WILMERHALE

REGULATORY AND GOVERNMENT AFFAIRS

April 27, 2017

AML and Sanctions: 2017 Trends and Developments

TABLE OF CONTENTS

I. Executive Summary

Over the past year, regulators continued to actively examine compliance, introduce new and heightened requirements, recalibrate global priorities, and aggressively pursue enforcement. This report reviews recent trends and developments impacting financial institutions with respect to the U.S. Bank Secrecy Act/Anti-Money Laundering (BSA/AML) and economic sanctions regulatory landscape.

It remains to be seen how the arrival of the Trump Administration will impact the government's approach and priorities in these areas. All current indications, however, are that BSA/AML and sanctions regulation are likely to remain a priority. Secretary of the U.S. Department of the Treasury (Treasury) Steven Mnuchin, for example, recently identified combating financial crime and terrorism financing as "core missions" of the Treasury in a statement supporting President Trump's discretionary budget proposal.[1] That proposal spares the Treasury's financial crime units from reduced funding.[2] In addition, other regulators at all levels continue to signal a sustained commitment to strengthening and policing the financial system's protections against financial crime.

Regulators in 2016 focused on strengthening anti-money laundering protections. A new BSA/AML rule intended to prevent criminals, kleptocrats, and others looking to hide ill-gotten proceeds from anonymously accessing the U.S. financial system was announced by the Financial Crimes Enforcement Network (FinCEN). The rule creates new requirements for customer due diligence and identification of beneficial owners—priorities that are likely to be at the top of the examination agenda, as compliance with the new rule becomes mandatory in 2018.

Other federal and state regulators also continue to play active roles. Prudential regulators focused on BSA/AML compliance in 2016, bringing over a half-dozen enforcement actions when significant deficiencies were identified. Securities regulators also focused on BSA/AML compliance in 2016, and have already signaled that BSA/AML issues will remain a priority for 2017. And at the state level, New York played a very active role in 2016 and appears poised to continue to do so with the rollout of new rules mandating certification of compliance with AML transaction monitoring and filtering program requirements, as well as new cybersecurity regulations.

Sanctions continue to play a central role in the U.S. government's response to geopolitical events, most prominently Iran's nuclear program, a deteriorated security situation in eastern Ukraine, and "normalized" relations between the United States and Cuba. Already in 2017, the Trump Administration has cautioned Iran that it is "on notice" concerning ballistic missile testing,[3] and followed that warning with new designations of individuals and entities related to those activities. While sanctions policy is always responsive to world events that can be difficult to predict, 2017 is likely to be an especially challenging year for companies seeking to identify the most relevant risks, requirements and trends likely to arise in this area of law.

As to enforcement, 2017 began with the resolution of significant enforcement actions involving both BSA/AML and sanctions violations that carried hefty penalties, included criminal charges, and were the result of parallel investigations by multiple regulators that have become the hallmark of enforcement in recent years. While the frequency and size of enforcement actions in 2016 were less than in recent years, the start of 2017 suggests the broader trend remains in the direction of continued intense scrutiny.

This report highlights the most notable BSA/AML and sanctions developments in 2016 and into the first quarter of 2017.

II. BSA/AML Regulatory Trends and Developments

The BSA/AML regulatory environment continued to evolve over the past year. Regulators addressed perceived weaknesses in the U.S. regulatory regime and other hot button issues, including a lack of transparency into the identities of beneficial owners behind accounts held by legal entities, the emerging threat posed by cybercriminals, and the de-risking of foreign correspondent accounts.

While the new Administration has signaled its intention to reduce the burden posed by financial regulation, there is little indication to date of significant plans to change course with respect to BSA/AML regulation. It therefore seems likely that regulators in the near term will continue to address transparency issues and cybersecurity, as well as other new threats that might emerge over the course of 2017. They may also respond to a number of reports and recommendations issued by lawmakers and industry groups in 2016.

To understand the issues that regulators are most likely to emphasize in the coming months, it is useful to review recent developments from last year. We begin with the most significant regulatory development of last year, which came from FinCEN—the Treasury's lead agency for combating money laundering and safeguarding the financial system from illicit use. In the first half of 2016, and in the wake of the "Panama Papers," FinCEN released much-anticipated **new rules for customer due diligence and the identification of beneficial ownership**—two priorities that are likely to remain at the top of the regulatory agenda for 2017.

Other notable developments at FinCEN include the issuance of geographic targeting orders focusing on identifying individuals behind high-end real estate; new guidance on cybersecurity; and a proposal to extend Customer Identification Program and AML requirements to banks lacking a federal functional regulator. Since Jennifer Shasky Calvery's departure from FinCEN's top post in May 2016, the agency has been operating under the interim leadership of Acting Director Jamal El-Hindi, who previously served as deputy director and head of FinCEN's Policy Division.

At the state level, New York continues to play an active role. **New York State's Department of Financial Services** (NYDFS), under the leadership of Maria T. Vullo, who took the helm from Benjamin Lawsky in 2016, appears committed to carrying forward New York's aggressive regulatory and enforcement posture. NYDFS issued new rules requiring certification of compliance with AML transaction monitoring and filtering program requirements, consistent with the desire to hold individuals accountable for compliance failings. Also notable—given the increasing convergence between AML and cybersecurity issues—is NYDFS's promulgation in February 2017 of new cybersecurity regulations requiring regulated financial institutions to establish and maintain cybersecurity programs.

Over the past year, we have seen a dramatic **convergence of AML and cybersecurity** and expect this trend to continue in 2017. Traditionally, financial institutions have approached cybersecurity and AML compliance separately, with different personnel and reporting lines. However, U.S. regulators now expect that financial institutions take a holistic approach to cyberthreats and incorporate such information into Suspicious Activity Reports (SARs) filed pursuant to the institution's BSA obligations. Notably, in October 2016, the federal banking regulators issued a joint advance notice of proposed rule-making on cybersecurity regulations and efforts to improve the safety and soundness of the U.S. financial system.[4]

Given the increased regulatory scrutiny at the state and federal levels, financial institutions should ensure that their cybersecurity and AML compliance personnel understand when to escalate a cyber-event to AML compliance and the information needed to satisfy the relevant reporting requirements.

In 2016, **securities regulators also continued to focus on AML compliance**. Both the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) already have announced an intention to make AML a priority in 2017. Last year was also characterized by a number of **significant policy developments** that are reviewed in more detail below: Congress devoted particular attention to the threat that terrorist financing poses to the U.S. financial system; the Financial Action Task

Force (FATF) released its "mutual evaluation" assessing the strength of the U.S. regime to combat money laundering and terrorist financing; and The Clearing House called for a paradigm shift to redesign the U.S. approach to AML to better protect national security and aid law enforcement.

The following is a discussion of the key BSA/AML regulatory developments in 2016 and early 2017.

A. Treasury and FinCEN

1. New Requirements for Customer Due Diligence and Identification of Beneficial Owners

FinCEN, on May 11, 2016, released its long-awaited Final Customer Due Diligence Rule (CDD Rule) that will require certain financial institutions to "look through" nominal legal entity account holders to identify the account's beneficial owners who own or control the entity.[5] The rule also explicitly establishes a "fifth pillar" in FinCEN's AML program requirement mandating that certain institutions implement risk-based procedures for conducting customer due diligence (CDD) on all customers. Compliance with the CDD Rule becomes mandatory on May 11, 2018.

The CDD Rule is intended to prevent criminals, kleptocrats and others looking to hide ill-gotten proceeds from accessing the financial system anonymously. FinCEN's announcement of the final rule last year was the culmination of an extensive, six-year rule-making process and a key step in the U.S. government's ongoing efforts to combat money laundering, terrorist financing and tax evasion on the heels of the Panama Papers. Publication of the final rule coincided with calls for Congress to adopt legislation that would require the collection of beneficial ownership information at the time legal entities are formed in the United States.[6]

The U.S. Department of Justice (DOJ) recently underscored its support for the new rule, explaining that the Criminal Division "remain[s] sharply focused on understanding the ownership structure and the apparent ease with which criminal organizations and individuals use shell companies to move and ultimately conceal criminal proceeds." The acting head of the Criminal Division recently described the rule "as a critical step toward greater transparency" and emphasized DOJ "will be taking a hard look at compliance with this rule in the course of our future investigations."[7]

The CDD Rule addresses a weakness in the U.S. AML regime identified by the FATF in its "mutual evaluations" of the United States[8]—namely, shortcomings with respect to the identification and verification of the individuals associated with legal entity customers. The rule does so by requiring the identification of the "beneficial owners" of legal entity customers. Beneficial owners are defined as each individual who owns 25 percent or more of the entity, and a single individual who has significant responsibility for controlling the entity.

In addition to its beneficial ownership requirement, the CDD Rule includes CDD standards for covered financial institutions subject to AML program requirements. The so-called "fifth pillar," which, according to FinCEN, merely formalizes existing practice, will require covered financial institutions to establish risk-based procedures to understand the "nature and purpose of the customer relationship," and to conduct ongoing monitoring to identify and report suspicious transactions and update customer information. FinCEN emphasized that the fifth pillar does not require a continuous or periodic refresh of customer information. Rather, an institution must update customer information, including beneficial ownership, if during its normal monitoring it detects information relevant to assessing or reevaluating customer risk.

The CDD Rule applies only to "covered financial institutions": banks, broker-dealers, mutual funds, futures commission merchants, and commodities introducing brokers, which are already subject to Customer Identification Program (CIP) requirements. FinCEN has also emphasized that the CDD Rule's provisions are a "floor, not a ceiling," suggesting that it may be appropriate for institutions to do more than the minimum required by the CDD Rule in circumstances of heightened risk.

Key Takeaways

- ***Updates to Existing CDD Programs.*** Many covered financial institutions already collect some beneficial ownership information and have updated their AML policies and procedures in anticipation of the CDD Rule. However, all covered financial institutions should revisit their policies, procedures and training materials to ensure their current practices meet the requirements of the CDD Rule by the May 2018 compliance deadline. While FinCEN asserts that the "fifth pillar" provisions are not new requirements, covered financial institutions may find that their procedures do not actually incorporate these expectations.

- ***CDD Expectations for Non-Covered Financial Institutions.*** Non-covered financial institutions with SAR responsibilities may want to consider establishing some form of risk-based customer due diligence processes. FinCEN and other federal functional regulators have emphasized that customer due diligence is a key input in SAR monitoring and analysis. And FinCEN's stated position that the "fifth pillar" merely formalizes existing expectations suggests that these expectations may be broadly applicable across FinCEN-regulated entities and not just applicable to covered financial institutions.

- ***Trigger-Based Updates.*** Also, while FinCEN expects financial institutions to conduct a "monitoring-triggered" update of customer information, it did not specify which triggers should be used. For example, FinCEN or prudential regulators may expect triggers to capture a change in ownership of a legal entity customer. Covered financial institutions may find themselves subject to criticism for a "silo effect" if salient information for purposes of ongoing monitoring is not effectively communicated from all relevant aspects of the firm to the AML compliance function. (This has been a frequent regulatory criticism with respect to institutions' SAR programs.)

- ***Financial Intermediaries.*** SAR monitoring should not necessarily stop at the level of the legal entity customer, notwithstanding the fact that the CDD Rule states that intermediaries may be treated as legal entity customers under certain circumstances. In fact, failure to monitor or report underlying customer activity in intermediated accounts can attract regulatory scrutiny and lead to enforcement actions.[9]

- ***Leveraging CDD for Other Compliance Efforts.*** One of the stated benefits of the CDD Rule is that it may serve to enhance financial institutions' compliance efforts in the areas of Office of Foreign Assets Control (OFAC) sanctions, currency transaction reporting requirements, tax and others. Covered financial institutions should assess the information flow among their new or updated CDD controls and the groups responsible for these other compliance requirements.

For additional details, refer to our Client Alert: FinCEN Finalizes Beneficial Ownership and Customer Due Diligence Requirements.

2. FinCEN Focuses on High-End Real Estate

In 2016, FinCEN turned its attention to the money laundering risks posed by high-end real estate. On January 13, 2016, FinCEN issued two Geographic Targeting Orders (GTOs), temporarily requiring certain title insurance companies to report the identities of the natural persons behind companies paying cash for high-end residential real estate in Manhattan and Miami-Dade County.[10] The GTOs were applicable to residential properties with a sale price of over $1 million in Miami-Dade and over $3 million in Manhattan. They were motivated by FinCEN's concern that individuals purchasing high-end residential real estate through limited liability companies or other legal entities and without bank financing might be trying to disguise their identity and hide assets.

The issuance of the GTOs marked the first time that the federal government required real estate companies to disclose the names of individuals behind cash transactions. Information gathered pursuant to the GTOs will be stored in a FinCEN database intended to help law enforcement identify the natural persons involved in transactions vulnerable to money laundering abuse.

The GTOs are part and parcel of a recent increase in law enforcement scrutiny of the real estate industry. The issuance of the GTOs brings the United States more in line with the United Kingdom, where real estate agents are required to submit SARs to the government when they suspect a transaction involves funds from a criminal source.

In August 2016, FinCEN extended the GTOs to six major U.S. geographic areas: (1) all boroughs of New York City; (2) Miami-Dade County, Florida, and the two counties immediately north (Broward and Palm Beach); (3) Los Angeles County, California; (4) three counties comprising part of the San Francisco area (San Francisco, San Mateo and Santa Clara counties); (5) San Diego County, California; and (6) the county that includes San Antonio, Texas (Bexar County).[11]

In February 2017, FinCEN renewed the GTOs for a period extending 180 days from February 24, 2017. In its press release announcing the renewal of the GTOs, FinCEN noted: "[A]bout 30 percent of the transactions covered by the GTOs involve a beneficial owner or purchaser representative that is also the subject of a previous SAR. This corroborates FinCEN's concerns about the use of shell companies to buy luxury real estate in 'all-cash' transactions."[12]

FinCEN may further increase regulatory or criminal enforcement actions in the real estate field in 2017. Depending on the results of these GTOs, it is also possible that FinCEN and other regulators may further expand AML compliance requirements in the real estate sector.

3. FinCEN Guidance on E-Mail Compromise Fraud Schemes and Cyber-Events

a) FinCEN Issues Guidance on E-Mail Compromise Fraud

On September 6, 2016, FinCEN issued an advisory to help financial institutions guard against e-mail fraud schemes wherein criminals misappropriate funds by deceiving financial institutions and their customers into conducting wire transfers.[13] FinCEN warned against two main types of e-mail compromise frauds:

- Business E-mail Compromise (BEC), which targets a financial institution's commercial customers; and

- E-mail Account Compromise (EAC), which targets a victim's personal accounts.

BEC and EAC schemes are part of a growing trend of cyber-enabled crime affecting financial institutions. Since 2013, there have been approximately 22,000 reported cases of BEC and EAC fraud involving $3.1 billion.

FinCEN notes that both BEC and EAC schemes typically have three stages:

- First, criminals unlawfully access a victim's e-mail account through social engineering (e.g., by tricking the victim into revealing information) or computer intrusion techniques. Criminals then exploit the victim's e-mail account to obtain information about the victim's financial institutions and account details.

- Second, criminals use the victim's stolen information to e-mail fraudulent wire transfer instructions to the financial institution in a manner appearing to be from the victim. Either the criminal will use the victim's actual e-mail account or will create a fake e-mail account that resembles the victim's actual one, inserting an underscore between the first and last names instead of a dot, for example.

- Third, the criminal will trick the victim's financial institution into conducting unauthorized wire transfers that appear legitimate. The fraudulent transaction instructions direct the wire transfer to the criminal's domestic or foreign bank accounts.[14]

Key Takeaways

- Companies should be on alert for the red flags[15] indicative of BEC and EAC fraud including:
    - A customer's seemingly legitimate e-mailed transaction instructions contain different language, timing, and amounts than previously verified and authentic transaction instructions.
    - Transaction instructions originate from an e-mail account closely resembling a known customer's e-mail account; however, the e-mail address has been slightly altered by adding, changing, or deleting one or more characters.
    - E-mailed transaction instructions direct payment to a known beneficiary; however, the beneficiary's account information is different from what was previously used.
- Financial institutions are encouraged to report unauthorized wire transfers to the FBI or U.S. Secret Service within 24 hours to increase the chances of recovering stolen funds.
- In addition to notifying these agencies, a financial institution may be required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, like a BEC. When filing a SAR, financial institutions should provide all pertinent available information, including cyber-related information in the SAR form and narrative.

b) FinCEN Guidance on Cyber-Events and Cyber-Enabled Crimes

On October 25, 2016, FinCEN issued an advisory to financial institutions on when to file SARs on cyber-events and cyber-enabled crimes.[16] FinCEN noted that financial institutions should include available IP addresses and accompanying timestamps associated with fraudulent wire transfers being reported, even if a cyber-event was not involved in the suspicious activity. And when suspicious transactions do involve cyber-events, FinCEN advised financial institutions to include in SARs all relevant and available information regarding the suspicious transactions and the cyber-event, including the type, magnitude, and methodology of the cyber-event, and the signatures that suggest a cyber intrusion.

Financial institutions are not required to file SARs reporting the continuous scanning or probing of their systems or networks, but should file a SAR where an otherwise reportable cyber-event has been unsuccessful. Financial institutions should encourage collaboration between their AML compliance personnel and cybersecurity personnel to efficiently detect and report cyber-events.

4. In Response to De-Risking, Regulators Issue Joint Fact Sheet on Foreign Correspondent Banking

De-risking continues to be a hot topic of conversation at gatherings of AML professionals and regulators. De-risking occurs when financial institutions withdraw from certain business lines or countries that they deem too risky from an AML or sanctions perspective and can have, among other consequences, the ultimate impact of driving transactions out of the well-regulated financial systems and away from the watchful eyes of regulators and law enforcement. De-risking is of particular concern to those engaged in foreign correspondent banking. In light of high compliance costs and regulatory scrutiny, banks have become reluctant to maintain correspondent accounts for foreign financial institutions (FFIs) from certain high-risk countries.

On August 30, 2016, the Treasury and the federal banking agencies[17] issued a Joint Fact Sheet on Foreign Correspondent Banking (and corresponding Blog post) in an effort to dispel two myths about U.S. supervisory expectations that presumably drive de-risking. The Joint Fact Sheet clarifies: (1) that there is no general expectation that U.S. banks conduct due diligence on the customers of their FFI customers (i.e., no requirement to know their customers' customers); and (2) that the AML and OFAC enforcement regime is not one of "zero tolerance."[18]

Under Section 312 of the USA PATRIOT Act and its implementing regulation, U.S. depository institutions are required to assess the money laundering risk presented by their foreign correspondent accounts. Such assessments must take into account: (1) the nature of the FFI's business and the markets it serves; (2) the type, purpose, and anticipated activity of the account; (3) the nature and duration of the account relationship; (4) the supervisory regime of the jurisdiction in which the FFI is licensed; and (5) information about the FFI's AML record.[19] Although the Joint Fact Sheet states that there is currently no requirement for U.S. depository institutions to conduct due diligence on an FFI's customers, banks should consider whether the due diligence information provided by their FFI customers is sufficient to fully assess the AML and sanctions risks posed by the foreign correspondent banking relationship. U.S. depository institutions may have to request additional information about the underlying activity in an FFI's account in order to satisfy their risk-based obligations under Section 312.

Financial institutions should also note that the Joint Fact Sheet reflects the views only of the Treasury and the federal banking agencies and not that of DOJ, state and local law enforcement; state banking regulators; or securities regulators, all of whom play an important role in the AML and OFAC enforcement regime.

5. Proposal to Extend CIP and AML Program Requirements to Banks Lacking a Federal Functional Regulator

On August 25, 2016, FinCEN proposed a rule that would conform the AML program obligations of banks not regulated by a federal functional regulator to those of banks that are regulated by a federal functional regulator.[20] The proposed rule would require banks lacking a federal functional regulator to establish and maintain an AML program that includes, at a minimum, the same five pillars as a traditional AML program: (1) internal controls; (2) independent testing; (3) a designated compliance officer; (4) training for appropriate personnel; and (5) risk-based procedures for conducting appropriate ongoing customer due diligence. In addition, the proposed rule would extend to these banks requirements to establish and implement a Customer Identification Program and to identify the beneficial owners of legal entity customers.

Banks without a federal functional regulator include state-chartered non-depository trust companies, non-federally insured credit unions, private banks, non-federally insured state banks and savings associations, and international banking entities. If finalized as proposed, the rule would fill a gap in the AML regime and subject banks, regardless of whether they have a federal functional regulator, to the full panoply of AML requirements.

Because banks without a federal functional regulator are already covered by other Bank Secrecy Act recordkeeping and reporting obligations, FinCEN anticipates that they will be able to leverage existing policies, procedures and internal controls to comply with the proposed obligations. If the rule is finalized, these banks should revise their existing AML policies, procedures, and internal controls to conform with the new minimum standards.

6. Leadership Changes

Treasury and FinCEN also saw recent leadership changes. On February 13, 2017, the Senate confirmed Steven Mnuchin as Secretary of the Treasury. In his written responses to questions posed by the Senate Finance Committee, Mnuchin, a former Goldman Sachs banker and Hollywood film financier, acknowledged the "serious challenges" law enforcement faces when it is unable to determine the beneficial ownership of companies that utilize the U.S. financial system. He pledged to work with

Congress and the various entities impacted by FinCEN's new customer due diligence requirements (discussed above) to address these challenges.[21]

In May 2016, Jennifer Shasky Calvery stepped down as director of FinCEN. A former prosecutor, Shasky served as director since September 2012. During that time, FinCEN overhauled its enforcement division and focused the agency's enforcement authority on certain non-bank financial institutions including casinos, money transmitters and fintech companies. Since Shasky's departure, FinCEN has been led by Acting Director Jamal El-Hindi, who previously led FinCEN's policy division and served as deputy director. A new director has not yet been appointed.

B. New York Department of Financial Services

In light of the Trump Administration's stated intention to roll back federal regulations,[22] we see the potential for increased activity by state regulators and attorneys general as they step in to fill perceived gaps in regulation and enforcement. New York, in particular, appears poised to continue to play an active role with respect to institutions that fall within its jurisdiction.

The head of NYDFS, Superintendent Maria Vullo, recently expressed her view that states are "well-positioned" to respond to any uncertainty at the federal level and emphasized that "whatever happens, we're going to continue to do our job in New York."[23] Superintendent Vullo, who was appointed last year by New York Governor Andrew Cuomo, has also indicated that New York supervisors will continue to aggressively review firms for compliance with BSA/AML obligations, cybersecurity rules and other mandates within the purview of NYDFS.[24]

Looking back at 2016, NYDFS appears well-positioned to do so. It continued to play an active role in enforcement, assessing several of the largest AML penalties of the year. On the regulatory front, NYDFS announced new rules requiring certification of compliance with state AML laws, which went into effect at the start of this year. And in February of this year, NYDFS finalized a first-in-the-nation cybersecurity regulation for financial institutions. These developments are described in more detail below.

1. NYDFS Issues Rule Requiring Certification of Compliance With AML Transaction Monitoring and Filtering Program Requirements

New York has taken the initiative in codifying regulatory expectations for transaction monitoring and filtering programs.

On June 30, 2016, NYDFS finalized a regulation requiring certification of compliance with AML transaction monitoring and filtering program requirements.[25] The regulation imposes three main requirements on New York-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 accountable for an institution's perceived AML and sanctions program failures. The regulation took effect January 1, 2017, and the initial certification is due to NYDFS on April 15, 2018.

The regulation creates specific state-level obligations for AML and sanctions compliance, areas that have traditionally been left to federal oversight. In some respects, the new rule goes beyond federal law, which has never codified the specific requirements of an AML transaction monitoring or sanctions filtering program in such detail.

On its face, the regulation applies only to the following entities that are subject to NYDFS AML regulations:

- all banks, trust companies, private bankers, savings banks, and savings and loan associations chartered under the New York Banking Law;

- all branches and agencies of foreign banking corporations licensed under the New York Banking Law to conduct banking operations in New York; and

- all check cashers and money transmitters licensed under New York Banking Law.

However, the practical effect of the rule may be even broader. For large banking organizations that include an institution regulated by NYDFS (such as international banks with a New York branch) and that have enterprise-wide AML monitoring and sanctions filtering systems, the system requirements in the rule could indirectly apply to entities not directly covered by the regulation, such as broker-dealers.

The regulation requires regulated institutions to establish and maintain a transaction monitoring program and a filtering program.

Transaction Monitoring Program. Regulated institutions are required to maintain a reasonably designed transaction monitoring program (either manual or automated) to monitor for potential violations of the BSA and to comply with their suspicious activity reporting obligations. A reasonably designed program should be based on the institution's risk assessment and include the attributes specified in the regulation, to the extent they are applicable.

Filtering Program. Regulated institutions are required to maintain a manual or automatic filtering program reasonably designed to interdict transactions prohibited by OFAC sanctions programs. In response to industry comments, the rule substituted a reasonableness standard for what appeared to be strict liability under the proposed rule. Like the transaction monitoring program, the filtering must also be based on the institution's risk assessment and include the attributes specified in the regulation, to the extent they are applicable.

Certification. The rule states that a "lack of robust governance, oversight, and accountability at senior levels" contributed to the risk that financial institutions do not detect money laundering and other criminal activity.[26] To address this issue, the rule requires regulated institutions to adopt either an annual board resolution, signed by each director, or a senior officer "compliance finding" to certify compliance. This requirement reflects a continuing trend by NYDFS and federal regulators toward holding executives accountable for AML failures. The regulation does not clarify whether a single person can satisfy the certification requirement or whether multiple signers may be required to cover all relevant areas.

Notably, the certification lacks a materiality standard, unlike the certification requirement of Sarbanes-Oxley. The board or senior officer must certify that the systems comply with the substantive and subjective requirements for AML transaction monitoring and filtering programs, not just that they are reasonably designed to detect money laundering and to block sanctioned transactions.

Although the regulation does not expressly reference criminal penalties, it states that it will be enforced pursuant to NYDFS's "authority under any applicable laws." NYDFS retains the authority to impose civil monetary and equitable sanctions and to refer matters to the New York attorney general for additional civil or criminal enforcement.[27]

For additional details, refer to our Client Alert: NYDFS Issues Final Rule Requiring Certification of Compliance With AML Transaction Monitoring and Filtering Program Requirements.

2. NYDFS Issues Cybersecurity Regulations for Financial Institutions

New York has also taken a leading role in promulgating a first-in-the-nation cybersecurity regulation applicable to banks, insurance companies, and certain other financial institutions regulated by NYDFS.[28] Entities covered by the regulation will have 180 days from the effective date (March 1, 2017) to come into compliance with most requirements, though certain provisions allow up to two years after the effective date.[29]

First proposed in September 2016 and revised after two rounds of public comment, the regulation establishes requirements that in some respects duplicate federal data security obligations for financial institutions, but in some important respects differ from and go beyond federal requirements. Notably, the regulation defines "Nonpublic Information" more broadly than the definition of "customer information" under the federal Interagency Guidelines Establishing Information Security Standards.[30]

The regulation imposes (1) obligations to report cybersecurity incidents to NYDFS; (2) an annual certification requirement concerning compliance with the regulation; (3) requirements concerning oversight of third-party service providers; (4) obligations concerning use of multifactor authentication and encryption; and (5) requirements concerning audit trail maintenance and document destruction.

For additional details, refer to our Client Alert: New York Finalizes Cybersecurity Regulations for Financial Institutions.

C. SEC and FINRA Examination Priorities for 2017

The SEC and FINRA have announced their examination priorities for 2017, and AML continues to be a focus for both securities industry regulators.[31]

The SEC's priorities for 2017 are similar to last year's priorities. They include assessing:

- whether broker-dealers' AML programs are tailored to specific risks;
- how broker dealers monitor for suspicious activity;
- the effectiveness of independent testing; and
- compliance with SAR requirements, including the timeliness and completeness of SARs.[32]

Whereas the SEC specifically cited AML examinations of clearing and introducing brokers in its 2016 priorities letter, there was no mention of clearing or introducing brokers in the AML section of the 2017 priorities letter.

FINRA will also continue to focus on AML in 2017, especially on areas where they "have observed shortcomings," including gaps in surveillance systems caused by data integrity problems, poorly set parameters and surveillance patterns that do not capture potentially suspicious activity.[33] In particular, FINRA will continue to focus on microcap activity. It will also focus on foreign currency transactions and transactions that flow through suspense accounts, as well as controls around accounts held by nominee companies. FINRA noted that firms may perform AML monitoring using the same trade surveillance systems they use for supervisory purposes; but if they do, those systems must also monitor for the firm's AML red flags.

D. Congress: The U.S. House Financial Services Committee

Congress is also playing an active role in exploring AML issues and proposing potential new measures. In 2016, the 114th Congress held hearings and introduced several bills pertaining to AML that are likely to serve as a starting place for the 115th Congress to revisit existing policies, assess effectiveness, and propose potential changes.

On December 20, 2016, the U.S. House Financial Services Committee's Task Force to Investigate Terrorism Financing released a bipartisan report, Stopping Terror Finance: Securing the U.S. Financial Sector, in connection with the culmination of its two-year investigation into the threats posed by terror financing to the U.S. financial system.[34] The Task Force, composed of 21 committee members, held 11 hearings from a range of expert witnesses on the terrorist financing threat and current response efforts. Topics included the nexus between terrorism, corruption and transnational crime; Iran's terrorist financing

capabilities; and terrorist financing methodologies. Based on the hearings, the Report details terrorist financing methods, key terrorist financiers such as ISIS and Boko Haram, the historical and current U.S. policy responses to terrorist financing, and methods of moving terrorist proceeds.

The Report's long-term recommendations include improved interagency coordination and efficiency, enhanced leveraging of suspicious activity reports and information flow between government and industry, an increased number of Treasury attachés internationally, continued focus on helping developing countries combat financial crimes, and a dedication to end trade-based money laundering, among other government and policy-driven initiatives.

Prior to the Report's publication, Task Force leaders introduced a package of five bills, none of which were passed before the end of the 114th Congress, but which may serve as a starting point for future legislation. The bills are summarized below:

- **H.R. 5594**, the "National Strategy for Combating Terrorist, Underground, and Other Illicit Financing Act," was sponsored by Task Force Chairman Michael Fitzpatrick (R-PA) and Reps. Kyrsten Sinema (D-AZ) and Nydia Velazquez (D-NY). The bill would require the President, acting through the Treasury Secretary, to develop and publish an annual whole-of-government strategy to combat money laundering and terrorist financing. The bill passed the House on July 11, 2016, by voice vote. The Senate took no action.

- **H.R. 5602**, sponsored by Task Force Ranking Member Stephen Lynch (D-MA) and Rep. Peter King (R-NY), required more detailed information to be reported to the Treasury regarding certain types of transactions in a specific area for a limited amount of time. The bill passed the House on July 11, 2016, by a vote of 356-47, and passed the Senate December 10, 2016, with an amendment by voice vote. The House did not act on the Senate amendment prior to adjournment.

- **H.R. 5607**, the "Enhancing Treasury's Anti-Terror Tools Act," was sponsored by Task Force Vice Chairman Robert Pittenger (R-NC) and Ranking Member Lynch (D-MA). The bill would enhance Treasury's anti-illicit finance tools by addressing issues that came up repeatedly in Task Force hearings. The bill passed the House on July 11, 2016, by a vote of 362-45. The Senate took no action.

- **H.R. 5603**, the "Kleptocracy Asset Recovery Rewards Act," was sponsored by Ranking Member Lynch (D-MA) and Rep. Keith Rothfus (R-PA). The bill would establish a reward program aimed at helping the U.S. identify, freeze, and, if appropriate, repatriate assets linked to foreign government corruption, which is often an enabler of terrorism. The bill saw no action.

- **H.R. 5606**, the "Anti-Terrorism Information Sharing Is Strength Act," was sponsored by Vice Chairman Pittenger (R-NC) and Financial Services Committee Ranking Member Maxine Waters (D-CA). The bill would refine "safe harbors" for the sharing of anti-terror information, reaffirming congressional intent in an existing statute that encourages the government to share terror methodologies with banks to help them better recognize such activity. The House tried to pass the bill under suspension of the rules (a procedure typically reserved for quick consideration of non-controversial legislation), but it failed to obtain the two-thirds vote needed to pass. The House took no further action.

Building off the work done by the Task Force, the House Financial Services Committee created a new Subcommittee on Terrorism and Illicit Finance to assist the new Administration in identifying ways to end terrorist financing. The subcommittee is chaired by Representative Stevan Pearce (R-NM). Ed Perlmutter (D-CO) is the ranking member.

E. FATF Mutual Evaluation of the United States

The Financial Action Task Force is an independent, intergovernmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. On December 1, 2016, the FATF published its Mutual Evaluation Report of the United States.[35] The Report presents a detailed assessment of the anti-money laundering and combating the financing of terrorism (AML/CFT) measures in place in the United States as of early 2016, when the FATF conducted its on-site visit.[36] The FATF's mutual evaluations influence U.S. regulatory policy by identifying deficiencies in the AML/CFT regime. The 2006 mutual evaluation, which concluded that the United States was non-compliant with FATF standards regarding beneficial ownership, spurred efforts to strengthen beneficial ownership standards, including FinCEN's promulgation of the CDD Rule, discussed above.

The generally positive 2016 Mutual Evaluation Report recognizes the overall effectiveness of the U.S. AML/CFT regime at combating money laundering and terrorist financing, and credits the robust supervision of the banking and securities sectors while acknowledging the strong supervisory focus placed on the casino industry in recent years. The Report also identifies several weaknesses in the U.S. AML/CFT regime, including the lack of a requirement to disclose to the government the identity of beneficial owners of a company when the company is formed and there is minimal AML/CFT regulatory coverage of investment advisers, lawyers, accountants, real estate agents, and trust and company service providers (other than trust companies).

In addition to a narrative assessment of U.S. AML/CFT measures, the Report contains discrete ratings of the United States' effectiveness and of its technical compliance with the FATF's 40 Recommendations. The FATF gave the United States high ratings on four of the eleven effectiveness ratings (namely those relating to asset forfeiture, combating terrorist financing, and counter-proliferation sanctions). On technical compliance with the 40 Recommendations, the FATF rated the United States fully compliant with nine recommendations, largely compliant with 21 recommendations, partially compliant with six recommendations, and non-compliant with four recommendations. The scoring reflects the fact that U.S. AML/CFT laws and regulations do not always align with the corresponding FATF recommendations.

Key Takeaways

- ***Beneficial Ownership.*** Perhaps the most significant gap in the U.S. AML/CFT framework, according to the Report, is the lack of transparency into the beneficial ownership of legal persons. Despite the known money laundering risk posed by legal persons and arrangements, gaps in the U.S. legal framework impede law enforcement's timely access to beneficial ownership information.[37] The CDD Rule, discussed above, will likely address some, but not all, of the FATF's concerns regarding beneficial ownership. The Report recommended that the United States take steps to ensure that beneficial ownership information of U.S. legal persons is timely made available to authorities by (1) requiring its collection at the federal level; and (2) requiring states to gather beneficial ownership information at the incorporation stage. Implementation of these recommendations would require legislative action by Congress and state legislatures.

- ***Investment Advisers.*** The Report recommended applying AML/CFT obligations to investment advisers. While some investment advisers are indirectly covered through their association with banks, bank holding companies, and/or broker dealers, investment advisers that operate outside the AML/CFT regime present a significant vulnerability. Applying AML rules to investment advisers directly would better address the vulnerability. FinCEN's proposed investment adviser rule was pending at the time of the FATF on-site visit, and is still pending.

- ***Other Under-Supervised Sectors.*** The Report identified oversight gaps for non-financial businesses and professions with the notable exception of casinos and dealers in precious metals and stones, which are subject to AML requirements. The Report recommended that the United States conduct a vulnerability analysis of the non-financial businesses and professions to consider what measures could be introduced to address the higher risks to which these sectors

are exposed. On the basis of that analysis, the Report recommended that the United States consider applying AML/CFT obligations to lawyers, accountants, and trust and company service providers (other than trust companies).

- ***State-Level Monitoring.*** Finding no uniform state-level AML efforts, the Report recommended that the United States improve the visibility of state-level AML activities and statistics, including through improved data-sharing. Enhanced collection of state-level money laundering investigations would allow federal authorities to better assess whether law enforcement activities at the state and local levels are consistent with federal AML/CFT priorities.

- ***Section 314 Information Sharing Program.*** Section 314 of the USA PATRIOT Act facilitates information exchange among financial institutions and between financial institutions and government authorities. The Report noted the importance of the Section 314 authorities and encouraged FinCEN to expand its use of Section 314(a), which allows federal, state, local, and foreign law enforcement agencies to reach out, through FinCEN, to points of contact at tens of thousands of financial institutions to locate accounts and transactions of persons that may be "engaged in or reasonably suspected . . . of engaging in terrorist acts or money laundering activities," with respect to a particular criminal investigation.[38]

- ***SAR Timing and Thresholds.*** The Report found that there were technical gaps that limited the information available to competent authorities at any given time, including the application of reporting thresholds for SARs. The Report recommended a focused risk review of the existing SAR reporting thresholds and the 30/60-day window in which to report suspicious activity. The Report also recommended that FinCEN issue guidance to clarify the scope of the immediate SAR reporting requirement to make clear that the requirement to immediately notify law enforcement of certain urgent circumstances, such as terrorist activity or ongoing money laundering, applies even below the otherwise applicable thresholds. In sum, the Report may be a chance for FinCEN to revisit these thresholds and expand certain SAR programs.

F. The Clearing House Advocates AML Reform

On February 16, 2017, The Clearing House, a banking trade association, published a report advocating a series of reforms to the U.S. AML/CFT regime. The report, titled "A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement," is the product of two closed-door symposia that convened approximately 60 leading experts from government, industry and academia to identify problems with the current regime and review potential solutions.[39]

The Clearing House notes in the report that U.S. financial firms, which are effectively deputized to identify and report money laundering and terrorist financing, spend billions of dollars each year on AML compliance, yet "many if not most of the resources devoted to AML/CFT by the financial sector have limited law enforcement or national security benefit" and may in fact damage other vital interests.[40]

The report identifies the following reforms for immediate action:

- The Treasury, through its Office of Terrorism and Financial Intelligence (TFI), should take a more prominent role in coordinating AML/CFT policy across the government.

- FinCEN should reclaim sole supervisory responsibility for large, multinational financial institutions that present complex supervisory issues.

- TFI and FinCEN should create a robust and inclusive annual process to establish AML/CFT priorities.

- Congress should enact legislation, already pending in various forms, that requires the reporting of beneficial owner information at the time of incorporation, preventing the establishment of anonymous companies.

- TFI should strongly encourage innovation, and FinCEN should propose a safe harbor rule allowing financial institutions to innovate in a “sandbox” without fear of examiner sanction.

- Policymakers should incentivize banks to work on investigations and reporting of activity of high law enforcement or national security consequence.

- Policymakers should further facilitate the flow of raw data from financial institutions to law enforcement to assist with the modernization of the current AML/CFT technological paradigm.

- Regulatory or statutory changes should be made to the safe harbor provision in the USA PATRIOT Act (Section 314(b)) to further encourage information sharing among financial institutions, and the potential use of utilities to allow for more robust analysis of data.

- Policymakers should enhance the legal certainty regarding the use and disclosure of SARs.

III. Sanctions Regulatory Trends and Developments

Sanctions have played an increasingly central role in the U.S. government's response to Iran's nuclear program, a deteriorated security situation in eastern Ukraine, improved relations with Cuba, and other geopolitical events. The 2016 U.S. presidential election, and the new Administration, present numerous questions about how the U.S. approach to sanctions may shift, especially in light of the prominence of the Iran nuclear deal in President Trump's 2016 campaign and controversies over improving U.S.-Russia relations. Already in 2017, the Trump Administration has cautioned Iran that it is "on notice" concerning ballistic missile testing,[41] and followed that warning with new designations of individuals and entities related to those activities. And, before its end, the Obama Administration used cyber sanctions for the first time to target Russian individuals and entities alleged to have made cyber-enabled attacks on the U.S. election system.

It is valuable, at this important juncture for U.S. sanctions policy, to reflect on the key developments in U.S. sanctions over the past year. In addition to potentially dramatic changes by the Trump Administration to Iran, Russia, and other sanctions programs, this may also be a year in which Congress takes a more active role in shaping U.S. sanctions. While sanctions policy is always responsive to world events that can be difficult to predict, 2017 is likely to be an especially challenging year for companies seeking to identify the most relevant risks, requirements and trends likely to arise in this area of law.

A. Russia Sanctions

1. Ukraine/Crimea

The United States and the European Union have maintained sanctions against Russia since 2014 in response to Russia's annexation of Crimea and its apparent support to separatist movements in eastern Ukraine. These sanctions fall into several categories.

First, pursuant to Executive Orders 13,660 and 13,661,[42] the Treasury Department's Office of Foreign Assets Control has added Russian and Ukrainian individuals and entities to its list of Specially Designated Nationals and Blocked Persons (SDN List). These designations began in 2014 and have continued at irregular intervals since that time, including new designations as recently as December 20, 2016.

Second, pursuant to Executive Order 13,662,[43] OFAC has developed a novel sectoral sanctions program that targets certain types of transactions (concerning access to U.S. capital markets and access to U.S.-origin goods, technology, and services related to nonconventional energy projects) involving designated Russian firms in certain targeted industries (financial services, energy, and defense). These sectoral sanctions designations likewise began in 2014 and have continued through the end of 2016.

Third, pursuant to Executive Order 13,685,[44] OFAC has administered an effective trade embargo with the Crimea region of Ukraine and has made a number of additions to the SDN List of entities and vessels operating there. These, too, have occurred through the end of 2016.

Fourth, the U.S. Departments of Commerce (Commerce) and State (State) have imposed heightened export controls on exports, re-exports, and transfers of certain U.S.-origin goods, software, technology and services targeting the Russian energy and defense sectors. There were no significant developments related to export controls in 2016.

OFAC also issued two general licenses under the Russia sanctions program in 2016. In September, OFAC issued General License No. 10, authorizing certain transactions with entities designated under Executive Order 13,685, the Crimea embargo, necessary to divest or transfer holdings in those entities.[45] And in December, OFAC issued General License No. 11, authorizing certain transactions with FAU Glavgosekspertiza Rossii in connection with obtaining project design reviews or permits from the Russian federal agency with authority for approving certain infrastructure projects in Russia.[46]

The election of President Trump has raised questions about the future of this sanctions program, as the existing multilateral commitment to maintain Russia sanctions unless and until Russia meets its commitments under the *Minsk II* cease-fire could be undermined if the Trump Administration pursues "a rapprochement with Putin."[47] The President and members of his Administration have suggested that rather than ease sanctions in exchange for Russia's adherence to *Minsk II* and its cessation of activities in Ukraine, the United States may provide sanctions relief in exchange for Russian cooperation on combating global terrorist threats such as ISIS or reducing its nuclear weapons capabilities.[48] Yet such suggestions have been followed by reports that President Trump "may shelve, at least temporarily, his plan to pursue a deal with Moscow on the Islamic State group and other national security matters."[49] And the White House and members of the Trump Administration have also signaled that, in fact, the easing of sanctions against Russia would remain subject to its adherence to *Minsk II* and the abandonment of Crimea.[50] Indeed, on April 21, 2017, Secretary Steve Mnuchin specifically stated that the Department of the Treasury would not authorize U.S. companies to proceed with currently prohibited energy projects in Russia.[51] Amid this uncertainty, there is strong support for sanctions among both Democratic and Republican leaders on Capitol Hill, where any effort by the Trump Administration to ease sanctions could be met with legislative action to "backfill" existing measures currently in place under executive action. In January, a bipartisan group of senators introduced legislation that would effectively codify and escalate (including by targeting U.S. and non-U.S. financial institutions that participate in Russian sovereign debt offerings) sanctions against Russia imposed by the Obama Administration.

In December 2016, the European Council extended the application of the EU's equivalent sectoral sanctions until July 31, 2017, and the EU is expected to renew its asset freezes and travel bans against targeted Russian individuals and entities by mid-March 2017.

2. Cyber Sanctions

In December 2016, President Obama amended a previously issued executive order[52] designed to address cyber-enabled activities in response to "Russia's cyber activities [that] were intended to influence the election, erode faith in U.S. democratic institutions, sow doubt about the integrity of our electoral process, and undermine confidence in the institutions of the U.S. government."[53] At the same time, OFAC added five entities and four individuals to the SDN List in connection with what the White House described as malicious Russian cyber activity.[54]

These new cyber sanctions were the first of their kind, targeting Russian intelligence services and their top officers, including the Federal Security Service, or FSB, as well as three companies that the Obama Administration identified as supporting Russia's cyber-enabled activities through intelligence activities, special training, and other capabilities.

The December 2016 action represented the first (and, thus far, only) use of the cyber sanctions, which President Obama promulgated in an April 2015 executive order in response to a number of apparent cyber-enabled threats to U.S. interests. Congress has previously authorized sanctions to combat cyber-related economic or industrial espionage, and these measures paralleled a separate executive order imposing sanctions against North Korea for "its destructive, coercive cyber-related actions during November and December 2014."[55]

In February 2017, OFAC announced a new general license authorizing U.S. and non-U.S. companies exporting U.S.-origin technology to the Russian Federation to engage the Russian security service in regulatory approval processes, provided that the export is otherwise licensed by the Commerce Department, the payment of any regulatory fees to the Federal Security Service does not exceed $5,000 per calendar year, and the Federal Security Service is not the end user of the exported technology.[56]

For additional detail on the general license, refer to our Client Alert: Treasury Department Imposes New Sanctions Against Iran and Clarifies Russia Cyber Sanctions.

3. Magnitsky Act

OFAC administers sanctions pursuant to the Sergei Magnitsky Rule of Law Accountability Act of 2012 and, in 2016, added 12 individuals to the SDN List because of their involvement in human rights abuses in Russia.

B. Cuba Sanctions

2016 saw the continued normalization of U.S.-Cuba relations, a policy shift set in motion by the Obama Administration in December 2014. President Trump has sent mixed signals about whether to continue that shift. He appeared to support the concept of liberalized U.S.-Cuba trade during last year's presidential election, but said that "we should have made a better deal."[57] The Trump Administration, like its predecessor, would require congressional cooperation to lift the embargo if it decided to significantly expand on existing sanctions relief.

But, more recently, President Trump and his representatives have emphasized the need for rejecting what he has called a "very weak agreement," including, if necessary, by revoking executive orders signed by President Obama that gave effect to the change in policy. Upon the death of Fidel Castro, the then-President-Elect affirmed that he would "terminate [the] deal" if Cuba proved "unwilling to make a better deal for the Cuban people."[58]

As in the case of Russia, the Obama Administration accomplished its sanctions objectives primarily through executive action; the Trump Administration, should it decide to reverse existing policies, could do so unilaterally by revoking executive orders.

1. January Round

In January 2016, Treasury and Commerce took action to implement President Obama's initiatives to normalize U.S.-Cuba relations and to "engage and empower the Cuban people." These included:[59]

- removing certain payment and financing restrictions for authorized exports and re-exports to Cuba of non-agricultural items or commodities;
- permitting blocked space, code-sharing, and leasing arrangements with Cuban airlines to further facilitate authorized travel to Cuba;
- authorizing additional travel-related and other transactions incident to the temporary sojourn of aircraft and vessels; and
- expanding travel authorizations related to professional meetings and other events, disaster preparedness and response projects, and information and information materials, including transactions incident to professional media or artistic productions, in Cuba.

2. March Round

In March 2016, Treasury and Commerce, in coordination with the State and Transportation Departments, announced new regulations that allowed scheduled air service between the United States and Cuba.[60] The regulations also included an expansion of Cuban and Cuban nationals' access to U.S. financial institutions and dollar-denominated transactions. In particular, OFAC allowed U.S. banks to process U-turn transactions in which Cuba or a Cuban national has an interest; to process U.S. dollar monetary instruments presented indirectly by Cuban financial institutions; and to open and maintain bank accounts in the United States for Cuban nationals in Cuba to receive payments for authorized or exempt transactions and to remit such payments back to Cuba.

3. October Round

In October 2016, Treasury and Commerce announced the sixth round of eased sanctions and export controls designed to bolster trade between the United States and Cuba.[61] These regulatory changes, like the five preceding rounds, reflected the exercise of presidential authority to reduce existing restrictions on U.S. dealings with Cuba within the constraints of a statutory embargo that only Congress can lift. They also coincided with the release of a new Presidential Policy Directive that set forth an interagency strategy to continue with the normalization of U.S.-Cuba relations. The Trump Administration has yet to provide clarity over whether it intends to continue to pursue normalization, or whether it will instead freeze or roll back the eased sanctions that occurred under President Obama.

For additional detail about the October round of Cuba sanctions relief, refer to our Client Alert: US Implements Sixth Round of Eased Sanctions.

C. Iran Sanctions

President Trump vowed during the 2016 presidential campaign to "dismantl[e] the [disastrous] nuclear deal with Iran."[62] The P5+1 (China, France, Germany, Russia, the United Kingdom and the United States), the European Union and Iran had agreed to the Joint Comprehensive Plan of Action (JCPOA) in July 2015, and implemented it in January 2016.

In particular, on January 16, 2016, the P5+1 announced the arrival of "Implementation Day" for the JCPOA. In return for Iran meeting certain nuclear benchmarks, the United States and the EU implemented measures to lift the "nuclear-related" trade and financial sanctions against Iran pursuant to the JCPOA Sanctions Annex, superseding interim sanctions relief that had been in place since 2013. Although the EU has lifted nearly all sanctions against Iran, most restrictions applicable to U.S. persons and firms remained in effect.

The United States provided sanctions relief through the issuance of a new executive order, new general licenses, a new statement of licensing policy, and new guidance and FAQs; the adoption of several statutory waivers; and the delisting of various individuals and entities from the SDN List and other sanctions lists. These measures lifted nearly all secondary sanctions applicable to the activities of non-U.S. persons relating to Iran, as well as restrictions on the Iran-related activities of non-U.S. entities that are owned or controlled by U.S. persons.

But "primary" U.S. sanctions against Iran that are applicable to U.S. persons and firms, in addition to sanctions targeting Iran's support for terrorism, human rights abuses, ballistic missile development and destabilizing regional activities, remain in effect. The prohibition on "facilitation" by U.S. persons of the Iran-related transactions of non-U.S. persons also remains in effect, albeit with limited exceptions related to the alteration of internal company policies and procedures and use of global business support systems in the context of foreign entities owned or controlled by U.S. persons, as explained more fully below.

In the EU, sanctions relief took the form of an EU Council decision implementing legislation on sanctions relief, including the delisting of Iran-related persons and entities from its sanctions lists. In contrast to U.S. sanctions relief, EU relief was relatively comprehensive by lifting most restrictions applicable to EU persons and entities, although certain sanctions relating to proliferation, missile technology, human rights and terrorism remain in effect.

These U.S. and EU measures created a variety of new compliance challenges for firms in the United States, EU and elsewhere. Most prominently, Implementation Day marked a significant divergence between U.S. and EU sanctions requirements, which now poses unique risks to firms with global operations.

Financial institutions and their risk appetites continue to play a pivotal role in the practical implementation of this sanctions relief. Indeed, since Implementation Day, the willingness of global firms to take

advantage of the new opportunities in Iran created by the sanctions relief has been mixed. The continued limits placed on the U.S. financial system presents banking and financing challenges for non-U.S. firms that limit their ability to operate in or with Iran. Non-sanctions risks, including those arising from the integrity of the Iranian financial system, anti-corruption compliance and related risks, contribute to making Iran a very challenging market in which to operate, even when U.S. or EU sanctions relief now allows it.

The election of President Trump, who has been a sharp critic of the JCPOA, raises the likelihood that sanctions will be re-imposed and/or more aggressively enforced. In the first weeks of the Trump Administration, OFAC imposed new non-nuclear related sanctions against Iran in response to its ballistic missile testing. While these were limited only to new SDN designations, they signaled the arrival of rising rather than dissipating hostilities between the United States and Iran. Indeed, in April 2017, the State Department certified to Congress that Iran was in compliance with the JCPOA as required by the Iran Nuclear Agreement Review Act of 2015. However, the State Department also stated at that time that the National Security Council will lead an interagency review of the JCPOA to determine whether it is "vital to the national security interests of the United States." Notably, the State Department certification concerning the JCPOA raised specific concerns over one non-nuclear related Iranian activity: Iranian support for terrorism.

For additional detail concerning the JCPOA, summarized below, refer to our Client Alert: Iran Nuclear Sanctions Relief Implemented.

1. U.S. Sanctions Relief

New Executive Order

On Implementation Day, the United States issued a series of statutory waivers and a new executive order that revoked or amended the following previous executive orders:

- Executive Order 13,574 of May 23, 2011[63] (authorizing the implementation of certain sanctions set forth in the Iran Sanctions Act of 1996, as amended);
- Executive Order 13,590 of November 20, 2011[64] (authorizing the imposition of certain sanctions with respect to the provision of goods, services, technology, or support for Iran's energy and petrochemical sectors);
- Executive Order 13,622 of July 30, 2012[65] (authorizing additional sanctions with respect to Iran);
- Executive Order 13,645 of June 3, 2013[66] (authorizing the implementation of certain sanctions set forth in the Iran Freedom and Counter-Proliferation Act of 2012 and additional sanctions with respect to Iran); and
- Executive Order 13,628 of October 9, 2012[67] (authorizing the implementation of certain sanctions set forth in the Iran Threat Reduction and Syria Human Rights Act of 2012 and additional sanctions with respect to Iran).

General Licensing for Foreign Entities Owned or Controlled by U.S. Persons

OFAC issued General License H (GL H) on Implementation Day, authorizing foreign subsidiaries and joint ventures of U.S. firms to engage in Iran-related business.[68] GL H is not limited to specific sectors, but OFAC's Guidance and FAQs accompanying the publication of GL H emphasize that authorized activities do not include those involving SDNs; U.S.-origin items controlled for export; or any Iranian Government military, intelligence or law enforcement entity, among other restrictions.

Notably, GL H does not authorize U.S. persons to directly engage in any Iran-related activities, and the general prohibition on facilitation by U.S. persons of the Iran-related activities of non-U.S. persons—such

as by approving, financing or guaranteeing such activities—remains in effect. However, GL H provides for certain limited exceptions from the prohibition on facilitation by authorizing U.S. persons to engage in an initial set of activities to give effect to GL H:

- activities related to the establishment or alteration of operating policies and procedures of a U.S. entity or a U.S.-owned or -controlled foreign entity, to the extent necessary to allow a U.S.-owned or -controlled foreign entity to engage in transactions authorized by GL H; and

- activities to make available to those foreign entities that the U.S. person owns or controls any automated and globally integrated computer; accounting; e-mail; telecommunications; or other business support system, platform, database, application or server necessary to store, collect, transmit, generate or otherwise process documents or information related to authorized transactions.

OFAC has clarified that these exceptions to the prohibition on facilitation are intended to authorize the involvement of U.S. persons who are "board members, senior management, and employees of either a U.S. parent company or a U.S.-owned or -controlled foreign entity in the establishment or alteration of operating policies and procedures," as well as "outside legal counsel or consultants to draft, alter, advise, or consult on such operating policies and procedures." It also authorizes the provision by U.S. persons of "training, advice, and counseling on the new or revised operating policies and procedures."[69]

GL H does not authorize U.S. persons to become involved in the ongoing Iran-related operations or decision making of U.S.-owned or -controlled foreign entities, including their day-to-day operations. GL H also does not authorize U.S. persons to facilitate any activity by a foreign entity that is not U.S.-owned or -controlled, including even initial alterations to those entities' policies and procedures.

On January 12, 2017, OFAC published "Guidance on the Provision of Certain Services Relating to the Requirements of U.S. Sanctions Laws," which clarified that U.S. persons may provide information and guidance regarding the requirements of U.S. sanctions laws, and may opine on the legality of specific transactions, regardless of whether the U.S. person himself or herself could engage in those transactions.[70] While the guidance is not specific to GL H or Iran sanctions, it does help to delineate the role that U.S. compliance and legal service providers can play with respect to activities by non-U.S. companies.

General License for the Importation of Iranian Foodstuffs and Carpets

OFAC issued a new general license on Implementation Day authorizing imports into the United States of, and dealings in, Iranian-origin carpets and certain foodstuffs, including pistachios and caviar.[71]

Statement of Licensing Policy Relating to Iranian Commercial Passenger Aircraft

OFAC also issued a new Statement of Licensing Policy, pursuant to which U.S. or non-U.S. firms may request specific authorization to engage in transactions for the sale or export of commercial passenger aircraft, spare parts and components, and associated services to Iran.[72] Unlike previous licensing policies in this sector, the new policy does not require that the transaction be focused solely on the safety of civil aviation in Iran but allows for commercial sales more broadly. It was followed, in March 2016, by new clarifying FAQs and the issuance of General License I, which authorized certain transactions related to the negotiation of, and entry into, contingent contracts for activities eligible for authorization under the Statement of License Policy.

In July 2016, OFAC issued General License J, which authorized the re-exportation of certain civil aircraft to Iran on temporary sojourn and related transactions.[73] In December 2016, OFAC amended that general license to allow the temporary re-export of eligible civil aircraft to Iran involving code sharing arrangements. These followed new FAQs in April 2016 in which OFAC addressed the payments or the facilitation of payments to Iranian civil aviation authorities for overflights of Iran or landing in Iran.

Delisting from the SDN and Other Sanctions Lists

On Implementation Day, OFAC removed more than 400 Iranian and non-Iranian individuals and entities from the SDN List, Foreign Sanctions Evaders List, and Non-SDN Iran Sanctions Act List, as set forth in Annex II of the JCPOA.[74]

Many individuals and entities remain on the SDN List and therefore subject to asset freezes under various sanctions authorities. The Government of Iran and certain Iranian financial institutions remain SDNs pursuant to Executive Order 13,599 and other legal authorities, and U.S. persons must continue to block the property and interest in property of all such entities unless otherwise authorized. Secondary sanctions, by contrast, no longer apply to such Executive Order 13,599 designees, and OFAC published a new Executive Order 13,599 List that assists with compliance by identifying entities that qualify as the "Government of Iran" or an "Iranian financial institution."[75]

2. EU Sanctions Relief

The EU adopted Council Decision (CFSP) 2016/37 on Implementation Day to give effect to the October 2015 Council Decision (CFSP) 2015/1863, setting forth the terms of the EU's Iran sanctions relief.[76] The European Council also published a comprehensive Information Note on EU sanctions relief.

In contrast to U.S. sanctions relief, EU relief is relatively comprehensive, lifting sanctions on nearly all financial and commercial dealings between the EU and Iran. These include financial transfers to and from Iran, including use of the SWIFT financial messaging services by non-listed Iranian entities. Certain non-listed Iranian banks are now able to open branches, subsidiaries or representative offices in the EU, and EU financial institutions may also open offices in Iran. The EU has also lifted nearly all sanctions on the Iranian oil, gas and petrochemical sectors; the shipping and shipbuilding sectors; the precious metals sector; and others.

Like the United States, the EU removed many Iranian and non-Iranian individuals and entities from its sanctions list, as set forth in Annex II of the JCPOA, and continues to apply certain limited types of sanctions against Iran, including an arms embargo and sanctions related to missile technology proliferation, human rights abuses, anti-terrorism and Iran's destabilizing regional policies.

3. Continuing Sanctions Against Iran

Despite the broad easing of nuclear-related sanctions against Iran, a variety of restrictions and Iran disclosure obligations remain in place.

First, the U.S. trade embargo against Iran remains in effect.[77] Under these primary sanctions, U.S. persons and firms remain prohibited from engaging in any transactions or dealings directly or indirectly with Iran, including the indirect export of goods or services to Iran, unless otherwise authorized. U.S. and non-U.S. persons are also prohibited from evading U.S. sanctions or "causing" a sanctions violation by a U.S. person, such as by stripping or omitting information from transaction documents involving Iran.

Second, both U.S. and non-U.S. persons continue to face restrictions on the export and re-export to Iran of U.S.-origin goods or technology controlled under the Export Administration Regulations or International Trafficking in Arms Regulations.

Third, the United States retains various authorities to impose sanctions in response to Iran's support for terrorism (e.g., Iran will remain designated as a State Sponsor of Terrorism under various statutes), human rights abuses, proliferation of weapons of mass destruction and their means of delivery, and destabilizing regional policies, such as in Syria and Yemen. The Government of Iran, including the Iranian military and intelligence establishment, remains sanctioned under these authorities.

Fourth, non-U.S. persons remain exposed to U.S. secondary sanctions for engaging in or facilitating transactions with persons or entities that will remain on the SDN List, unless such entities are on the Executive Order 13,599 List by virtue of their affiliation with the Government of Iran. SDN designees include the Iranian Revolutionary Guard Corps, an arm of the Iranian military with a pervasive presence in the Iranian economy, and other persons and entities engaged in conventional weapons proliferation or support for terrorism.

Fifth, so-called Section 219 SEC disclosure requirements under the Iran Threat Reduction Act remain in place following sanctions relief.[78] Section 219 does not prohibit any specific conduct, but instead requires that "issuers" under the Securities Exchange Act of 1934 disclose in reports filed with the SEC various types of transactions in Iran undertaken by the issuer or its "affiliates."

D. Other Significant Developments

1. Sudan

On January 13, 2017, OFAC issued a general license that authorizes all transactions with Sudan that were previously prohibited by the Sudanese Sanctions Regulations (SSR), 31 C.F.R. Part 538, and Executive Orders 13,067 and 13,412.[79] President Obama also issued an executive order that would revoke the sanctions provisions applicable to Sudan through the previous executive orders on July 12, 2017, provided that the government of Sudan continues its cooperation with the United States on specified U.S. foreign policy priorities, including the cessation of hostilities in Sudanese conflict areas, improved humanitarian access in Sudan, and cooperation with the United States on addressing regional conflicts and the threat of terrorism.[80]

The measures effectively suspend Sudan's current status as a sanctioned country. U.S. persons are now able to conduct transactions with Sudan, and the property of the government of Sudan is unblocked.

The unique framework of this action means that the Trump Administration, based on the assessment and recommendation of the secretary of state and other incoming administration officials, will determine whether Sudan sanctions should be lifted permanently in July 2017.

For additional details about the January 2017 action with respect to Sudan, refer to our Client Alert: Sudan Embargo Lifted.

2. North Korea

North Korea has been at the center of worldwide attention in 2016 and 2017 due to its continued bellicosity, including underground nuclear testing and its launch of a new type of intermediate-range ballistic missile that it claimed could be nuclear-equipped. In response, the Trump Administration has rejected direct talks with North Korea and appears to be directing its attention at China. As discussed below, a key tool available to the United States are "secondary sanctions" that permit U.S. action against foreign companies that deal with North Korea. China, including its financial sector, would be a likely target of any U.S. secondary sanctions.

On February 18, 2016, President Obama signed the North Korea Sanctions and Policy Enhancement Act of 2016.[81] Its scope was substantially broader than a contemporaneous United Nations Security Council Resolution in targeting North Korea's weapons development and illicit financing activities and in creating new secondary sanctions against third-country firms that engage in certain types of activities in or with North Korea.

The Act provided for both mandatory and discretionary sanctions based on several criteria. The President must designate any firm or person determined to have knowingly assisted with the development of North Korea's weapons of mass destruction program, delivery systems, or other military programs; exported luxury goods to North Korea; engaged in money laundering, counterfeiting or narcotics trafficking on

behalf of North Korea; engaged in cyberattacks on behalf of North Korea; or dealt in precious metals, minerals, or software related to weapons development. If a firm is designated under this "mandatory" subsection of the Act, then the President must impose asset-blocking requirements and prohibit all transactions in the property and property interests of that firm.

The President also has "discretionary" authority to select from a menu of sanctions to impose against persons who provide any material assistance to persons designated under UNSC resolutions, engage in bribery in North Korea, assist in the misappropriation of North Korean funds or financially support any of these activities. Those designated under this discretionary provision of the Act may be subject to one or more of the sanctions described in the Act, including the application of special measures for U.S. financial institutions to address money laundering; prohibitions on foreign exchange; prohibitions on transfers of credit or payments in or through the U.S. financial system; and certain other measures related to procurement, travel, and shipping.

In March 2016, President Obama signed Executive Order 13,722, blocking property of the Government of North Korea and the Workers' Party of Korea, and authorizing additional designations of individuals or entities found to engage in certain activities including operation in the North Korean economy and certain dealings with the Government of North Korea or the Workers' Party of Korea.[82] OFAC simultaneously issued several general licenses authorizing certain activities (including noncommercial, personal remittances, support of nongovernment organizations, certain telecommunications activities, and the provision of certain legal services), but proceeded to make several rounds of new designations under this and other authorities targeting North Korea through 2016 and into 2017.[83]

For additional details, refer to our Client Alert: Enhanced North Korea Sanctions Adopted.

3. Burma

In October 2016, following a series of measures in 2016 and earlier easing of sanctions against Burma, President Obama signed an executive order terminating the national emergency with respect to Burma, revoking the Burma sanctions executive orders, and waiving other statutory blocking and financial sanctions on Burma.[84] These measures ended the economic and financial sanctions against Burma.

4. Côte d'Ivoire

In September 2016, President Obama signed an executive order terminating the national emergency with respect to Côte d'Ivoire.[85] President Bush, in 2006, had imposed sanctions against Côte d'Ivoire to address human rights abuses, political violence and unrest, and attacks against international peacekeeping forces. Such sanctions had been limited to the blocking of property and property interests of specifically identified individuals and entities. President Obama's termination of the national emergency with respect to Côte d'Ivoire ended the sanctions program.

5. Kingpin Act

Since 2000, OFAC has designated almost 1,900 individuals and entities under the Kingpin Act for engaging in international narcotics trafficking.[86] Throughout 2016 and early 2017, OFAC granted several general licenses, permitting transactions and activities that would otherwise be prohibited under the Kingpin Act. OFAC also designated certain individuals and institutions that have been connected to the Panama Papers leak.

In May 2016, OFAC published five general licenses, allowing transactions and activities related to the hotel at Millennium Plaza, Panama; two newspapers, La Estrella and El Siglo; the Soho Mall Panama; and transferring funds from Balboa Bank & Trust, seized by Panama. The general licenses for the Soho Mall Panama and Millennium Plaza are intended to assist with winding down transactions for a limited time; both entities are associated with the Waked Money Laundering Organization, which OFAC designated in May 2016. In June 2016, OFAC added general licenses for Importadora Maduro, S.A.;

Maduro Internacional, S.A.; and Lindo & Maduro, S.A. OFAC amended several of these general licenses later in the year and additionally amended the 2015 general license for Banco Continental, S.A.[87]

6. Libya

In April 2016, President Obama signed Executive Order 13,726, blocking property and suspending entry into the United States of those contributing to the ongoing violence in Libya (including attacks by armed groups, human rights abuses, violations of the United Nations arms embargo, and misappropriation of Libyan resources).[88] The order expanded the previous executive order from February 25, 2011, and blocks the property of any person responsible for or complicit in, directly or indirectly, any actions or policies that threaten peace, political transition, misappropriation of state assets, and other threats.

IV. Enforcement

Intense scrutiny in the areas of BSA/AML and sanctions enforcement is likely to continue based on current trends. At the start of 2017, all of the five largest U.S. banks by asset size had been subject to public regulatory actions relating to BSA/AML or sanctions deficiencies at some point within the past five years. Public disclosures also reflect that regulators and law enforcement remain active in these areas of enforcement, with a number of the largest financial institutions disclosing ongoing inquiries at the end of 2016.

In 2015, we saw record-setting penalties imposed, at times approaching and exceeding the billion-dollar mark. While the frequency and size of enforcement actions in 2016 was lighter than in the prior year, 2017 has seen a noticeable uptick in the announcement of significant enforcement actions that suggests the larger trend remains in the direction of very high regulatory expectations and continued enforcement.

A. AML Enforcement

Federal and state regulators announced two significant AML enforcement actions at the start of this year. Each action imposed large fines, eclipsing the biggest penalties assessed in 2016 and, consistent with current trends, required admissions of wrongdoing, significant AML program enhancements, and the appointment of independent monitors.

In January 2017, The Western Union Company forfeited $586 million to federal regulators and admitted to criminal violations that included willfully failing to maintain an effective AML program and allowing the processing of transactions in connection with an international consumer fraud scheme. Less than two weeks later, NYDFS announced a $425 million fine against Deutsche Bank AG and its New York branch in connection with violations of AML laws involving a long-running Russian “mirror trading” scheme. The actions reflect the culmination of a sustained focus by federal and state regulators on AML enforcement in recent years—a trend we expect to continue.

By contrast, 2016 was a year that saw a decrease in the number and size of public AML-related settlements compared to previous years, which had seen a number of record-setting fines and criminal prosecutions for violations of BSA/AML and sanctions laws. All indications continue to be that regulators and law enforcement agencies’ expectations remain high when it comes to the role that financial institutions are required to play in establishing effective compliance programs to monitor, detect, and report suspicious activity.

A variety of regulators, including DOJ, FinCEN, FINRA, the Office of the Comptroller of the Currency (OCC), SEC and NYDFS, brought notable enforcement actions over the past year. In connection with these actions, we observed several trends:

- Banking regulators continued to focus on the failure to file timely and effective SARs and, at the state level, NYDFS imposed the largest AML penalties of 2016, with a particular focus on foreign banks.

- AML actions involving broker-dealers were on the rise in 2016. These actions included the SEC’s first enforcement action premised entirely on a broker-dealer’s failure to file SARs, as well as FINRA’s imposition of the largest-ever AML fine. Microcap trading also continues to give rise to significant penalties.

- The imposition of independent monitors and consultants also continues to be a very common requirement in BSA/AML-related settlements. Last year alone, the oversight of at least a half-dozen independent parties was imposed as a condition of settlement by FinCEN, the SEC and NYDFS, including in actions involving banks, broker-dealers and gaming companies.

- NYDFS imposed the most monitors last year. Acting under the newly appointed leadership of Superintendent Vullo, NYDFS required oversight by independent monitors, consultants or other third parties in all but one of the five BSA/AML enforcement actions NYDFS announced last year. The trend continued into 2017, with NYDFS requiring Deutsche Bank to engage an independent monitor for a two-year term. The common practice includes reserving the option to extend the monitorship at the end of the term, depending on the outcome of the institution's remedial efforts.

- FinCEN increased scrutiny of gaming companies, announcing three significant actions in 2016.

- Compliance professionals continue to face independent liability for policing internal conduct as regulators advance efforts to hold individuals liable for compliance errors at their companies. FinCEN secured a significant legal victory at the start of 2016 when a federal district court in Minnesota held that the BSA permits it to bring suit against individuals for willfully violating the BSA's AML program requirement.[89]

- In 2016, the OCC, the SEC and FINRA each imposed AML-related fines against senior compliance officers and a CEO, ranging from $2,500 to $50,000. These fines were imposed on individuals in parallel with related AML settlements with those individuals' financial institutions involving substantially larger penalties.

A brief summary of notable AML enforcement trends and the related actions that underlie them follows.

1. Money Services Businesses

Recently, federal regulators have focused their attention on AML compliance in the money services business (MSB) sector. In January 2017, **Western Union** agreed to forfeit $586 million and enter into agreements with DOJ, the Federal Trade Commission (FTC), several U.S. Attorneys' Offices, and FinCEN.[90] Western Union entered into a Deferred Prosecution Agreement (DPA), admitting to criminal violations including willfully failing to maintain an effective AML program and aiding and abetting wire fraud. According to the DPA, Western Union failed to file SARs identifying its own agents as suspicious actors who repeatedly facilitated consumer fraud–related transactions.[91] Western Union also acquired a significant agent, FEXCO, that it knew, prior to the acquisition, had an ineffective AML program and had contracted with other agents who were facilitating significant levels of consumer fraud. Despite this knowledge, Western Union moved forward with the acquisition and did not remedy the AML failures or terminate the high-fraud agents.[92] As part of the settlement with FinCEN, Western Union agreed to implement stricter AML/fraud policies. The FTC's order required the appointment of an independent compliance auditor to assess compliance and issue periodic reports for a term of three years. The $586 million penalty will be used to reimburse consumers who were victims of the fraud.

2. Banking Cases

a) NYDFS Continues to Impose Substantial AML Penalties

At the state level, New York continues to impose substantial penalties for AML violations. In January 2017, NYDFS entered a consent order with **Deutsche Bank** in connection with a Russian mirror-trading scheme that went undetected among the bank's Moscow, London and New York offices and allowed an estimated $10 billion to be moved out of Russia.[93] The scheme involved closely related parties making a series of offsetting stock trades that, according to NYDFS, "lacked economic purpose and could have been used to facilitate money laundering or enable other elicit conduct."[94] Deutsche Bank cooperated with the investigation and agreed to pay a $425 million fine and hire an independent monitor for a two-year term in connection with violations of New York anti-money laundering law. NYDFS coordinated its investigation with the UK Financial Conduct Authority, which in parallel assessed a penalty of £168 million (approximately $210 million). NYDFS also used its announcement of the settlement to highlight the importance of its new risk-based anti-terrorism and anti-money laundering regulation, which became effective on January 1, 2017, and is described in more detail above under Regulatory Trends and Developments.

All of NYDFS's public AML enforcement actions in 2016 focused on international banks. In December 2016, NYDFS fined **Intesa Sanpaolo SpA** and its New York branch $235 million and extended the term of engagement with its current independent consultant by up to two years for violations of New York anti-money laundering and Bank Secrecy Act laws.[95] Intesa's violations included a failure to follow written procedures to clear transactions and improperly closing alerts as "false positives" without investigation using ad hoc procedures when 41 percent of the alerts closed should have merited investigation. NYDFS also found that Intesa deliberately concealed information from bank examiners, and that from approximately 2002 to 2006 it used opaque methods and practices to conduct more than 2,700 U.S. dollar-clearing transactions, amounting to more than $11 billion, on behalf of Iranian clients and other entities possibly subject to U.S. economic sanctions. The consent order requires Intesa to strengthen compliance procedures, submit a revised compliance plan, and extend the engagement of its independent consultant for up to two years to test the results of remediation efforts.[96]

In November 2016, NYDFS fined the **Agricultural Bank of China** $215 million for engaging in "intentional wrongdoing" resulting in AML violations.[97] The NYDFS investigation discovered that the Bank ramped up its dollar-clearing activities through foreign correspondent accounts starting in 2013, even though NYDFS warned it not to increase those transactions until it significantly upgraded its internal compliance program. The Bank also severely curtailed the independence of the chief compliance officer at the New York branch, who tried to raise serious concerns to branch management and conduct internal investigations regarding suspicious activity. In addition to paying the penalty, the Bank agreed to take immediate steps to improve its legal compliance, including hiring an outside monitor.

In August 2016, NYDFS fined **Mega International Bank of Taiwan** (Mega Bank) $180 million, imposed a two-year independent monitor, and mandated reforms for AML violations.[98] NYDFS found that the New York branch's BSA/AML officer and chief compliance officer both lacked familiarity with U.S. regulatory requirements. In addition, the chief compliance officer had conflicted interests because she had key business and operational responsibilities along with her compliance role. Compliance staff at both the head office and branch failed to periodically review surveillance filter criteria designed to detect suspicious transactions. Also, numerous documents relied upon in transaction monitoring were not translated to English from Chinese, precluding effective examination by regulators. Finally, the New York branch procedures provided virtually no guidance concerning the reporting of continuing suspicious activities, had inconsistent compliance policies, and failed to determine whether foreign affiliates had adequate AML controls in place.

In the first quarter of 2016, NYDFS also announced entering into written agreements without penalties with the **Industrial Bank of Korea** and the **National Bank of Pakistan,** under which the banks agreed to enhance AML compliance and controls after examinations revealed significant deficiencies relating to risk management and compliance with relevant AML and sanctions laws.[99] In the case of National Bank of Pakistan, the engagement of an independent third party was required for the purpose of conducting a transactional review. The Federal Reserve was also a party to both written agreements.

b) Continued Focus on Failures to File Timely and Effective SARs

2016 also saw a continued enforcement focus on the failure to maintain adequate anti-money laundering programs that result in the filing of timely and effective SARs. Among other examples, actions against Gibraltar Private Bank & Trust and Stearns Bank are illustrative of the types of conduct that have given rise to recent enforcement actions by FinCEN and the OCC.

In February 2016, FinCEN fined **Gibraltar Private Bank & Trust** $4 million for admitted failures in monitoring and detecting suspicious activity despite red flags.[100] Gibraltar's transaction monitoring system contained incomplete and inaccurate account opening information and customer risk profiles, and its automated monitoring system generated an unmanageable number of alerts, including large numbers of false positives. Gibraltar also failed to properly train its compliance staff, and failed to develop and implement an adequate Customer Identification Program. As a result, Gibraltar failed to timely file at least 120 SARs involving nearly $558 million in transactions occurring from 2009 to 2013. Gibraltar also unreasonably delayed SAR reporting regarding accounts related to a $1.2 billion Ponzi scheme led by

Florida attorney Scott Rothstein. In parallel, OCC fined Gibraltar $2.5 million, payment of which offset FinCEN's $4 million fine.[101]

In April 2016, the OCC settled its own SAR timeliness enforcement with **Stearns Bank**.[102] Beginning in March 2010, Stearns Bank became aware of suspicious transactions associated with the manipulation and fabrication of accounts receivables and factoring invoices, but failed to follow its internal policies and procedures governing the monitoring and reporting of suspicious activity, including the maintenance of appropriate documentation to support its SAR determinations. As a result, Stearns Bank failed to file timely SARs and was required to pay a $1 million penalty.

On February 27, 2017, FinCEN announced a $7 million civil penalty assessment against **Merchants Bank of California** for failing to establish an adequate AML compliance program, conduct due diligence on foreign correspondent accounts, and detect and report suspicious activity.[103] The California-based community bank provided banking services to MSBs such as check-cashers and money transmitters, but did not adequately assess the money laundering risks presented by servicing the MSBs. In a press release announcing the settlement, FinCEN Acting Director Jamal El-Hindi described the bank as "an institution run by insiders essentially to provide banking services to MSBs that the insiders owned, combined with directions from Bank leadership to staff to ignore BSA requirements with respect to those MSB customers and others."[104] The bank's leadership, according to FinCEN's assessment, impeded the investigation and reporting of suspicious activity by threatening employees who attempted to report suspicious transactions in accounts affiliated with bank executives.[105] Among other violations, the bank also failed to conduct independent testing commensurate with its customer complexity and risk profile and failed to designate a BSA officer. Concurrent with the FinCEN order, the OCC imposed a $1 million penalty (which FinCEN credited toward satisfying its own $7 million penalty) for AML compliance failures that led to violations of previous OCC consent orders.

3. Securities Cases

a) Microcap Trading Continues to Give Rise to AML Actions

FINRA continues to focus on AML violations relating to microcap trading. In December 2016, FINRA fined **Credit Suisse Securities (USA) LLC** $16.5 million for AML compliance program failures, alleging that Credit Suisse failed to effectively review microcap trading for AML purposes from January 2011 to September 2013 and to review potentially suspicious money transfers from 2011 to 2015.[106] FINRA concluded that Credit Suisse's systems and procedures were not adequately designed to detect potentially suspicious transactions in order to cause the filing of SARs. Although the firm used an automated surveillance system to identify red flags, it failed to properly implement the system, including by failing to input adequate data and to use applicable risk scenarios in its assessments. FINRA also alleged that Credit Suisse did not have adequate staffing to review the tens of thousands of alerts its automated system generated in any given year.

Another major microcap-related enforcement action was resolved in 2015 against **Oppenheimer & Co.** There, the SEC and FinCEN fined the broker-dealer a total of $20 million for failing to establish and implement an adequate anti-money laundering program, failing to conduct adequate due diligence on a foreign correspondent account, and failing to comply with requirements under Section 311 of the USA PATRIOT Act.[107] Sixteen customers engaged in patterns of suspicious microcap trading through Oppenheimer's branch offices. Oppenheimer failed to report patterns of activity in which customers deposited large blocks of unregistered or illiquid microcaps, moved large volumes of microcaps among accounts with no apparent purpose, or immediately liquidated those securities and wired the proceeds out of the account. In addition, Oppenheimer designated a customer foreign financial institution as "high risk" but failed to assess the specific risks as a foreign financial institution or conduct adequate due diligence. As a result, Oppenheimer did not detect or investigate numerous suspicious transactions conducted through the account, including prohibited third-party activity and illegal penny stock trading.

b) FINRA Imposes Its Largest-Ever AML Fine

In May 2016, FINRA issued its largest-ever AML fine totaling $17 million against two **Raymond James** entities – Raymond James & Associates, Inc., and Raymond James Financial Services, Inc. (collectively, Raymond James).[108] FINRA alleged that Raymond James' significant growth between 2006 and 2014 was not matched by commensurate growth in their AML compliance systems and processes. This left the firms unable to establish AML programs tailored to their businesses, and forced them instead to rely on a patchwork of written procedures and systems across different departments to detect suspicious activity. The end result was that red flags of potentially suspicious activity went undetected or inadequately investigated. FINRA stated that these alleged failures were "particularly concerning" because Raymond James was previously sanctioned in 2012 for inadequate AML procedures and, as part of that settlement, had agreed to review its program and procedures and certify that they were reasonably designed to achieve compliance.

c) SEC's First Stand-Alone Action Premised on Failure to File SARs

The SEC's June 2016 settlement with **Albert Fried & Company** (AF & Co.) is significant in that it represents the first SEC enforcement action premised solely on a broker-dealer's failure to file SARs and not any other securities law violations.[109] AF & Co., a Wall Street-based brokerage firm, agreed to pay a $300,000 penalty to settle charges that it failed to file SARs for more than five years despite red flags tied to its customers' high-volume liquidations of low-priced securities. On more than one occasion, an AF & Co. customer's trading in a security on a given day exceeded 80 percent of the overall market volume. In other instances, customers were trading in stocks issued by companies that were delinquent in their regulatory filings or involved in questionable penny stock promotional campaigns. The SEC found that AF & Co. violated Section 17(a) of the Securities Exchange Act of 1934 and Rule 17a-8 thereunder.

4. Gaming Companies

Over the past year, FinCEN increased its scrutiny of gaming companies, giving rise to three actions, summarized below.

In October 2016, FinCEN assessed a $12 million civil money penalty against **Cantor Gaming**.[110] Concurrently, Cantor Gaming reached a non-prosecution agreement with the U.S. Attorney's Office for the Eastern District of New York, including a fine of $10.5 million and forfeiture of $6 million.[111] FinCEN determined that Cantor Gaming failed to implement and maintain an effective AML program by failing to have sufficient internal controls and mandatory independent audits and failing to sufficiently train its officers and employees. FinCEN determined that Cantor Gaming also failed to properly and timely file Currency Transaction Reports and SARs and committed thousands of recordkeeping violations, including by failing to keep required records on its highest-volume patron, who placed more than $300 million in wagers between 2010 and 2013.

In July 2016, FinCEN assessed a $2.8 million civil money penalty against **Hawaiian Gardens Casino** for violations of its BSA/AML program and reporting obligations.[112] IRS investigations in 2011 and 2014 revealed multiple BSA violations, and many of the violations uncovered in 2011 remained unaddressed in 2014, despite identification by the casino's independent consultant in 2013. Hawaiian Gardens failed to implement and maintain an effective AML program, failed to report large cash transactions, failed to file SARs and failed to keep certain required records. Although the casino had a variety of tools including casino surveillance and open source information at its disposal, it failed to use those tools to gather customer information and, as a result, 80 percent of the SARs it filed between January 2013 and September 2014 included at least one unknown subject. Certain employees had also been identified multiple times by the IRS for assisting customers with structuring. Similarly, Hawaiian Gardens continued to conduct business with patrons that they had identified as suspicious, even after they had repeatedly refused to provide identification information.

In April 2016, FinCEN fined **Sparks Nugget** $1 million for violating AML program requirements, reporting obligations, and recordkeeping requirements.[113] Sparks Nugget allegedly lacked a "culture of

compliance": the casino routinely disregarded its BSA compliance manager, chose not to file SARs that the compliance manager believed should have been filed, instructed her to not interact with the IRS's BSA auditors, and prevented her from reviewing a copy of the IRS's completed exam report. The management committee that Sparks Nugget established to determine whether to file SARs never met, and some committee members were unaware that they were even on the committee. Further, Sparks Nugget lacked any mechanism to document decisions not to file SARs, and its day-to-day managers maintained that no suspicious activity ever transpired at the casino.

5. High Risk of Personal Liability for Compliance Officers

The start of 2016 saw a significant legal development in FinCEN's landmark *Haider* case: A federal district court held that the Bank Secrecy Act permits FinCEN to bring suit against individuals for willfully violating the BSA's AML program requirement.[114] The decision was significant not only because it appears to be the first court decision in a FinCEN civil action but also because the opinion addressed important aspects of FinCEN's enforcement authority. The case arose after MoneyGram settled with DOJ for admitted AML program failures, and **Thomas Haider**, former chief compliance officer of MoneyGram, was fined $1 million by FinCEN for failing to ensure an effective AML program and failing to ensure timely filing of SARs.[115] In addition to the $1 million penalty, FinCEN also sought to bar Mr. Haider from the financial industry. Haider, however, sought to dismiss the case, arguing that he could not be held liable under 31 U.S.C § 5318(h) because that section of the BSA—which requires each regulated "financial institution" to establish an AML program—applies only to financial institutions, rather than individuals. The court rejected Haider's argument, concluding that his focus on the text of § 5318(h) was misplaced. Instead, the court looked to 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, with the exception of two BSA sections. The court held that because § 5318(h) is not one of those two exceptions, FinCEN can assess civil money penalties against financial institution officers or employees who violate § 5318(h). The court's analysis of this issue is not expansive, and its reasoning—which arguably expands the substantive requirements of the BSA based on the civil penalty provision—is not free from doubt. The *Haider* opinion is unlikely to be the last word on the issue of whether individuals may be held liable under the BSA for what appear to have been, at bottom, institutional failures.

Regulators are showing a sustained interest in holding compliance officers personally liable for compliance deficiencies. Last year, Raymond James' former AML compliance officer **Linda Busby** was fined $25,000 and suspended for three months for alleged failures to detect or investigate red flags.[116] In March 2016, the OCC fined **Charles Sanders**, the former chief compliance officer and chief risk officer of Gibraltar Private Bank & Trust, $2,500 for failing to "file suspicious activity reports on a set of accounts for a customer that was later convicted of crimes related to an illegal Ponzi scheme."[117] Sanders was also ordered to disclose the settlement to any future employers that fall under the definition of a "depository institution." Finally, in mid-October 2016, the SEC settled an action against **Lia Yaffar-Pena**, the former president and CEO of Miami-based brokerage firm E.S. Financial, for aiding and abetting and causing violations of AML rules by allowing foreign entities to buy and sell securities without verifying the identities of the non-U.S. citizens who beneficially owned them.[118] Yaffar-Pena agreed to a one-year supervisory suspension and payment of a $50,000 penalty. The SEC had previously settled an enforcement action against Yaffar-Pena's brokerage firm, **E.S. Financial**, for $1 million for the same alleged violations.[119]

While the unmistakable trend in recent years has been an increasing risk of individual liability for compliance professionals, it remains to be seen how the new Administration's policymakers will balance the desire for individual accountability against the potential negative effects that such actions may have on the ability of the industry to hire and retain qualified professionals willing to take on the job. Compliance professionals, who are an important backstop and internal check on the business, are now facing the specter of being held individually responsible after the fact for the advice they provide on where lines can be drawn in today's complex regulatory environment.

B. Sanctions Enforcement

Last year was a relatively light year for OFAC enforcement, both in terms of the number of cases finalized and the total penalty amounts paid in those cases. In 2016, OFAC announced penalties or settlements in just nine cases, with a total penalty/settlement amount of just over $21 million. By contrast, 2015 saw 15 cases totaling nearly $600 million, and 2014 saw 23 cases totaling $1.2 billion. Much of the penalty and settlement total amounts in the preceding year was the result of major enforcement actions against global financial institutions, such as the $963 million settlement with BNP Paribas SA in 2014, the $329 million settlement with Crédit Agricole Corporate and Investment Bank in 2015, and the $258 million settlement with Commerzbank AG in 2015.

The largest sanctions settlement in 2016 was in July for just $7.6 million and with a non-financial institution. That case involved a Texas company, **Alcon Laboratories, Inc.**, and its Swiss affiliate, who agreed to settle with OFAC and the Commerce Department's Bureau of Industry and Security (BIS) for potential civil liability arising from sales and exports of medical end-use surgical and pharmaceutical products to distributors in Iran and Sudan without OFAC authorization. Among the aggravating factors under OFAC's Enforcement Guidelines was the fact that the company's senior management knew of the conduct giving rise to the apparent violations and that the company "is a sophisticated multinational corporation with extensive experience in international trade."[120]

The next-largest settlement in 2016 was in November, when **National Oilwell Varco, Inc.**, and its subsidiaries agreed to settle their potential civil liability for apparent violations of U.S. sanctions against Cuba, Iran, and Sudan. OFAC alleged that the company had approved commission payments by its subsidiary to a UK-based entity related to the sale and export of goods to Iran and had engaged in other transactions involving the sale and export of goods to Iran, Cuba, and Sudan. The case was an egregious one under OFAC's Enforcement Guidelines because, among other reasons, the company's senior-level finance executives approved the commission payments and the company appeared to have willfully blinded itself by "acquiescing" to its subsidiary's "deliberate non-identification of Iran in its communications."[121]

The largest OFAC settlement with a financial institution in 2016 was in February, when **Barclays Bank Plc** agreed to remit $2.48 million to settle its potential civil liability for 159 alleged violations of U.S. sanctions against Zimbabwe. OFAC alleged that the bank processed over $3 million in transactions to or through financial institutions in the United States, including its New York branch, for or on behalf of corporate customers of Barclays Bank of Zimbabwe Limited that were owned 50 percent or more by a person on OFAC's SDN List. OFAC found that the Zimbabwe bank's KYC procedures "were ambiguous and difficult to follow with respect to the requirement to identify related parties and/or beneficial owners of corporate customers."[122] OFAC determined that the alleged violations constituted a "non-egregious case," and recognized as mitigating factors Barclays' significant remedial actions and substantial cooperation.[123]

No 2016 action met the level in 2015, where we saw two major sanctions-related enforcements. First, in March 2015, **Commerzbank AG** settled with DOJ, OFAC, the Federal Reserve Board of Governors (FRB), and NYDFS for $1.4 billion for violations of the International Emergency Economic Powers Act (IEEPA) and for failing to have an effective AML program, failing to conduct due diligence on foreign correspondent accounts, and failing to file SARs.[124] Regarding sanctions, Commerzbank concealed hundreds of millions of dollars in transactions on behalf of sanctioned Iranian and Sudanese businesses, even though managers inside the bank raised red flags about its sanctions-violating practices. Commerzbank also admitted to AML deficiencies that made it a conduit for over a billion dollars of the Olympus securities fraud. In addition to the fine, Commerzbank also agreed to implement rigorous internal controls. Second, in October 2015, **Crédit Agricole** paid $787.3 million to settle with DOJ, OFAC, FRB, and NYDFS over violations of the IEEPA and the Trading with the Enemy Act.[125] Between August 2003 and September 2008, subsidiaries of the Bank in Geneva knowingly and willfully moved approximately $312 million through the U.S. financial system on behalf of sanctioned entities located in Sudan, Burma, Iran and Cuba.

This decrease in OFAC penalty cases during 2016 is unlikely to represent a change or a significant shift in enforcement policy. To the contrary, the Trump Administration is expected to maintain or even intensify sanctions enforcement, especially with respect to U.S. sanctions against Iran. And civil penalties, when they are imposed, will now be greater than before: On February 9, 2017, OFAC issued regulations to implement the Federal Civil Penalties Adjustment Act of 1990, adjusting for inflation the maximum amount of civil monetary penalties that may be assessed.[126] Violations of the IEEPA, the statute under which most OFAC sanctions regulations have been promulgated, may now be subject to a penalty of the greater of $289,238 (per violation) or twice the amount of the underlying transaction.

In addition to three penalties or settlement agreements in January 2017 alone, the new year has also delivered the largest OFAC penalty ever against a non-financial institution. On March 7, 2017, OFAC, BIS, and DOJ announced a $1.2 billion settlement agreement with **ZTE Corp.** for civil and criminal violations of the export control and sanctions laws, which included a guilty plea for conspiring to violate the IEEPA. Of the settlement amount, nearly $101 million will go to OFAC for violations of U.S. sanctions against Iran. The settlement agreement followed an investigation into ZTE Corp.'s "multi-year and systematic practice of utilizing third-party companies to surreptitiously supply Iran with a substantial volume of U.S.-origin goods, including controlled goods appearing on the Commerce Control List (CCL)." ZTE's misconduct also included serious charges of obstructing justice and taking affirmative steps to mislead the U.S. government, which likely influenced the record-setting penalty.[127]

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 U.S. Department of Justice, U.S. Attorneys' Offices, the U.S. Department of the Treasury, the U.S. 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 United States 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 their 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 rule-makings. 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 U.S. and non-U.S. 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 lifecycle of enforcement, from responding to initial formal and informal requests for information through negotiating consent orders and compliance 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:

New York

Sharon Cohen Levin	+1 212 230 8804	sharon.levin@wilmerhale.com
Boyd M. Johnson III	+1 212 230 8862	boyd.johnson@wilmerhale.com

Washington DC

Franca Harris Gutierrez	+1 202 663 6557	franca.gutierrez@wilmerhale.com
Reginald J. Brown	+1 202 663 6430	reginald.brown@wilmerhale.com
Ronald I. Meltzer	+1 202 663 6389	ronald.meltzer@wilmerhale.com
Michael J. Leotta	+1 202 663 6526	michael.leotta@wilmerhale.com
Jeremy Dresner	+1 202 663 6176	jeremy.dresner@wilmerhale.com
David M. Horn	+1 202 663 6749	david.horn@wilmerhale.com

[1] Press Release, U.S. Dep't of the Treasury, *Statement from Secretary Mnuchin on President Trump's Budget Proposal*, Washington, D.C. (Mar. 16, 2017), https://www.treasury.gov/press-center/press-releases/Pages/sm0032.aspx.

[2] Evan Weinberger, *Trump Spares Treasury Financial Crimes Units From Cuts*, Law360 (Mar. 16, 2017), https://www.law360.com/articles/902768/trump-spares-treasury-financial-crimes-units-from-cuts.

[3] Louis Nelson and Matthew Nussbaum, *White House puts Iran 'on notice,' won't rule out military force*, Politico (Feb. 1, 2017), http://www.politico.com/story/2017/02/iran-on-notice-trump-michael-flynn-234503.

[4] Joint Advance Notice of Proposed Rulemaking, Enhanced Cyber Risk Management Standards (Oct. 19, 2016), https://www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf.

[5] 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.

[6] *See* Jacob J. Lew, Secretary of the Treasury, Letter to the Honorable Paul D. Ryan, Speaker, U.S. House of Representatives (May 5, 2016), https://www.treasury.gov/press-center/press-releases/Documents/Lew%20to%20Ryan%20on%20CDD.PDF.

[7] Press Release, Off. of Pub. Affairs, U.S. Dep't of Justice, *Acting Assistant Attorney General Kenneth A. Blanco Speaks at the American Bar Association National Institute on White Collar Crime*, Miami, Florida (Mar. 10, 2017) (Remarks as prepared for delivery), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-kenneth-blanco-speaks-american-bar-association-national.

[8] *See* FATF, *Anti-Money Laundering and Counter-Terrorist Financing Measures – United States, Mutual Evaluation Report* (Dec. 2016), http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf; FATF, *Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism – United States* (June 23, 2006), http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20US%20full.pdf.

[9] *See, e.g.*, *In re Brown Brothers Harriman & Co.*, FINRA Letter of Acceptance, Waiver, and Consent, No. 2013035821401, at 2 (Feb. 4, 2014) ("BBH was obligated under federal law to investigate customer activity on a risk basis; omnibus accounts transacting in higher-risk activity, such as suspicious penny stock transactions, merited additional scrutiny."), http://disciplinaryactions.finra.org/Search/ViewDocument/35225.

[10] *See* Press Release, FinCEN, *FinCEN Takes Aim at Real Estate Secrecy in Manhattan and Miami* (Jan. 13, 2016), https://www.fincen.gov/news/news-releases/fincen-takes-aim-real-estate-secrecy-manhattan-and-miami.

[11] *See* Press Release, FinCEN, *FinCEN Expands Reach of Real Estate "Geographic Targeting Orders" Beyond Manhattan and Miami* (July 27, 2016), https://www.fincen.gov/news/news-releases/fincen-expands-reach-real-estate-geographic-targeting-orders-beyond-manhattan. The monetary thresholds for reporting varied by location and ranged from $500,000 (Bexar County) to $3 million (Manhattan). The full table of monetary thresholds is available here: https://www.fincen.gov/sites/default/files/shared/Title_Ins_GTO_Table_072716.pdf.

[12] Press Release, FinCEN, *FinCEN Renews Real Estate "Geographic Targeting Orders" to Identify High-End Cash Buyers in Six Major Metropolitan Areas* (Feb. 23, 2017), https://www.fincen.gov/news/news-releases/fincen-renews-real-estate-geographic-targeting-orders-identify-high-end-cash.

[13] *See* FinCEN, *Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes*, FIN-2016-A003 (Sept. 6, 2016), https://www.fincen.gov/sites/default/files/advisory/2016-09-09/FIN-2016-A003.pdf.

[14] *Id.* at 2.

[15] *See id.* at 4-5 for a full list of red flags.

[16] *See* FinCEN, *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime*, FIN-2016-A005 (Oct. 25, 2016), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005.

[17] The Federal Banking Agencies are the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency.

[18] U.S. Department of the Treasury and Federal Banking Agencies Joint Fact Sheet on Foreign Correspondent Banking: Approach to BSA/AML and OFAC Sanctions Supervision and Enforcement (Aug. 30, 2016), https://www.treasury.gov/press-center/press-

releases/Documents/Foreign%20Correspondent%20Banking%20Fact%20Sheet.pdf; Nathan Sheets, Adam Szubin, and Amias Gerety, *Complementary Goals - Protecting the Financial System from Abuse and Expanding Access to the Financial System* (Aug. 30, 2016), https://www.treasury.gov/connect/blog/Pages/Complementary-Goals---Protecting-the-Financial-System-from-Abuse-and-Expanding-Access-to-the-Financial-System.aspx.

[19] USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 312, 115 Stat. 272, 304; 31 C.F.R. §§ 1010.610(a)(2)(i)-(v).

[20] Customer Identification Programs, Anti-Money Laundering Programs, and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator, 81 Fed. Reg. 58,425 (proposed Aug. 25, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-08-25/pdf/2016-20219.pdf.

[21] *Hearing on the Nomination of Steven Mnuchin to be Secretary of the Treasury, Senate Finance Committee*, Written Responses to Questions for the Record, at 29, 93 (Jan. 2017), https://dlbjbjzgnk95t.cloudfront.net/0884000/884398/mnuchinresponses.pdf.

[22] *See, e.g.*, Presidential Exec. Order on Reducing Regulation and Controlling Regulatory Costs (Jan. 30, 2017), https://www.whitehouse.gov/the-press-office/2017/01/30/presidential-executive-order-reducing-regulation-and-controlling.

[23] Maria Vullo, NYDFS Superintendent, Remarks Delivered at event hosted by the Exchequer Club (Jan. 18, 2017).

[24] Evan Weinberger, *NY To Keep Up Pressure on Banks in Age of Trump*, Law360 (Nov. 15, 2016), https://www.law360.com/articles/862656/ny-to-keep-up-pressure-on-banks-in-age-of-trump.

[25] *See* NYDFS Superintendent's Regulations Part 504, http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp504t.pdf; Press Release, NYDFS, *DFS Issues Final Anti-Terrorism Transaction Monitoring and Filtering Program Regulation* (June 30, 2016), http://www.dfs.ny.gov/about/press/pr1606301.htm.

[26] NYDFS Superintendent's Regulations § 504.1.

[27] *See* N.Y. Fin. Serv. Law § 301(c)(4) (giving NYDFS the authority to refer matters to the New York Attorney General); N.Y. Banking Law § 672 (prohibiting the falsification of books, reports, or statements of banks).

[28] The regulation is codified at 23 NYCRR § 500, http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.

[29] Covered entities have until March 1, 2018, to comply with the following provisions: 500.04(b) (annual CISO reports to the board of directors), 500.05 (penetration and vulnerability assessments), 500.09 (risk assessments), 500.12 (multi-factor authentication) and 500.14(b) (cybersecurity awareness training). Covered entities have until September 1, 2018, to comply with the following provisions: 500.06 (audit trails), 500.08 (application security), 500.13 (data retention and destruction), 500.14 (a) (monitoring of authorized users) and 500.15 (encryption). Covered entities have until March 1, 2019, to comply with the third-party service provider provision, section 500.11.

[30] Board of Governors of the Federal Reserve System, Interagency Guidelines Establishing Information Security Standards, § II, https://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm. *See* 23 NYCRR § 500.01(g) (defining "Nonpublic Information" as "all electronic information that is not Publicly Available Information and is: (1) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity; (2) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) Social Security number, (ii) driver's license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records; (3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.").

[31] SEC, *Examination Priorities for 2017* (Jan. 12, 2017), https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2017.pdf (SEC 2017 Exam Priorities); FINRA, *2017 Annual Regulatory and Examination Priorities Letter* (Jan. 4, 2017), http://www.finra.org/sites/default/files/2017-regulatory-and-examination-priorities-letter.pdf (FINRA 2017 Exam Priorities).

[32] *See* SEC 2017 Exam Priorities at 4-5.

[33] FINRA 2017 Exam Priorities, at 8.

[34] Staff of The Task Force to Investigate Terrorism Financing, Committee on Financial Services, U.S. House of Representatives, 114th Congress, Second Session, *Stopping Terror Finance: Securing the US Financial Sector* (Dec. 20, 2016), http://financialservices.house.gov/uploadedfiles/terror_financing_report_12-20-2016.pdf.

[35] FATF, *Anti-Money Laundering and Counter-Terrorist Financing Measures – United States, Mutual Evaluation Report* (Dec. 2016), http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf. The Financial Action Task Force is the international standard-setting body for AML/CFT. The FATF conducts peer reviews—called "mutual evaluations"—of its 37 member countries, including the United States, to assess compliance with its standards.

[36] The FATF conducted its on-site visit from January 18, 2016, to February 5, 2016.

[37] FinCEN issued its final customer due diligence rule on May 11, 2016, after the close of the FATF on-site visit.

[38] USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 314(a), 115 Stat. 272, 307.

[39] The Clearing House, *A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement* (Feb. 2017), https://www.theclearinghouse.org/-/media/tch/documents/tch%20weekly/2017/20170216_tch_report_aml_cft_framework_redesign.pdf. WilmerHale serves as special counsel to The Clearing House and assisted with the symposia and preparing the report.

[40] *Id.* at 3.

[41] Louis Nelson and Matthew Nussbaum, *White House puts Iran 'on notice,' won't rule out military force*, Politico (Feb. 1, 2017), http://www.politico.com/story/2017/02/iran-on-notice-trump-michael-flynn-234503.

[42] Exec.Order No. 13,660 of March 6, 2014, 79 Fed. Reg. 13,493 (Mar. 10, 2014), https://www.gpo.gov/fdsys/pkg/FR-2014-03-10/pdf/2014-05323.pdf; Exec. Order No. 13,661 of March 16, 2014, 79 Fed. Reg. 15,535 (Mar. 19, 2014), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/ukraine_eo2.pdf.

[43] Exec. Order No. 13,662 of March 20, 2014, 79 Fed. Reg. 16,169 (Mar. 24, 2014), https://www.gpo.gov/fdsys/pkg/FR-2014-03-24/pdf/2014-06612.pdf.

[44] Exec. Order No. 13,685 of December 19, 2014, 79 Fed. Reg. 77,357 (Dec. 24, 2014), https://www.gpo.gov/fdsys/pkg/FR-2014-12-24/pdf/2014-30323.pdf.

[45] U.S. Dep't of Treasury, OFAC, General License No. 10 under Executive Order 13,685 (Aug. 31, 2016), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/ukraine_gl10.pdf.

[46] U.S. Dep't of Treasury, OFAC, General License No. 11 under Executive Order 13,685 (Dec. 20, 2016), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/ukraine_gl11.pdf.

[47] Eli Stokols, *Trump eager to work with Putin*, Politico (Jan. 15, 2017), http://www.politico.com/story/2017/01/trump-russia-europe-putin-may-233644.

[48] Guy Faulconbridge and William James, *Trump's offer to Russia: an end to sanctions for nuclear arms cut*, Reuters (Jan. 16, 2017), http://www.reuters.com/article/us-usa-trump-russia-arms-deal-idUSKBN14Z0YE; Peter Nicholas, Paul Beckett and Gerald F. Seib, *Trump Open to Shift on Russia Sanctions, 'One China' Policy*, The Wall Street Journal (Jan. 13, 2017), https://www.wsj.com/articles/donald-trump-sets-a-bar-for-russia-and-china-1484360380.

[49] Julie Pace, *Trump wary of Russian deal; new advisers urge tougher stand*, AP (Mar. 4, 2017), http://bigstory.ap.org/article/8bf076a9e5314c19a28f79dbc5d967fe/amid-firestorm-trump-appears-waiver-russia-deal.

[50] *E.g.*, Ambassador Nikki Haley, *Remarks at a UN Security Council Briefing on Ukraine* (Feb. 2, 2017), https://usun.state.gov/remarks/7668.

[51] Press Release, U.S. Dep't of Treasury, *Statement from Secretary Mnuchin on OFAC Sanctions* (April 21, 2017), https://www.treasury.gov/press-center/press-releases/Pages/sm0052.aspx.

[52] Exec. Order No. 13,757 of December 28, 2016, 82 Fed. Reg. 1 (Jan. 3, 2017), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber2_eo.pdf.

[53] Press Release, Off. of Press Sec., The White House, *FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment* (Dec. 29, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and.

[54] OFAC also designated two additional individuals—Evgeniy Mikhailovich Bogachev and Aleksey Alekseyevich Belan—for their cyber-enabled misappropriation of financial information and personal identifiers for private financial

gain. OFAC stated that Mr. Bogachev developed the Zeus malware, which is associated with the theft of financial information and other criminal activity. According to OFAC, Mr. Bogachev directly benefited from the use of the malware by other cybercriminals, and he also used a form of "ransomware" to hold at least 120,000 U.S. victims' data hostage for financial gain in excess of $100 million. OFAC stated that Mr. Belan's attacks on at least three U.S.-based e-commerce companies' computer networks led to the theft of e-mail addresses, customer names and encrypted passwords, which he sold for private financial gain.

[55] Exec. Order No. 13,687 of January 2, 2015, 80 Fed. Reg. 819 (Jan. 6, 2015), https://www.gpo.gov/fdsys/pkg/FR-2015-01-06/pdf/2015-00058.pdf.

[56] U.S. Dep't of Treasury, Resource Center: Publication of Cyber-Related General License (Feb. 2, 2017), https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20170202_33.aspx.

[57] David Wright, *Trump threatens to roll back US-Cuba relations*, CNN (Nov. 28, 2016), http://www.cnn.com/2016/11/28/politics/cuba-trump-threat/.

[58] Elizabeth Gurdus, *Trump Threatens to Terminate US-Cuba Deal if 'Cuba is Unwilling to Make a Better Deal,'* CNBC (Nov. 28, 2016), http://www.cnbc.com/2016/11/28/trump-threatens-to-terminate-us-cuba-deal-if-cuba-is-unwilling-to-make-a-better-deal.html.

[59] Cuban Assets Control Regulations, 81 Fed. Reg. 4583 (Jan. 27, 2016), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cacr_20160126.pdf; Cuba Licensing Policy Revisions, 81 Fed. Reg. 4580 (Jan. 27, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-01-27/pdf/2016-01557.pdf.

[60] Cuban Assets Control Regulations, 81 Fed. Reg. 13,989 (Mar. 16 ,2016), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/fr81_13989.pdf; Cuba: Revisions to License Exceptions and Licensing Policy, 81 Fed. Reg. 13,972 (Mar. 16, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-03-16/pdf/2016-06019.pdf.

[61] Cuban Assets Control Regulations, 81 Fed. Reg. 71,372 (Oct. 17, 2016), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cacr_10142016.pdf; Cuba: Revisions to License Exceptions, 81 Fed. Reg. 71,365 (Oct. 17, 2016), https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2016/1569-81-fr-71365/file.

[62] Jenna Johnson, *A new Donald Trump emerges at AIPAC, flanked by teleprompters*, The Washington Post (Mar. 21, 2016), https://www.washingtonpost.com/news/post-politics/wp/2016/03/21/a-new-donald-trump-emerges-at-aipac-flanked-by-teleprompters/?tid=a_inl&utm_term=.3f1b05e2120d.

[63] Exec. Order No. 13,574, 76 Fed. Reg. 30,505 (May 25, 2011), https://www.gpo.gov/fdsys/pkg/FR-2011-05-25/pdf/2011-13173.pdf.

[64] Exec. Order No. 13,590, 76 Fed. Reg. 72,609 (Nov. 23, 2011), https://www.gpo.gov/fdsys/pkg/FR-2011-11-23/pdf/2011-30463.pdf.

[65] Exec. Order No. 13,622, 77 Fed. Reg. 45,897 (Aug. 2, 2012), https://www.gpo.gov/fdsys/pkg/FR-2012-08-02/pdf/2012-19055.pdf.

[66] Exec. Order No. 13,645, 78 Fed. Reg. 33,953 (June 5, 2013), https://www.gpo.gov/fdsys/pkg/FR-2013-06-05/pdf/2013-13523.pdf.

[67] Exec. Order No. 13,628, 77 Fed. Reg. 62,139 (Oct. 12, 2012), https://www.gpo.gov/fdsys/pkg/FR-2012-10-12/pdf/2012-25236.pdf.

[68] U.S. Dep't of Treasury, OFAC, General License H under the Iranian Transactions and Sanctions Regulations (Jan. 16, 2016), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/iran_glh.pdf.

[69] U.S. Dep't of Treasury, OFAC, Frequently Asked Questions Relating to the Lifting of Certain U.S. Sanctions Under the Joint Comprehensive Plan of Action (JCPOA) on Implementation Day, FAQ K.7 (last updated Dec. 15, 2016), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/jcpoa_faqs.pdf.

[70] U.S. Dep't of Treasury, OFAC, Guidance on the Provision of Certain Services Relating to the Requirements of U.S. Sanctions Laws (Jan. 12, 2017), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/compliance_services_guidance.pdf.

[71] Iranian Transactions and Sanctions Regulations, 82 Fed. Reg. 3330 (Jan. 21, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-01-21/pdf/2016-01227.pdf.

[72] U.S. Dep't of Treasury, OFAC, Statement of Licensing Policy for Activities Related to the Export or Re-Export to Iran of Commercial Passenger Aircraft and Related Parts and Services (Jan. 16, 2016), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/lic_pol_statement_aircraft_jcpoa.pdf.

[73] U.S. Dep't of Treasury, OFAC, General License J Authorizing the Reexportation of Certain Civil Aircraft to Iran on Temporary Sojourn and Related Transactions (July 29, 2016), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/iran_glj.pdf.

[74] U.S. Dep't of State, Annex II – Sanctions-related Commitments, https://www.state.gov/documents/organization/245320.pdf.

[75] U.S. Dep't of Treasury, Resource Center: List of Persons Identified as Blocked Solely Pursuant to Executive Order 13,599, https://www.treasury.gov/resource-center/sanctions/Programs/Pages/13599_list.aspx.

[76] Council Decision (CFSP) 2016/37 of 16 January 2016 concerning the date of application of Decision (CFSP) 2015/1863 amending Decision 2010/413/CFSP concerning restrictive measures against Iran, http://eur-lex.europa.eu/eli/dec/2016/37/oj; Council Decision (CFSP) 2015/1863 of 18 October 2015 amending Decision 2010/413/CFSP concerning restrictive measures against Iran, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015D1863.

[77] Exec. Order No. 12,957, 60 Fed. Reg. 14,615 (Mar. 17, 1995), https://www.gpo.gov/fdsys/pkg/FR-1995-03-17/pdf/95-6849.pdf; Iranian Transactions and Sanctions Regulations, 31 C.F.R. § 560.

[78] *See* U.S. Securities Exchange Commission, Notice Required by the Iran Threat Reduction and Syria Human Rights Act of 2012 to be Filed through EDGAR (Dec. 19, 2012), https://www.sec.gov/divisions/corpfin/cfannouncements/itr-act2012.htm.

[79] Sudanese Sanctions Regulations, 82 Fed. Reg. 4793 (Jan. 17, 2017), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/SSR_amendment.pdf.

[80] Exec. Order No. 13,761 of January 13, 2017, 82 Fed. Reg. 5331 (Jan. 18, 2017), https://www.gpo.gov/fdsys/pkg/FR-2017-01-18/pdf/2017-01197.pdf.

[81] North Korea Sanctions and Policy Enhancement Act of 2016, Pub. L. 114-122 (114th Cong.), 130 Stat. 93 (2016), https://www.congress.gov/114/plaws/publ122/PLAW-114publ122.pdf.

[82] Exec. Order No. 13,722, 81 Fed. Reg. 14,943 (Mar. 18, 2016), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/nk_eo_20160316.pdf.

[83] *See generally* U.S. Dep't of Treasury, Resource Center: North Korea Designations (July 7, 2016), https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20160706.aspx.

[84] Exec. Order No. 13,742, 81 Fed. Reg. 70,593 (Oct. 12, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-10-12/pdf/2016-24847.pdf.

[85] Exec. Order No. 13,739, 81 Fed. Reg. 63,673 (Sept. 16, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-09-16/pdf/2016-22454.pdf.

[86] U.S. Dep't of Treasury, Sanctions Pursuant to the Foreign Narcotics Kingpin Designation Act, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/narco_sanctions_kingpin.pdf (last updated Nov. 21, 2016).

[87] U.S. Dep't of Treasury, Resource Center: 2017 OFAC Recent Actions, https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/OFAC-Recent-Actions.aspx; U.S. Dep't of Treasury, Resource Center: OFAC FAQs: Other Sanctions Programs, General Licenses Issued Authorizing Certain Activities Pertaining to Panama, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#panama.

[88] Exec. Order No. 13,726, 81 Fed. Reg. 23,559 (Apr. 21, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-04-21/pdf/2016-09483.pdf.

[89] *See U.S. Dep't of Treasury v. Haider*, Civ. No. 15-1518, 2016 WL 107940 (D. Minn. Jan. 8, 2016).

[90] *In re Western Union Fin. Servs., Inc.*, FinCEN No. 2017-01 (Jan. 19, 2017) (Assessment of Civil Money Penalty), https://www.fincen.gov/sites/default/files/enforcement_action/2017-01-19/WUFSI%20Assessment%20of%20Civil%20Money%20Penalty-%201-19%20-%202017.pdf; *FTC v. Western Union Co.*, 1:17-CV-0110 (M.D. Pa. Jan. 20, 2017) (Stipulated Order for Permanent Injunction and Final Order); *see also* Press Release, Off. of Pub. Affairs, U.S. 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.

[91] *United States v. The Western Union Company,* 1:17-cr-00011-CCC, Dkt#. 3-1 (M.D. Pa. Jan. 19, 2017) (Statement of Facts, ¶¶ 1-2).

[92] *In re Western Union Fin. Servs., Inc.*, FinCEN No. 2017-01 (Jan. 19, 2017) (Assessment of Civil Money Penalty), https://www.fincen.gov/sites/default/files/enforcement_action/2017-01-19/WUFSI%20Assessment%20of%20Civil%20Money%20Penalty-%201-19%20-%202017.pdf; *FTC v. Western Union Co.*, 1:17-CV-0110 (M.D. Pa. Jan. 20, 2017) (Stipulated Order for Permanent Injunction and Final Order); *see also* Press Release, Off. of Pub. Affairs, U.S. 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.

[93]*In re Deutsche Bank AG* (Jan. 30, 2017) (NYDFS Consent Order), http://www.dfs.ny.gov/about/ea/ea170130.pdf.

[94] Press Release, NYDFS, *DFS Fines Deutsche Bank $425 Million for Russian Mirror-Trading Scheme* (Jan. 20, 2017), http://www.dfs.ny.gov/about/press/pr1701301.htm.

[95] *In re Intesa Sanpaolo* (Dec. 15, 2016) (NYDFS Consent Order), http://www.dfs.ny.gov/about/ea/ea161215.pdf.

[96] Press Release, NYDFS*, DFS Fines Intesa Sanpaolo $235 Million for Repeated Violations of Anti-Money Laundering Laws* (Dec. 15, 2016), http://www.dfs.ny.gov/about/press/pr1612151.htm.

[97] *In re Agricultural Bank of China Limited* (Nov. 4, 2016) (NYDFS Consent Order), http://www.dfs.ny.gov/about/ea/ea161104.pdf.

[98] *In re Mega International Commercial Bank Co., LTD.* (Aug. 19, 2016) (NYDFS Consent Order), http://www.dfs.ny.gov/about/ea/ea160819.pdf.

[99] *See* Press Release, NYDFS, *Industrial Bank of Korea Agrees to Strengthen Anti-Money Laundering Compliance and Controls at Bank's New York Branch* (Mar. 1, 2016), http://www.dfs.ny.gov/about/press/pr1603011.htm; Press Release, NYDFS, *National Bank of Pakistan Agrees to Enhance Anti-Money Laundering Compliance and Controls* (Mar. 24, 2016), http://www.dfs.ny.gov/about/press/pr1603241.htm.

[100] *In re Gibraltar Private Bank and Trust Company*, FinCEN No. 2016-01 (Feb. 25, 2016) (Assessment of Civil Money Penalty), https://www.fincen.gov/sites/default/files/enforcement_action/Gibraltar_%20Assessment.pdf.

[101] *In re Gibraltar Private Bank and Trust Company*, OCC No. 2016-018 (Feb. 22, 2016) (Consent Order for the Assessment of a Civil Penalty), https://www.occ.gov/static/enforcement-actions/ea2016-018.pdf.

[102] *In re Stearns Bank, N.A.*, OCC N. 2016-048 (Apr. 5, 2016) (Consent Order for a Civil Money Penalty), https://www.occ.gov/static/enforcement-actions/ea2016-048.pdf.

[103] *In re Merchants Bank of California, N.A.*, FinCEN No. 2017-02 (Feb. 16, 2017) (Assessment of Civil Money Penalty), https://www.fincen.gov/sites/default/files/enforcement_action/2017-02-27/Merchants%20Bank%20of%20California%20Assessment%20of%20CMP%2002.24.2017.v2.pdf.

[104] 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.

[105] *In re Merchants Bank of California, N.A.*, FinCEN No. 2017-02 (Feb. 16, 2017) (Assessment of Civil Money Penalty), at 4-5, https://www.fincen.gov/sites/default/files/enforcement_action/2017-02-27/Merchants%20Bank%20of%20California%20Assessment%20of%20CMP%2002.24.2017.v2.pdf.

[106] *In re Credit Suisse Secs. (USA) LLC*, FINRA No. 2013038726101 (Dec. 5, 2016) (Letter of Acceptance, Waiver and Consent), http://www.finra.org/sites/default/files/CreditSuisse_AWC_120516.pdf.

[107] *In re Oppenheimer & Co. Inc.*, SEC Rel. No. 74141 (Jan. 27, 2015) (Order Instituting Admin. and Cease-and-Desist Proceedings), https://www.sec.gov/litigation/admin/2015/33-9711.pdf; *In re Oppenheimer & Co. Inc.*, FinCEN No. 2015-01 (Jan. 26, 2015) (Assessment of Civil Money Penalty), https://www.fincen.gov/sites/default/files/enforcement_action/Oppenheimer_Assessment_20150126.pdf.

[108] *In re Raymond James & Assocs. Servs., Inc.*, FINRA No. 2014043592001 (May 18, 2016) (Letter of Acceptance, Waiver and Consent), https://www.finra.org/sites/default/files/RJFS_AWC_051816_0.pdf.

[109] *In re Albert Fried & Co., LLC,* SEC Rel. No. 34-77971 (June 1, 2016) (Order Instituting Admin. and Cease-and-Desist Proceedings), https://www.sec.gov/litigation/admin/2016/34-77971.pdf.

[110] *In re CG Tech., L.P., f/k/a Cantor G&W (Nevada), L.P. d/b/a Cantor Gaming*, FinCEN No. 2016-05 (Oct. 3, 2016) (Assessment of Civil Money Penalty), https://www.fincen.gov/sites/default/files/enforcement_action/2016-10-03/20161003%20Cantor%20Assessment%20Final.pdf.

[111] Press Release, U.S. Attorney's Off., E.D.N.Y., *Cantor Fitzgerald Affiliate to Pay More than $16 Million in Penalties and Forfeiture for Engaging in Illegal Gambling and Money Laundering Schemes* (Oct. 3, 2016), https://www.justice.gov/usao-edny/pr/cantor-fitzgerald-affiliate-pay-more-16-million-penalties-and-forfeiture-engaging.

[112] *In re Hawaiian Gardens Casino, Inc.*, FinCEN No. 2016-04 (July 15, 2016) (Assessment of Civil Money Penalty), https://www.fincen.gov/sites/default/files/enforcement_action/2016-09-09/20160715%20HG%20Assessment%20Final.pdf.

[113] *In re Sparks Nugget, Inc. d/b/a John Ascuaga's Nugget*, FinCEN No. 2016-03 (Apr. 5, 2016) (Assessment of Civil Money Penalty), https://www.fincen.gov/sites/default/files/enforcement_action/Sparks_Nugget_EA.pdf.

[114] *U.S. Dep't of Treasury v. Haider*, Civ. No. 15-1518, 2016 WL 107940 (D. Minn. Jan. 8, 2016).

[115] *In re Thomas E. Haider*, FinCEN No. 2014-08 (Dec. 18, 2014) (Assessment of Civil Money Penalty), https://www.fincen.gov/sites/default/files/enforcement_action/Haider_Assessment.pdf.

[116] *In re Raymond James & Assocs. Servs., Inc.*, FINRA No. 2014043592001 (May 18, 2016) (Letter of Acceptance, Waiver and Consent), https://www.finra.org/sites/default/files/RJFS_AWC_051816_0.pdf.

[117] *In re Charles Sanders*, OCC No. 2016-038 (Mar. 15, 2016) (Consent Order), https://www.occ.gov/static/enforcement-actions/ea2016-038.pdf.

[118] *In re Yaffar-Pena*, SEC Rel. No. 34-79124 (Oct. 19, 2016) (Order Instituting Admin. and Cease-and-Desist Proceedings), https://www.sec.gov/litigation/admin/2016/34-79124.pdf.

[119] *In re E.S. Financial Services, Inc. n/k/a Brickell Global Markets, Inc.*, SEC Rel. No. 77056 (Feb. 4, 2016) (Order Instituting Admin. and Cease-and-Desist Proceedings), https://www.sec.gov/litigation/admin/2016/34-77056.pdf.

[120] U.S. Dep't of Treasury, Enforcement Information for July 5, 2016, *Alcon Laboratories, Inc., Alcon Pharmaceuticals Ltd., and Alcon Management, SA, Settle Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations and the Sudanese Sanctions Regulations*, https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20160705_alcon.pdf.

[121] U.S. Dep't of Treasury, Enforcement Information for Nov. 14, 2016, *National Oilwell Varco, Inc. Settles Potential Civil Liability for Apparent Violations of the Cuban Assets Control Regulations, the Iranian Transactions and Sanctions Regulations, and the Sudanese Sanctions Regulations*, https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20161114_varco.pdf.

[122] U.S. Dep't of Treasury, Enforcement Information for February 8, 2016, *Barclays Bank Plc Settles Potential Civil Liability for Apparent Violations of the Zimbabwe Sanctions Regulations*, https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20160208_barclays.pdf.

[123] *Id.* at 1.

[124] *Commerzbank Deferred Prosecution Agreement* (Mar. 12, 2015), https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/12/commerzbank_deferred_prosecution_agreement_1.pdf; *Commerzbank Settlement Agreement*, OFAC No. 713262 (Mar. 11, 2015); *In re Commerzbank AG*, FRB No. 15-001-B-FB (Mar. 12, 2015); *In re Commerzbank AG* (Mar. 12, 2015) (NYDFS Consent Order), http://www.dfs.ny.gov/about/ea/ea150312.pdf.

[125] *Credit Agricole Deferred Prosecution Agreement* (Dec. 8, 2015); U.S. Dep't of Treasury, Enforcement Information for October 20, 2015, *Crédit Agricole Corporate and Investment Bank Settles Potential Civil Liability for Apparent Violations of Multiple Sanctions Programs*, https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20151020_cacib.pdf; *In re Credit Agricole*, FRB No. 15-028-B-FM (Oct. 19, 2015); *In re Credit Agricole* (Oct. 15, 2015) (NYDFS Consent Order), http://www.dfs.ny.gov/about/ea/ea151019.pdf.

[126] Inflation Adjustment of Civil Monetary Penalties, 82 Fed. Reg. 10,434 (Feb. 10, 2017), https://www.treasury.gov/resource-center/sanctions/Documents/fr82_10434.pdf.

[127] Press Release, Off. of Pub. Affairs, U.S. Dep't of Justice, *ZTE Corporation Agrees to Plead Guilty and Pay Over $430.4 Million for Violating U.S. Sanctions by Sending U.S.-Origin Items to Iran* (Mar. 7, 2017), https://www.justice.gov/opa/pr/zte-corporation-agrees-plead-guilty-and-pay-over-4304-million-violating-us-sanctions-sending.