files/2018-03/fincen-ico-letter-march-2018-coin-center.pdf.

[8] *See* Memorandum from David W. Ogden, Deputy Att'y Gen., US Dep't of Justice, to Selected US Att'ys: Investigations and Prosecutions in States Authorizing the Medical Use of Marijuana (Oct. 19, 2009); Memorandum from James M. Cole, Deputy Att'y Gen., US Dep't of Justice, to U.S. Att'ys: Guidance Regarding the Ogden Memo in Jurisdictions Seeking to Authorize Marijuana for Medical Use (June 29, 2011); Memorandum from James M. Cole, Deputy Att'y Gen., US Dep't of Justice, to All U.S. Att'ys: Guidance Regarding Marijuana Enforcement (Aug. 29, 2013); Memorandum from James M. Cole, Deputy Att'y Gen., U.S. Dep't of Justice, to All U.S. Att'ys: Guidance Regarding Marijuana Related Financial Crimes (Feb. 14, 2014).

[9] Memorandum from Jefferson B. Sessions III, Att'y Gen., US Dep't of Justice, to All US Att'ys: Marijuana Enforcement (Jan. 4, 2018), https://www.justice.gov/opa/press-release/file/1022196/download.

[10] Tom Angell, *Trump Attorney General Pick Puts Marijuana Enforcement Pledge In Writing*, FORBES.COM (Jan. 28, 2019, 1:23 PM), https://www.forbes.com/sites/tomangell/2019/01/28/trump-attorney-general-pick-puts-marijuana-enforcement-pledge-in-writing.

[11] *See* Consolidated and Further Continuing Appropriations Act, 2015, Pub. L. No. 113-235, 128 Stat. 2130 (2014); Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2242 (2015); Consolidated Appropriations Act, 2017, Pub. L. No. 115-31, 131 Stat. 135; Continuing Appropriations Act, 2018 and Supplemental Appropriations for Disaster Relief Requirements Act, 2017, Pub. L. No. 115-56, 131 Stat. 1129 (2017); Second Continuing Appropriations, Fiscal Year 2018, Pub. L. No. 115-90, 131 Stat. 1280 (2017); Third Continuing Appropriations for Fiscal Year 2018, Missile Defense, Health Provisions, Other Matters, and Budgetary Effects, 2018, Pub. L. No. 115-96, 131 Stat. 2044 (2017); Fourth Continuing Appropriations for the Fiscal Year 2018 Federal Register Printing Savings, Healthy Kids, Health-Related Taxes, and Budgetary Effects, Pub. L. No. 115-120, 132 Stat. 28; Continuing Appropriations Amendments Act, 2018, Pub. L. No. 115-124, 132 Stat. 314; Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, 132 Stat. 348.

[12] The 2018 Farm Bill defines "hemp" as any part of the cannabis plant "with a [THC] concentration of not more than 0.3 percent on a dry weight basis." Agriculture Improvement Act of 2018, § 297A, Pub. L. No. 115-334, H.R. Doc. No. 2 (signed by President, Dec. 20, 2018).

[13] *See*, *e.g.*, US Food and Drug Administration, FDA and Marijuana: Questions and Answers (last visited Feb. 5, 2019) (Q. "Can products that contain THC or cannabidiol (CBD) be sold as dietary supplements? A. No. Based on available evidence, FDA has concluded that THC and CBD products are excluded from the dietary supplement definition under Sections 201(ff)(3)(B)(i) and (ii) of the FD&C Act, respectively.").

[14] Medical marijuana–related businesses present an even lower risk of prosecution given the Rohrabacher-Blumenauer Amendment.

[15] FinCEN, FIN-2014-G001, BSA Expectations Regarding Marijuana-Related Businesses (Feb. 14, 2014), https://www.fincen.gov/sites/default/files/shared/FIN-2014-G001.pdf.

[16] *See* Press Release, Andrew M. Cuomo, Governor, New York State, *Governor Cuomo Announces Further Action to Support Development of Medical Marijuana and Industrial Hemp Businesses in New York* (July 3, 2018), https://www.governor.ny.gov/news/governor-cuomo-announces-further-action-support-development-medical-marijuana-and-industrial.

[17] *See* Secure and Fair Enforcement Banking Act of 2017, H.R. Doc. No. 2215, 115th Cong. (2017), and S. Doc. No. 1152, 115th Cong. (2017).

[18] *See*, *e.g.*, Reps. Ed Perlmutter (Colo.) & Denny Heck (Wash.), *Open the Banking System to the Marijuana Industry*, THE HILL (Feb. 7, 2018, 8:25 AM).

[19] Directive (EU) 2018/1673, 2018 O.J. (L 284) 22, https://eur-lex.europa.eu/eli/dir/2018/1673/oj.

[20] Proceeds of Crime Act 2002, c. 29, § 340(3) (UK).

[21] Press Release, US Dep't of the Treasury, *Treasury Publishes National Illicit Finance Strategy and Supporting Risk Assessments* (Dec. 20, 2018), https://home.treasury.gov/news/press-releases/sm581; US Dep't of the Treasury, National Strategy for Combating Terrorist and Other Illicit Financing (2018), https://home.treasury.gov/system/files/136/nationalstrategyforcombatingterroristandotherillicitfinancing.pdf.

[22] US Dep't of the Treasury, National Money Laundering Risk Assessment (2018) (NMLRA), https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf; US Dep't of the Treasury, National Terrorist Financing Risk Assessment (2018), https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf; US Dep't of the Treasury, National Proliferation Financing Risk Assessment (2018), https://home.treasury.gov/system/files/136/2018npfra_12_18.pdf.

[23] NMLRA at 2.

[24] NMLRA at 16.

[25] NMLRA at 20.

[26] NMLRA at 28.

[27] Brett Wolf, *'El Chapo' Renews U.S. Law Enforcement Concerns About Money Laundering via Prepaid Cards*, REUTERS (Mar. 7, 2019), https://www.reuters.com/article/bc-finreg-money-laundering/el-chapo-renews-us-law-enforcement-concerns-about-money-laundering-via-prepaid-cards-idUSKCN1QN218.

[28] The CDD Rule is codified at 31 C.F.R. § 1010.230.

[29] 31 C.F.R. § 1010.230(a).

[30] Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29,398 (May 11, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf.

[31] 31 C.F.R. § 1010.230(d).

[32] Customer Due Diligence Requirements for Financial Institutions; Final Rule, 81 Fed. Reg. 29,398 (May 11, 2016) (to be codified at 31 C.F.R. pts. 1010, 1020, 1023, 1024, 1026), https://www.govinfo.gov/content/pkg/FR-2016-05-11/pdf/2016-10567.pdf.

[33] 31 C.F.R. § 1010.230(d)(1).

[34] 31 C.F.R. § 1010.230(d)(2).

[35] Appendix A to 31 U.S.C. § 1010.230 – Certification Regarding Beneficial Owners of Legal Entity Customers, 81 Fed. Reg. 29,454 (May 11, 2016).

[36] 31 C.F.R. § 1010.230(b)(2).

[37] 31 C.F.R. § 1010.230(j).

[38] Customer Due Diligence Requirements for Financial Institutions; Final Rule, 81 Fed. Reg. 29,398 (May 11, 2016) (to be codified at 31 C.F.R. pts. 1010, 1020, 1023, 1024, 1026), https://www.govinfo.gov/content/pkg/FR-2016-05-11/pdf/2016-10567.pdf.

[39] FinCEN, FIN-2018-G001, Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (Apr. 3, 2018) (CDD Rule FAQs), https://www.fincen.gov/sites/default/files/2018-04/FinCEN_Guidance_CDD_FAQ_FINAL_508_2.pdf.

[40] CDD Rule FAQs no. 37.

[41] CDD Rule FAQs no. 37. *See also* 81 Fed. Reg. 29,398.

[42] CDD Rule FAQs no. 36.

[43] CDD Rule FAQs no. 1.

[44] CDD Rule FAQs no. 2.

[45] CDD Rule FAQs no. 13.

[46] CDD Rule FAQs no. 13.

[47] *See, e.g.*, CDD Rule FAQs nos. 3, 6, and 21.

[48] CDD Rule FAQs no. 3.

[49] CDD Rule FAQs no. 21.

[50] CDD Rule FAQs no. 4.

[51] CDD Rule FAQs nos. 4 and 6.

[52] CDD Rule FAQs nos. 7 and 10.

[53] CDD Rule FAQs no. 7.

[54] CDD Rule FAQs no. 10.

[55] *See, e.g.*, CDD Rule FAQs nos. 24, 25, 26, 27, and 28.

[56] CDD Rule FAQs no. 24.

[57] CDD Rule FAQs no. 25.

[58] CDD Rule FAQs no. 25.

[59] CDD Rule FAQs no. 26.

[60] CDD Rule FAQs no. 26.

[61] CDD Rule FAQs no. 26. *See also* CDD Rule FAQs no. 21.

[62] CDD Rule FAQs no. 27.

[63] CDD Rule FAQs no. 27.

[64] CDD Rule FAQs no. 26.

[65] CDD Rule FAQs no. 26.

[66] CDD Rule FAQs no. 18.

[67] CDD Rule FAQs no. 33.

[68] CDD Rule FAQs no. 32.

[69] CDD Rule FAQs no. 33.

[70] FinCEN, Geographic Targeting Order Covering Title Insurance Company (Nov. 15, 2018), https://www.fincen.gov/sites/default/files/shared/Real%20Estate%20GTO%20GENERIC_111518_FINAL%20508.pdf.

[71] *See* NYDFS Superintendent's Regulations, N.Y. Comp. Codes R. & Regs. tit.3, pt. 504, https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsp504t.pdf; Press Release, NYDFS, *NYDFS Issues Final Anti-Terrorism Transaction Monitoring and Filtering Program Regulation* (June 30, 2016), http://www.dfs.ny.gov/about/press/pr1606301.htm.

[72] NYDFS, Transaction Monitoring – Frequently Asked Questions Regarding 3 NYCRR 504, https://www.dfs.ny.gov/industry_guidance/transaction_monitoring_faqs.

[73] NYDFS, Transaction Monitoring – Frequently Asked Questions Regarding 3 NYCRR 504, https://www.dfs.ny.gov/industry_guidance/transaction_monitoring_faqs.

[74] NYDFS, Transaction Monitoring – Frequently Asked Questions Regarding 3 NYCRR 504, https://www.dfs.ny.gov/industry_guidance/transaction_monitoring_faqs (emphasis added).

[75] NYDFS, Transaction Monitoring – Frequently Asked Questions Regarding 3 NYCRR 504, https://www.dfs.ny.gov/industry_guidance/transaction_monitoring_faqs; N.Y. Comp. Codes R. & Regs. tit.3, § 504.3(d).

[76] N.Y. Comp. Codes R. & Regs. tit.3, § 504.3(a)(2).

[77] NYDFS, Frequently Asked Questions Regarding 3 NYCRR 504 (Apr. 9, 2018), https://www.dfs.ny.gov/industry_guidance/transaction_monitoring_faqs.

[78] N.Y. Comp. Codes R. & Regs. tit.3, § 504.3(c)(7).

[79] NYDFS, Transaction Monitoring – Frequently Asked Questions Regarding 3 NYCRR 504, https://www.dfs.ny.gov/industry_guidance/transaction_monitoring_faqs.

[80] FRB, FDIC, FinCEN, NCUA, & OCC, Interagency Statement on Sharing Bank Secrecy Act Resources (Oct. 3, 2018), https://www.fincen.gov/sites/default/files/2018-10/Interagency%20Statement%20on%20Sharing%20BSA%20Resources%20-%20%28Final%2010-3-18%29%20%28003%29.pdf.

[81] FRB, FDIC, FinCEN, NCUA, & OCC, Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing (Dec. 3, 2018), https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf.

[82] Press Release, FinCEN, *FinCEN Launches "FinCEN Exchange" to Enhance Public-Private Information Sharing* (Dec. 4, 2017), https://www.fincen.gov/news/news-releases/fincen-launches-fincen-exchange-enhance-public-private-information-sharing.

[83] Press Release, US Dep't of the Treasury, *Under Secretary Sigal Mandelker Speech before the American Bankers Association & American Bar Association Financial Crimes Enforcement Conference* (Dec. 4, 2017), https://www.treasury.gov/press-center/press-releases/Pages/sm0229.aspx.

[84] Press Release, US Dep't of the Treasury, *Under Secretary Sigal Mandelker Speech before the American Bankers Association & American Bar Association Financial Crimes Enforcement Conference* (Dec. 4, 2017), https://www.treasury.gov/press-center/press-releases/Pages/sm0229.aspx.

[85] Press Release, FinCEN, *FinCEN Launches "FinCEN Exchange" to Enhance Public-Private Information Sharing* (Dec. 4, 2017), https://www.fincen.gov/news/news-releases/fincen-launches-fincen-exchange-enhance-public-private-information-sharing.

[86] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001), § 314(b).

[87] Press Release, US Dep't of the Treasury, *Under Secretary Sigal Mandelker Speech before the American Bankers Association & American Bar Association Financial Crimes Enforcement Conference* (Dec. 4, 2017), https://www.treasury.gov/press-center/press-releases/Pages/sm0229.aspx.

[88] FinCEN, FIN-2017-A004, Advisory on Political Corruption Risks in South Sudan (Sept. 6, 2017), https://www.fincen.gov/sites/default/files/advisory/2017-09-06/South%20Sudan%20Advisory_09-06-2017_0.pdf.

[89] FinCEN, FIN-2017-A006, Reports from Financial Institutions are Critical to Stopping, Deterring, and Preventing the Proceeds Tied to Suspected Venezuelan Public Corruption from Moving through the U.S. Financial System (Sept. 20, 2017), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a006.

[90] FinCEN, FIN-2017-A006, Reports from Financial Institutions are Critical to Stopping, Deterring, and Preventing the Proceeds Tied to Suspected Venezuelan Public Corruption from Moving through the U.S. Financial System (Sept. 20, 2017), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a006.

[91] FinCEN, FIN-2019-A002, Updated Advisory on Widespread Public Corruption

in Venezuela (May 3, 2019), https://www.fincen.gov/sites/default/files/advisory/2019-05-08/Venezuela%20Advisory%20FINAL%20508.pdf.

[92] FinCEN, FIN-2017-A007, Financial Institutions Should be Aware of Potential Fraudulent Activity Related to Disaster Relief Efforts (Oct. 31, 2017), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a007-0.

[93] FinCEN, FIN-2017-A002, Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies (Apr. 5, 2017), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a002.

[94] FinCEN, FIN-2018-A007, Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combatting the Financing of Terrorism Deficiencies (Oct. 31, 2018), https://www.fincen.gov/sites/default/files/advisory/2018-10-31/FATF%20Advisory%20Oct_FINAL%20508.pdf.

[95] FinCEN, FIN-2019-A001, Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combatting the Financing of Terrorism Deficiencies (Mar. 8, 2019), https://www.fincen.gov/sites/default/files/advisory/2019-03-08/FAFT_Advisory_March_final_508.pdf.

[96] FinCEN, FIN-2018-A003, Advisory on Human Rights Abuses Enabled by Corrupt Senior Foreign Political Figures and their Financial Facilitators, at 2 (June 12, 2018), *accessible at* https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2018-a003.

[97] FinCEN, FIN-2018-A005, Advisory to Financial Institutions on the Risk of Proceeds of Corruption from Nicaragua (Oct. 4, 2018), https://www.fincen.gov/sites/default/files/advisory/2018-10-04/Nicaragua_Advisory_FINAL_508_0.pdf.

[98] FinCEN, FIN-2018-A006, Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System (Oct. 11, 2018), https://www.fincen.gov/sites/default/files/advisory/2018-10-12/Iran%20Advisory%20FINAL%20508.pdf.

[99] Letter from Andrea M. Sharrin, Assoc. Dir., Policy Div., FinCEN, to David Schwartz, Pres. & CEO, Florida Int'l Bankers Assoc. (Feb. 21, 2018), https://www.jonesday.com/files/upload/FinCen%20letter.pdf.

[100] SEC, 2019 Examination Priorities (SEC 2019 Exam Priorities), https://www.sec.gov/files/OCIE%202019%20Priorities.pdf; FINRA, 2019 Risk Monitoring and Examination Priorities Letter (Jan. 2019) (FINRA 2019 Exam Priorities), http://www.finra.org/sites/default/files/2019_Risk_Monitoring_and_Examination_Priorities_Letter.pdf.

[101] SEC 2019 Exam Priorities, at 12, https://www.sec.gov/files/OCIE%202019%20Priorities.pdf.

[102] FINRA 2019 Exam Priorities, at 4, http://www.finra.org/sites/default/files/2019_Risk_Monitoring_and_Examination_Priorities_Letter.pdf.

[103] FINRA 2019 Exam Priorities, at 4, http://www.finra.org/sites/default/files/2019_Risk_Monitoring_and_Examination_Priorities_Letter.pdf.

[104] FINRA, Report on FINRA Examination Findings (Dec. 2018), http://www.finra.org/sites/default/files/2018_exam_findings.pdf.

[105] *See generally* Memo from Financial Services Committee Majority Staff to Members, Committee on Financial Services (Mar. 13, 2019), https://financialservices.house.gov/uploadedfiles/hhrg-116-ba10-20190313-sd002_-_memo.pdf.

[106] The sanctions menu is set out in Section 235 of CAATSA, Pub. L. No. 115-44, 131 Stat. 886, 919 (2017), https://www.congress.gov/115/plaws/publ44/PLAW-115publ44.pdf. It contains sanctions that range from limitations on financing from the Export-Import Bank of the United States and restrictions on US export privileges to prohibitions on banking transactions and the exclusion of corporate officers from the United States.

[107] US Dep't of the Treasury, *CAATSA - Russia-related Designations* (Sept. 20, 2018), https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20180920_33.aspx.

[108] US Dep't of State, *CAATSA Section 231: "Addition of 33 Entities and Individuals to the List of Specified Persons and Imposition of Sanctions on the Equipment Development Department"* (Sept. 20, 2018), https://www.state.gov/r/pa/prs/ps/2018/09/286077.htm.

[109] The State Department had published this list in October 2017 pursuant to Section 231 of CAATSA, which required that the administration issue guidance to specify those persons that are part of the Russian defense and intelligence sectors.

[110] *See* CAATSA, § 241.

[111] *See* US Dep't of the Treasury, OFAC FAQs (updated Feb. 6, 2019) (OFAC FAQs), nos. 567-586.

[112] These include Ukraine-/Russia-related General Licenses 12 (A, B, and C), 13 (A, B, and C), 14, 15, and 16 (A, B, C, and D).

[113] Letter from Andrea M. Gacki, Director, OFAC, to Sen. Mitch McConnell, Majority Leader of the US Senate (Dec. 19, 2018), https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/20181219_notification_removal.pdf.

[114] *See* Determinations Regarding Use of Chemical Weapons by Russia, 83 Fed. Reg. 43,723 (Aug, 27, 2018), https://www.govinfo.gov/content/pkg/FR-2018-08-27/pdf/2018-18503.pdf.

[115] The State Department, however, also stated that exports/reexports pursuant to new licenses for Russian state-owned or state-funded enterprises will be reviewed on a case-by-case basis, though subject to a presumption of denial. *See* 83 Fed. Reg. 43,723.

[116] Lesley Wroughton, *U.S. Intends More Sanctions on Russia Over Chemical Weapons: Spokeswoman*, REUTERS (Nov. 6, 2018), https://www.reuters.com/article/us-usa-russia-sanctions-law/u-s-intends-more-sanctions-on-russia-over-chemical-weapons-spokeswoman-idUSKCN1NB2O8.

[117] Exec. Order No. 13,848, 83 Fed. Reg. 46,843 (Sept. 14, 2018), https://www.govinfo.gov/content/pkg/FR-2018-09-14/pdf/2018-20203.pdf.

[118] Exec. Order No. 13,848 sets out a reporting process that is to occur after each federal election to identify foreign interference.

[119] Press Release, Office of the Dir. of Nat'l Intelligence, *DNI Coats Statement on the Intelligence Community's Response to Executive Order 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election* (Dec. 21, 2018), *accessible at* https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2018.

[120] National Security Presidential Memorandum, Ceasing United States Participation in the Joint Comprehensive Plan of Action and Taking Additional Action to Counter Iran's Malign Influence and Deny

Iran All Paths to a Nuclear Weapon (May 8, 2018), https://www.whitehouse.gov/presidential-actions/ceasing-u-s-participation-jcpoa-taking-additional-action-counter-irans-malign-influence-deny-iran-paths-nuclear-weapon/.

[121] *See* US Dep't of State, *Briefing on Iran Sanctions* (Nov. 2, 2018), https://www.state.gov/secretary/remarks/2018/11/287090.htm.

[122] Iraq was granted a 45-day waiver to purchase natural gas from Iran.

[123] *See* US Dep't of State, *Briefing on Iran Sanctions* (Nov. 2, 2018), https://www.state.gov/secretary/remarks/2018/11/287090.htm ("The Obama administration issued SREs to 20 countries multiple times between 2012 and 2015. We will have issued, if our negotiations are completed, eight and have made it clear that they are temporary. Not only did we decide to grant many fewer exemptions, but we demanded much more serious concessions from these jurisdictions before agreeing to allow them to temporarily continue to import Iranian crude oil. These concessions are critical to ensure that we increase our maximum pressure campaign and accelerate towards zero." (comments by Michael Pompeo, US Sec'y of State); Ellie Geranmayeh & Esfandyar Batmanghelidj, *America's Latest Wave of Iran Sanctions: An Explainer*, BOURSE & BAZAAR (Nov. 7, 2018), https://www.bourseandbazaar.com/articles/2018/11/7/americas-latest-wave-of-iran-sanctions-an-explainer; Steven Erlanger & Milan Schreuer, *Europe Asks U.S. for an Exemption From Sanctions on Iran,* N.Y. TIMES (June 6, 2018), https://www.nytimes.com/2018/06/06/world/europe/iran-europe-us-sanctions.html.

[124] *INSTEX: Europe sets up transactions channel with Iran*, DW.COM (Jan. 31, 2019), https://www.dw.com/en/instex-europe-sets-up-transactions-channel-with-iran/a-47303580.

[125] In a letter to INSTEX, the Treasury Department's under secretary for terrorism and financial intelligence, Sigal Mandelker, also stated, "I urge you to carefully consider the potential sanctions exposure of Instex." Jonathan Stearns and Helene Fouquet, *U.S. Warns Europe That Its Iran Workaround Could Face Sanctions*, Bloomberg (May 29, 2019), https://www.bloomberg.com/news/articles/2019-05-29/u-s-warns-europe-that-its-iran-workaround-could-face-sanctions.

[126] Statement from the President on the Designation of the Islamic Revolutionary Guard Corps as a Foreign Terrorist Organization (Apr. 8, 2019), https://www.whitehouse.gov/briefings-statements/statement-president-designation-islamic-revolutionary-guard-corps-foreign-terrorist-organization/.

[127] Strengthening the Policy of the United States Toward Cuba, 82 Fed. Reg. 48,875 (Oct. 20, 2017).

[128] The Department of Commerce's Bureau of Industry and Security has also established a general policy of denial for export applications to these entities, unless the transactions are determined to be consistent with the National Security Presidential Memorandum. *See* 15 C.F.R. § 746.2(b)(3)(i). Before November 9, 2017, BIS evaluated export license applications based on a presumption of approval with respect to certain products, including certain medicine and agricultural commodities. In addition, BIS concurrently expanded the preexisting License Exception Support for the Cuban People to ease restrictions on exports to the Cuban private sector—a change that may provide US companies greater opportunities to engage commercially in Cuba provided their business does not involve any state-owned entities. *See* 15 C.F.R. § 740.21.

[129] *See* US Dep't of State, List of Restricted Entities and Subentities Associated With Cuba as of April 24, 2019, https://www.state.gov/cuba-sanctions/cuba-restricted-list/list-of-restricted-entities-and-subentities-associated-with-cuba-as-of-april-24-2019/.

[130] Press Release, US Dep't of State, *State Department Updates the Cuba Restricted List* (Nov. 14, 2018), https://www.state.gov/r/pa/prs/ps/2018/11/287357.htm.

[131] *See* 31 C.F.R. § 515.209(c).

[132] Fed. Reg. 25992 (June 5, 2019).

[133] In 2018, the Trump Administration also limited the general license for "travel for support for the Cuban people" by requiring individuals traveling pursuant to this general license to engage in a full-time schedule of activities related to enhancing Cuban civil society and independence from the Cuban authorities.

[134] North Korea was also targeted under CAATSA. In particular, Section 311 of CAATSA expands the North Korea Sanctions and Policy Enhancement Act of 2016 (NKSPEA) by increasing mandatory blocking sanctions against North Korea, including by applying them to those connected to trade with North Korea in certain extractives and rare earth minerals and in rocket, aviation, or jet fuel (with a limited exceptions). It also broadens the scope of NKSPEA's defense export controls, mandates sanctions against those engaged in transactions involving US- or UN-designed vessels or aircraft, and mandates sanctions against those who knowingly maintain a correspondent account with any North Korean financial institution.

[135] *See* Press Release, US Dep't of the Treasury, *Treasury Designates Singapore-Based Targets for Laundering Money in Support of North Korea* (Oct. 25, 2018), https://home.treasury.gov/news/press-releases/sm533; Press Release, US Dep't of the Treasury, *Treasury Designates Company in Turkey for Attempting to Trade Arms and Luxury Goods with North Korea* (Oct. 4, 2018) https://home.treasury.gov/news/press-releases/sm503; US Dep't of the Treasury, North Korea

Designations; Publication of North Korea Vessel Advisory (Feb. 23, 2018), https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20180223.aspx; Press Release, US Dep't of the Treasury, *Treasury Sanctions North Korean Overseas Representatives, Shipping Companies, and Chinese Entities Supporting the Kim Regime* (Jan. 24, 2018), https://home.treasury.gov/news/press-releases/sm0257.

[136] *See* 22 U.S.C. § 9241a.

[137] *See* US Dep't of the Treasury, Sanctions Risks Related to North Korea's Shipping Practices (Feb. 23, 2018), https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/dprk_vessel_advisory_02232018.pdf.

[138] *See* US Dep't of the Treasury, Risks for Businesses with Supply Chain Links to North Korea (July. 23, 2018), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/dprk_supplychain_advisory_07232018.pdf. The Department of Homeland Security has also issued guidance on Section 321 of CAATSA related to imports made with North Korean forced labor, including general expectations with respect to due diligence best practices.

[139] Choe Sang-Hun, *South Korea Considers Lifting Sanctions Against North Korea*, N.Y. TIMES (Oct. 10, 2018), https://www.nytimes.com/2018/10/10/world/asia/south-korea-sanctions-north-korea.html.

[140] Removal of the Sudanese Sanctions Regulations and Amendment of the Terrorism List Government Sanctions Regulations, 83 Fed. Reg. 30,539 (June 29, 2018). OFAC also incorporated a general license (General License A) into the Terrorism List Government Sanctions Regulations, 31 C.F.R. Part 596, authorizing exports and reexports to Sudan of agricultural commodities, medicine and medical devices. The export and reexport of such items previously required an OFAC license due to Sudan's continued inclusion on the State Sponsors of Terrorism List.

[141] Prior to August 2017, US sanctions against Venezuela were generally limited to SDN designations.

[142] The term "debt" is interpreted broadly to include bonds, loans, extensions of credit, loan guarantees, letters of credit, drafts, bankers acceptances, discount notes or bills, or commercial paper. Equity includes stocks, share issuances, depository receipts, and any other evidence of title or ownership.

[143] "New" debt or equity refers to debt or equity issued after August 24, the effective date of these new sanctions measures. The sanctions against PdVSA do not apply to old debt (though sanctions applicable to the Government of Venezuela include previously issued sovereign bonds). OFAC has also issued several general licenses accompanying the sanctions. The general licenses authorize transactions related to certain previously issued bonds, transactions dealing with only CITGO Holding Inc. and any of

its subsidiaries, and transactions related to the export or reexport of certain agricultural commodities, medicine, medical devices and replacement parts.

[144] *See* OFAC FAQs nos. 628-29. FAQ 629 states that "OFAC expects to use its discretion to target in particular those who operate corruptly in the gold or other identified sectors of the Venezuela economy, and not those who are operating legitimately in such sectors."

[145] Press Release, US Dep't of the Treasury, *Treasury Sanctions Venezuela's State-Owned Oil Company Petroleos de Venezuela, S.A.* (Jan. 28, 2019), https://home.treasury.gov/news/press-releases/sm594.

[146] *See* Meg Wagner and Brian Ries, *Trump Meets with Brazil's President*, CNN (Mar. 19, 2019) (President Trump stating, "At some point, I would imagine things will change, but we really haven't done the really tough sanctions yet, ... We can do the tough sanctions, and all options are open so we may be doing that, but we haven't done the toughest of sanctions, . . ."), https://edition.cnn.com/politics/live-news/trump-brazil-president-jair-bolsonaro-march-2019/index.html.

[147] OFAC has since designated additional individuals and organizations for their cyber-related activities. *See* Press Release, US Dep't of the Treasury, *Treasury Sanctions Iranian Organizations and Individuals Supporting Intelligence and Cyber Targeting of U.S. Persons* (Feb. 13, 2019), https://home.treasury.gov/news/press-releases/sm611.

[148] For example, OFAC FAQ 564, issued in relation to Exec. Order No. 13,827 (Venezuela), explains that the phrase "digital currency, digital coin, or digital token" includes the petro and petro gold.

[149] Exec. Order No. 13,851 also suspends the entry of designated persons into the United States, unless the Secretary of State determines that a person's entry is in the US national interest.

[150] Press Release, US Dep't of the Treasury, *Treasury Targets Finances of Nicaraguan President Daniel Ortega's Regime* (Apr. 17, 2019), https://home.treasury.gov/index.php/news/press-releases/sm662.

[151] National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, 130 Stat. 2000, 2533 *et seq*. (2016).

[152] Press Release, US Dep't of the Treasury, *Treasury Sanctions 17 Individuals for Their Roles in the Killing of Jamal Khashoggi* (Nov. 15, 2018), https://home.treasury.gov/news/press-releases/sm547.

[153] The letter triggered a requirement under the Global Magnitsky Act for the President to report to Congress within 120 days with a decision on the imposition of sanctions on foreign persons connected to the killing. Pub. L. No. 114-328 § 1263(d).

[154] Press Release, US Dep't of the Treasury, *Treasury Sanctions Turkish Officials with Leading Roles in Unjust Detention of U.S. Pastor Andrew Brunson* (Aug. 1, 2018), https://home.treasury.gov/news/press-releases/sm453.

[155] US Dep't of the Treasury, *Global Magnitsky Designations Removals* (Nov. 2, 2018), https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20181102.aspx.

[156] OFAC FAQs nos. 559-662.

[157] OFAC FAQs nos. 646-647.

[158] Press Release, US Dep't of the Treasury, *Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses* (Nov. 28, 2018), https://home.treasury.gov/news/press-releases/sm556.

[159] Press Release, FinCEN, *FinCEN and Manhattan U.S. Attorney Announce Settlement with Former MoneyGram Executive Thomas E. Haider* (May 4, 2017), https://www.fincen.gov/sites/default/files/2017-05/HaiderSettlement_050417.pdf.

[160] Press Release, US Dep't of Justice, *Rabobank NA Pleads Guilty, Agrees to Pay Over $360 Million* (Feb. 7, 2018), https://www.justice.gov/opa/pr/rabobank-na-pleads-guilty-agrees-pay-over-360-million.

[161] Press Release, FINRA, *FINRA Hearing Panel Fines C.L. King & Associates $750,000 for Negligent Misrepresentations and Omissions in Connection with Death Put Investments and AML-Related Violations* (Sept. 12, 2017), http://www.finra.org/newsroom/2017/finra-hearing-panel-fines-cl-king-associates-750000-negligent-misrepresentations-and.

[162] *Revere Securities, LLC*, No. 2014039396101, Letter of Acceptance, Waiver and Consent (FINRA Sept. 7, 2017), http://www.finra.org/sites/default/files/fda_documents/2014039396101_FDA_VA702409.pdf.

[163] Press Release, FinCEN, *FinCEN and Manhattan U.S. Attorney Announce Settlement with Former MoneyGram Executive Thomas E. Haider* (May 4, 2017), https://www.fincen.gov/sites/default/files/2017-05/HaiderSettlement_050417.pdf.

[164] WilmerHale Client Alert*, AML Litigation and Individual Liability: FinCEN's Landmark Haider Case Moves Forward* (Jan. 21, 2016), https://www.wilmerhale.com/en/insights/client-alerts/2016-01-21-aml-litigation-and-individual-liability-fincens-landmark-haider-case-moves-forward.

[165] Press Release, US Dep't of Justice, *Rabobank NA Pleads Guilty, Agrees to Pay Over $360 Million* (Feb. 7, 2018), https://www.justice.gov/opa/pr/rabobank-na-pleads-guilty-agrees-pay-over-360-million.

[166] Press Release, OCC, *OCC Enforcement Actions and Terminations for April 2018* (April 19, 2018), https://www.occ.treas.gov/news-issuances/news-releases/2018/nr-occ-2018-40.html; Press Release, OCC, *OCC Enforcement Actions and Terminations for May 2018* (May 17, 2018), https://www.occ.treas.gov/news-issuances/news-releases/2018/nr-occ-2018-47.html.

[167] Press Release, OCC, *OCC Enforcement Actions and Terminations for July 2018* (July 20, 2018), https://www.occ.gov/news-issuances/news-releases/2018/nr-occ-2018-73.html.

[168] Press Release, OCC, *OCC Enforcement Actions and Terminations for April 2016* (April 15, 2016), https://www.occ.treas.gov/news-issuances/news-releases/2016/nr-occ-2016-48.html.

[169] Press Release, OCC, *OCC Enforcement Actions and Terminations for October 2018* (October 19, 2018), https://www.occ.gov/news-issuances/news-releases/2018/nr-occ-2018-111.html.

[170] *Dep't of Enforcement v. C.L. King & Assoc., Inc.*, No. 2014040476901, Extended Hearing Panel Decision, at 60-61 (FINRA Sept. 6, 2017), https://www.finra.org/sites/default/files/King_Miller_action_091217.pdf.

[171] *Revere Securities, LLC*, No. 2014039396101, Letter of Acceptance, Waiver and Consent (FINRA Sept. 7, 2017), http://www.finra.org/sites/default/files/fda_documents/2014039396101_FDA_VA702409.pdf.

[172] Complaint, *United States v. Edwards*, No. 18MAG8861 (S.D.N.Y. Oct. 16, 2018), https://www.justice.gov/usao-sdny/press-release/file/1101511/download; Press Release, US Atty's Off., S.D.N.Y., *Senior FinCen Employee Arrested and Charged with Unlawfully Disclosing SARs* (Oct. 17, 2018), https://www.justice.gov/usao-sdny/pr/senior-fincen-employee-arrested-and-charged-unlawfully-disclosing-sars; Aruna Viswanatha & Rebecca Davis O'Brien, *Treasury Official Accused of Leaks Is a Trump Supporter Who Feuded with Another Unit*, WALL ST. J. (Oct. 25, 2018), https://www.wsj.com/articles/treasury-official-accused-of-leaks-had-bureaucratic-complaints-about-another-unit-1540465200.

[173] *See* 31 U.S.C. § 5318(g).

[174] *See* 31 C.F.R. § 320(e)(1)(i).

[175] *See* 31 U.S.C. §§ 5321-5322; 31 C.F.R. §§ 1010.820, 1010.840.

[176] *See* 31 U.S.C. §§ 5321-5322; 31 C.F.R. §§ 1010.820, 1010.840.

[177] 31 U.S.C. § 5321(a)(1).

[178] *See* FinCEN, FIN-2012-A002, SAR Confidentiality Reminder for Internal and External Counsel of Financial Institutions (Mar. 2, 2012), https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A002.pdf.

[179] *See* FinCEN, FIN-2012-A002, SAR Confidentiality Reminder for Internal and External Counsel of Financial Institutions (Mar. 2, 2012), https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A002.pdf.

[180] Bank Secrecy Act Advisory Group, *The SAR Activity Review: Trends Tips & Issues, Issue 7* (Aug 2004), https://www.fincen.gov/sites/default/files/shared/sar_tti_07.pdf.

[181] Bank Secrecy Act Advisory Group, *The SAR Activity Review: Trends Tips & Issues, Issue 7* (Aug 2004), https://www.fincen.gov/sites/default/files/shared/sar_tti_07.pdf.

[182] Bank Secrecy Act Advisory Group, *The SAR Activity Review: Trends Tips & Issues, Issue 7* (Aug 2004), https://www.fincen.gov/sites/default/files/shared/sar_tti_07.pdf.

[183] Bank Secrecy Act Advisory Group, *The SAR Activity Review: Trends Tips & Issues, Issue 7* (Aug 2004), https://www.fincen.gov/sites/default/files/shared/sar_tti_07.pdf.

[184] Opinion & Order, *U.S. Secs. & Exchange Comm'n v. Alpine Secs. Corp.*, No. 17-cv-4179 (DLC) (S.D.N.Y. Dec. 11, 2018) [hereinafter "*Alpine Secs.*"].

[185] 17 C.F.R. § 240.17a-8.

[186] *See Alpine Secs.* at 3 (citing 31 C.F.R. § 1023.320).

[187] *Alpine Secs.* at 31-32 (citing 15 U.S.C. § 78q(a)(1)).

[188] 31 C.F.R. § 1023.320.

[189] *Alpine Secs.* at 32.

[190] *Alpine Secs.* at 35-36.

[191] *Alpine Secs.* at 36.

[192] *Alpine Secs.* at 45. Alpine had argued that failure to file a SAR cannot give rise to liability; the court disagreed. *Id.* at 48.

[193] *Alpine Secs.* at 53 (citing 2002 SAR Form at 3). The court held that Alpine narratives did not comply with this requirement: "Alpine repeatedly used template narratives that failed to include any details, positive or negative, about the transactions. While a fulsome SAR narrative could present a question of fact as to whether the narrative was deficient, except in rare instances Alpine has not shown that its SAR narratives contained sufficient information to create a question of fact." *Id.* at 53-54.

[194] *Alpine Secs.* at 52.

[195] *Alpine Secs.* at 25 (citing SAR Narrative Guidance at 3–6; SAR Activity Review, Issue 22, at 39–40; 2012 SAR Instructions at 110–12). The court further explained: "FinCEN guidance refers to the who, what, where, when, and why, as the 'five essential elements' of a SAR narrative, but also adds that a sixth element, 'the method of operation['] (or how?)[,] is also important." *Id.* at 25 n.22 (citing SAR Narrative Guidance at 3).

[196] *Alpine Secs.* at 88-89.

[197] *Alpine Secs.* at 89.

[198] *Alpine Secs.* at 93-94.

[199] *Alpine Secs.* at 96-97 (citing 31 C.F.R. § 1023.320(b)(3)).

[200] *Alpine Secs.* at 97.

[201] *Alpine Secs.* at 97-99 (citing 31 C.F.R. § 1023.320(d); 17 C.F.R. § 240.17a-4).

[202] *Alpine Secs.* at 44.

[203] Press Release, US Dep't of Justice, *Rabobank NA Pleads Guilty, Agrees to Pay Over $360 Million* (Feb. 7, 2018), https://www.justice.gov/opa/pr/rabobank-na-pleads-guilty-agrees-pay-over-360-million.

[204] Press Release, OCC, *OCC Assesses $50 Million Civil Money Penalty and Terminates Consent Order Against Rabobank, N.A.* (Feb. 7, 2018), https://www.occ.gov/news-issuances/news-releases/2018/nr-occ-2018-15.html.

[205] Press Release, US Atty's Off., S.D.N.Y., *Manhattan U.S. Attorney Announces Criminal Charges Against U.S. Bancorp for Violations of the Bank Secrecy Act* (Feb. 15, 2018), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-criminal-charges-against-us-bancorp-violations-bank; Stipulation and Order of Settlement and Dismissal, *U.S. Dep't of the Treasury vs. U.S. Bank Nat'l Ass'n*, No. 18 Civ. 1358 (S.D.N.Y.) (Feb. 15, 2018), https://www.justice.gov/usao-sdny/press-release/file/1035071/download; *U.S. Bancorp Deferred Prosecution Agreement* (Feb. 12, 2018), https://www.justice.gov/usao-sdny/press-release/file/1035081/download.

[206] Samuel Rubenfeld, *Société Générale to Pay $1.3 Billion to Resolve U.S. Sanctions, Money-Laundering Violations*, WALL ST. J. (Nov. 19, 2018).

[207] Agreement Between UBS AG New York, New York and OCC, No. 2017-030 (Mar. 24, 2017), https://www.occ.gov/static/enforcement-actions/ea2017-030.pdf.

[208] *Bank of China, New York Branch*, No. AA-EC-2018-19, Consent Order for a Money Penalty (OCC Apr. 24, 2018), https://www.occ.gov/static/enforcement-actions/ea2018-038.pdf.

[209] Press Release, OCC, *OCC Assesses $100 Million Civil Money Penalty Against Capital One* (Oct. 23, 2018), https://www.occ.treas.gov/news-issuances/news-releases/2018/nr-occ-2018-112.html; *Capital One, N.A. & Capital One Bank (U.S.A.), N.A.*, No. AA-EC-2018-62, Consent Order (OCC Oct. 23, 2018), https://www.occ.gov/static/enforcement-actions/ea2018-080.pdf.

[210] Press Release, FRB, *Federal Reserve Board Announces $41 Million Penalty and Consent Cease and Desist Order Against Deutsche Bank AG* (May 30, 2017), https://www.federalreserve.gov/newsevents/pressreleases/enforcement20170530a.htm; *Deutsche Bank AG,* No. 17-009-B-FB, Order to Cease and Desist and Order of Assessment of a Civil Money Penalty, at 3 (FRB May 26, 2017), https://www.federalreserve.gov/newsevents/pressreleases/files/enf20170530a1.pdf.

[211] Press Release, FRB, *Federal Reserve Board Announces $41 Million Penalty and Consent Cease and Desist Order Against Deutsche Bank AG* (May 30, 2017), https://www.federalreserve.gov/newsevents/pressreleases/enforcement20170530a.htm; *Deutsche Bank AG,* No. 17-009-B-FB, Order to Cease and Desist and Order of Assessment of a Civil Money Penalty at 3 (May 26, 2017), https://www.federalreserve.gov/newsevents/pressreleases/files/enf20170530a1.pdf.

[212] Press Release, FRB, *Federal Reserve Board Announces $29 Million Penalty Against U.S. Operations of Mega International Commercial Bank Co., Ltd.* (Jan. 17, 2018), https://www.federalreserve.gov/newsevents/pressreleases/enforcement20180117a.htm; *Mega Int'l Commercial Bank Co., Ltd.*, No. 18-002-B-FB, Order to Cease and Desist and Order of Assessment of a Civil Money Penalty (FRB Jan. 17, 2018), https://www.federalreserve.gov/newsevents/pressreleases/files/enf20180117a1.pdf.

[213] Press Release, FRB, *Federal Reserve Board Issues Enforcement Action with BB&T Corporation* (Jan. 27, 2017), https://www.federalreserve.gov/newsevents/pressreleases/enforcement20170127a.htm; *BB&T Corp.*, No. 17-004-B-HC, Cease and Desist Order (FRB Jan. 25, 2017), https://www.federalreserve.gov/newsevents/pressreleases/files/enf20170127a1.pdf.

[214] Press Release, FRB, *Federal Reserve Issues Enforcement Action with Industrial and Commercial Bank of China Ltd.* (Mar. 13, 2018), https://www.federalreserve.gov/newsevents/pressreleases/enforcement20180313a.htm; *Industrial & Commercial Bank of China Ltd.*, No. 18-013-B-FB, Cease and Desist Order (FRB Mar. 12, 2018), https://www.federalreserve.gov/newsevents/pressreleases/files/enf20180313a1.pdf.

[215] Press Release, FinCEN, *FinCEN Penalizes Texas Bank for Violations of Anti-Money Laundering Laws Focusing on Section 312 Due Diligence Violations* (Nov. 1, 2017), https://www.fincen.gov/news/news-releases/fincen-penalizes-texas-bank-violations-anti-money-laundering-laws-focusing.

[216] Press Release, FinCEN, *FinCEN Penalizes Texas Bank for Violations of Anti-Money Laundering Laws Focusing on Section 312 Due Diligence Violations* (Nov. 1, 2017), https://www.fincen.gov/news/news-releases/fincen-penalizes-texas-bank-violations-anti-money-laundering-laws-focusing.

[217] Press Release, FinCEN, *FinCEN Penalizes California Bank for Egregious Violations of Anti-Money Laundering Laws* (Feb. 27, 2017), https://www.fincen.gov/news/news-releases/fincen-penalizes-california-bank-egregious-violations-anti-money-laundering-laws; *Merchants Bank of Cal., N.A.*, No. 2017-02, Assessment of Civil Money Penalty (FinCEN Feb. 16, 2017), https://www.fincen.gov/sites/default/files/enforcement_action/2017-02-27/Merchants%20Bank%20of%20California%20Assessment%20of%20CMP%2002.24.2017.v2.pdf.

[218] *Shinhan Bank America,* No. FDIC-16-0237b, Consent Order (June 12, 2017).

[219] Press Release, NYDFS, *DFS Fines Habib Bank and Its New York Branch $225 Million for Failure to Comply with Laws and Regulations Designed to Combat Money Laundering, Terrorist Financing, and Other Illicit Financial Transactions* (Sept. 7, 2017), http://www.dfs.ny.gov/about/press/pr1709071.htm.

[220] Press Release, NYDFS, *DFS Fines Western Union $60 Million for Violations of New York's Anti-Money Laundering Laws and for Ignoring Suspicious Transactions to Locations in China* (Jan. 4, 2018), https://www.dfs.ny.gov/about/press/pr1801041.htm.

[221] Press Release, NYDFS, *DFS Fines Deutsche Bank $425 Million for Russian Mirror-Trading Scheme* (Jan. 30, 2017).

[222] Press Release, US Dep't of Justice, *MoneyGram International Inc. Agrees to Extend Deferred Prosecution Agreement, Forfeits $125 Million in Settlement with Justice Department and Federal Trade Commission* (Nov. 8, 2018), https://www.justice.gov/opa/pr/moneygram-international-inc-agrees-extend-deferred-prosecution-agreement-forfeits-125-million.

[223] *See* Deferred Prosecution Agreement, *United States v. MoneyGram Int'l, Inc.*, No. 1:12-cr-00291 (M.D. Pa. Nov. 8, 2012), https://www.justice.gov/opa/press-release/file/1109461/download.

[224] *See* Amendment to and Extension of Deferred Prosecution Agreement, *United States v. MoneyGram Int'l, Inc.*, No. 1:12-cr-00291 (M.D. Pa. Nov. 8, 2018), https://www.justice.gov/opa/press-release/file/1109466/download.

[225] *See* Stipulated Order for Compensatory Relief and Modified Order for Permanent Injunction, *F.T.C. v. MoneyGram Int'l, Inc.*, No. 1:09-cv-6576 (N.D. Ill. Nov. 13, 2018), https://www.ftc.gov/system/files/documents/cases/moneygram_stipulated_order_11-13-18.pdf.

[226] *Western Union Fin. Servs., Inc.,* No. 2017-01, Assessment of Civil Money Penalty (FinCEN Jan. 19, 2017); Stipulated Order for Permanent Injunction and Final Order, *F.T.C. v. Western Union Co.,* No. 1:17-cv-0110 (M.D. Pa. Jan. 20, 2017), https://www.ftc.gov/system/files/documents/cases/western_union_consent_order_final_jan2017.pdf; *see also* Press Release, US Dep't of Justice, *Western Union Admits Anti-Money Laundering and Consumer Fraud Violations, Forfeits $586 Million in Settlement with Justice Department and Federal Trade Commission* (Jan. 19, 2017), https://www.justice.gov/opa/pr/western-union-admits-anti-money-laundering-and-consumer-fraud-violations-forfeits-586-million.

[227] *BTC-e a/k/a Canton Bus. Corp. & Alexander Vinnik,* No. 2017-03, Assessment of Civil Money Penalty (FinCEN July 26, 2017), https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-27/Assessment%20for%20BTCeVinnik%20FINAL2.pdf.

[228] FinCEN, FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

[229] FinCEN, FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, at 7 (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

[230] *See* Samuel Gibbs, *"Criminal Mastermind" of $4bn Bitcoin Laundering Scheme Arrested*, The Guardian (July 27, 2017), https://www.theguardian.com/technology/2017/jul/27/russian-criminal-mastermind-4bn-bitcoin-laundering-scheme-arrested-mt-gox-exchange-alexander-vinnik.

[231] *Eric Powers,* No. 2019-01, Assessment of Civil Money Penalty (FinCEN April 18, 2019), https://www.fincen.gov/sites/default/files/enforcement_action/2019-04-18/Assessment%20Eric%20Powers%20Final%20for%20Posting%2004.18.19_1.pdf.

[232] Press Release, US Atty's Off., S.D.N.Y., *Manhattan U.S. Attorney Announces Bank Secrecy Act Charges Against Kansas Broker Dealer*, (Dec. 19, 2018), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-bank-secrecy-act-charges-against-kansas-broker-dealer.

[233] *UBS Fin. Servs. Inc.*, No. 2018-03, Assessment of Civil Money Penalty (FinCEN Dec. 11, 2018), https://www.fincen.gov/sites/default/files/enforcement_action/2018-12-18/UBS%20Assessment%2012.17.2018%20FINAL_508%20Revised.pdf.

[234] *UBS Fin. Servs. Inc.*, Exch. Act Release No. 84,828, Administrative and Cease-and-Desist Order (SEC Dec. 17, 2018), https://www.sec.gov/litigation/admin/2018/34-84828.pdf.

[235] *UBS Fin. Servs. Inc. & UBS Securities LLC*, No. 2012034427001, Letter of Acceptance, Waiver and Consent (FINRA Dec. 17, 2018), http://www.finra.org/sites/default/files/UBS_AWC_121718.pdf.

[236] *See* SEC, Litigation Release No. 24189, *SEC Charges Charles Schwab with Failing to Report Suspicious Transactions* (July 9, 2018), https://www.sec.gov/litigation/litreleases/2018/lr24189.htm.

[237] *Valdes & Moreno, Inc.*, No. 2016048244301, Letter of Acceptance, Waiver and Consent (FINRA Apr. 26, 2017), http://www.finra.org/sites/default/files/fda_documents/2016048244301_FDA_JG412336.pdf.

[238] Press Release, FINRA, *FINRA Hearing Panel Fines C.L. King & Associates $750,000 for Negligent Misrepresentations and Omissions in Connection with Death Put Investments and AML-Related Violations* (Sept. 12, 2017), https://www.finra.org/newsroom/2017/finra-hearing-panel-fines-cl-king-associates-750000-negligent-misrepresentations-and; *Dep't of Enforcement v. C.L. King & Assoc., Inc.*, No. 2014040476901, Extended Hearing Panel Decision (FINRA Sept. 6, 2017), https://www.finra.org/sites/default/files/King_Miller_action_091217.pdf.

[239] *Revere Securities LLC*, No. 2014039396101, Letter of Acceptance, Waiver and Consent (FINRA Sept. 7, 2017), http://www.finra.org/sites/default/files/fda_documents/2014039396101_FDA_VA702409.pdf.

[240] *Alexander Capital, L.P.*, No. 2014039351101, Letter of Acceptance, Waiver and Consent (FINRA Sept. 29, 2017), http://www.finra.org/sites/default/files/fda_documents/2014039351101_AWC.pdf.

[241] *Dep't of Enforcement v. Elec. Trans. Clearing, Inc.*, No. 213037709301, Order Accepting Offer of Settlement (FINRA July 24, 2017), http://www.finra.org/sites/default/files/fda_documents/2013037709301_FDA_VA702292.pdf.

[242] *Artichoke Joe's d/b/a Artichoke Joe's Casino*, No. 2017-05, Assessment of Civil Money Penalty (FinCEN Nov. 15, 2017), https://www.fincen.gov/sites/default/files/enforcement_action/2017-11-17/AJC%20Proposed%20Assessment%20Signed%2011.15.17.pdf. *See also Artichoke Joe's d/b/a Artichoke Joe's Casino*, No. 2018-02, Assessment of Civil Money Penalty (FinCEN May 3, 2018), https://www.fincen.gov/sites/default/files/enforcement_action/2018-05-03/AJC%20Assessment%2005.03.18.pdf.

[243] *See* US Dep't of the Treasury, Civil Penalties and Enforcement Information, 2019 Enforcement Information, https://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx.

[244] *Standard Chartered Bank.*, Enforcement Information (OFAC Apr. 9, 2019), https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190408_scb_webpost.pdf.

[245] *Stanley Black & Decker*, Enforcement Information (Mar. 27, 2019), https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190327_decker.pdf.

[246] *Exxon Mobil Corp. v. Mnuchin*, Civ. No. 3:17-cv-1930 (N.D. Tex. July 20, 2017).

[247] SCB reached settlements with: the Board of Governors of the Federal Reserve System, the Federal Reserve Bank of New York, the US Department of Justice, Criminal Division, Money Laundering and Asset Recovery Section, the US Attorney's Office for the District of Columbia, the New York County District Attorney's Office, the New York State Department of Financial Services, and the United Kingdom's Financial Conduct Authority.

[248] Separate from the global settlement, SCB agreed to pay OFAC $18,016,283 to settle its potential civil liability for apparent violations of Zimbabwe-related sanctions.

[249] *Standard Chartered Bank*, Enforcement Information (Apr. 9, 2019), https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190408_scb_webpost.pdf.

[250] Press Release, US Dep't of the Treasury, OFAC, *Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Société Générale S.A.*, (Nov. 19, 2018), https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20181119_33.aspx.

[251] Press Release, NYDFS, *DFS Fines Société Générale SA and its New York Branch $420 Million for Violations of laws Governing Economic Sanctions and Violations of New York Anti-Money Laundering and Recordkeeping Laws* (Nov. 19, 2018), https://www.dfs.ny.gov/reports_and_publications/press_releases/1811191.

[252] *JPMorgan Chase Bank, N.A.*, Enforcement Information (OFAC Oct. 5, 2018), https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/jpmc_10050218.pdf.

[253] US Dep't of the Treasury, OFAC, *A Framework for OFAC Compliance Commitments* (May 2, 2019), https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf. Notably, OFAC issued the Compliance Framework several days after the US Department of Justice's Criminal Division released an updated version of its Evaluation of Corporate Compliance Programs guidance document for white-collar prosecutors evaluating corporate compliance program (the DOJ published the previous version of the guidance document in February 2017). OFAC's guidance thus appears to be part of a broader US government effort to clarify and convey to the private sector its expectations for an effective compliance program.

[254] Under Secretary Mandelker proceeded to identify the five components of compliance described above. *See* OFAC Press Release, Under Secretary Sigal Mandelker Remarks ABA/ABA Financial Crimes Enforcement Conference December 3, 2018 (Dec. 3, 2018), https://home.treasury.gov/news/press-releases/sm563.