SULLIVAN & CROMWELL LLP

March 3, 2016

2015 Year-End Review of BSA/AML and Sanctions Developments and Their Importance to Financial Institutions

Continued Trend in 2015 of Record-Setting Fines, Significant Criminal and Regulatory Enforcement Actions and Focus on Individual Accountability Means BSA/AML and Sanctions Compliance Must Remain a Focus of Boards of Directors and Senior Management of Financial Institutions

This memorandum highlights what we believe to be the most significant developments and trends during 2015 for financial institutions with respect to U.S. Bank Secrecy Act/anti-money-laundering ("BSA/AML") and U.S. sanctions programs, including sanctions administered by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"). In 2015, the overarching trend continued to be an intense focus on BSA/AML and sanctions compliance by multiple government agencies, combined with increasing regulatory expectations and significant enforcement actions and penalties, and an increased focus on individuals. Government agencies continued to emphasize money-laundering and terrorist-financing risks, threats and vulnerabilities seen in prior years, as well as the emergence of certain new threats associated with advances in technology. We do not see these trends abating in the near term.

This memorandum is aimed at keeping our clients and practitioners informed of regulatory and enforcement developments in the areas of BSA/AML and OFAC sanctions. We encourage you to contact us if you have any questions about the information and analysis presented in this memorandum or how the developments and trends we highlight may be relevant to your organization. Please follow our AML and Sanctions Watchlist for developments in BSA/AML and sanctions enforcement and compliance.

EXECUTIVE SUMMARY

In 2015, we continued to see record-setting fines and significant criminal prosecutions and enforcement actions against financial institutions for violations of BSA/AML and sanctions laws. As of year-end 2015, four of the five largest banks by asset size were subject to public enforcement actions addressing BSA/AML or sanctions compliance concerns. Of the 151 public enforcement actions issued by the federal banking agencies against financial institutions in 2015, 34 (approximately 22 percent) addressed primarily BSA/AML compliance concerns, while nine (approximately six percent) addressed both BSA/AML and OFAC or only OFAC sanctions compliance concerns. Accordingly, more than 28 percent of public enforcement actions issued by federal banking agencies against financial institutions in 2015 addressed BSA/AML and/or OFAC sanctions concerns. These statistics leave no doubt that BSA/AML and OFAC compliance risk management must remain a focus of boards of directors and senior management of financial institutions.

Importantly, in 2015 we saw a continued focus on holding individuals accountable in corporate cases. This emphasis was apparent in a new policy from the U.S. Department of Justice (the "DOJ") addressing individual liability in matters of corporate wrongdoing, new proposed regulations from the New York Department of Financial Services ("DFS"), public enforcement actions, and the public remarks of high-level agency officials. For example, Mary Jo White, Chair of the Securities and Exchange Commission ("SEC") stated that "in the enforcement arena, the most effective deterrent is strong enforcement against responsible individuals, especially senior executives," while Stanley Fischer, Vice Chairman of the Federal Reserve, observed that individuals responsible for some of the "worst aspects of bank behavior" have not been punished severely and that this may have resulted in misaligned incentives and ineffective risk management, and Benjamin M. Lawsky, then-Superintendent of the DFS, highlighted the DFS's "actions to expose and penalize misconduct by individual senior executives—including all the way up to the C-Suite, when appropriate."

We anticipate this focus will continue in 2016, with regulators and law enforcement increasingly seeking to hold individual directors, officers and employees accountable in cases arising from corporate investigations.

At the same time, we also saw an emphasis on traditional money-laundering and terrorist-financing risks, threats and vulnerabilities, both in the banking agencies' enforcement actions and in the publication of the National Money Laundering Risk Assessment ("NMLRA") and the National Terrorist Financing Risk Assessment ("NTFRA"). In 2015, regulators and law enforcement focused heavily on customer-based risk and, in particular, risks presented by third-party payment processors and correspondent banking customers. This is not a new emphasis, and it has almost certainly contributed to the "de-risking" we discuss later in this memorandum. Indeed, the NMLRA and NTFRA warn of the particular vulnerabilities associated with correspondent banking (and, in the case of the NMLRA, third-party payment processing).

The long-awaited assessments—the last NMLRA was published 10 years ago and this is the first NTFRA—provided insights into these and other familiar risks, threats and vulnerabilities facing the U.S. financial system, including: widespread use of cash (*e.g.*, bulk cash smuggling), use of funnel accounts and trade-based money-laundering ("TBML") schemes, use of structured transactions to avoid reporting requirements, unregistered money service businesses ("MSBs"), concealment of the nature, purpose, ownership and control of accounts (*e.g.*, master/sub accounts, omnibus accounts and intermediated relationships), AML compliance deficiencies, and complicit merchants and violators within financial institutions. The assessments also highlighted several risks, threats and vulnerabilities associated with advancements in technology, including virtual currency and cybercrime. In particular, according to the NMLRA, "the rapid evolution of the market, the development of new business models and entry of new virtual currency payments developers and providers—many from a non-financial services environment (*e.g.*, the technology sector), where industry is not as highly regulated as in the financial sector—together with the potential to operate without a domestic presence, is leading to service providers entering the market that do not comply with BSA obligations." As a result, virtual currencies and other new payment technologies are vulnerable to exploitation by cybercriminals for money-laundering purposes. The NTFRA similarly identified virtual currency and cybercrime as potential emerging terrorist-financing threats and vulnerabilities.

The NMLRA and NTFRA findings highlight a final trend we observed in 2015: the increasing convergence of cybersecurity and virtual currency, on the one hand, with BSA/AML and sanctions compliance, on the other hand. It is unclear what the practical implications of convergence will be. With respect to cybersecurity, regulators focused on cyber-preparedness and the incorporation of cybersecurity considerations into the BSA/AML frameworks of individual institutions. At the same time, there was a recognition that the response to cyber threats needs to be broad-based. Indeed, in the Cybersecurity Act of 2015, Congress acknowledged the need for a broad-based response, empowering institutions to share cybersecurity information with one another—information that may be key to thwarting money-laundering and terrorist financing.

With respect to virtual currencies, in 2015, the Conference of State Bank Supervisors issued a model regulatory framework, and at least one state issued final rules for regulating virtual currency firms, each of which includes provisions related to BSA/AML compliance, and the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") highlighted virtual currency as an ongoing priority, including through its first enforcement action against a virtual currency exchange.

In sum, the clear trend continues to be an intense focus on BSA/AML and sanctions compliance by multiple government agencies, combined with increasing regulatory expectations and significant enforcement actions and penalties, and an increasing focus on individuals. Institutions remain potentially vulnerable to all of the money-laundering and terrorist-financing risks, threats and vulnerabilities seen in

the past, plus an expanding list of new threats stemming from advances in technology. We do not see these trends abating soon. Accordingly, BSA/AML and OFAC compliance risk management must remain a focus of boards of directors and senior management of financial institutions, and financial institutions must remain aware of their vulnerabilities, assess the risk of their activities and client base, and take appropriate measures to mitigate those risks and remediate any deficiencies.

Table of Contents

I. CUSTOMER-BASED RISK

A. CONTINUED DE-RISKING PHENOMENON

In 2015, as was the case in 2014, both U.S. regulators and international standard-setting bodies continued to express concern that some institutions are "de-risking," or exiting entire business lines that carry increased risk. Principal among those risks are the potential repercussions from non-compliance with regulatory and supervisory expectations that seem increasingly difficult to achieve.[1] Groups of customers affected by what has become known as the "de-risking phenomenon" have also voiced concerns and directly confronted, through lobbying and litigation, the banking regulators seen as responsible for de-risking by virtue of those regulatory and supervisory expectations. To combat de-risking activity, regulators continue to clarify existing policies and discourage financial institutions from de-risking, as they did in 2014, but have also begun to plan concrete regulatory changes to address the factors currently driving de-risking activity.

Several negative side effects of de-risking are motivating regulators to take measures to address the phenomenon. Regulators are concerned that de-risking could force certain groups—both individuals and entities—out of the regulated financial system,[2] thus potentially preventing certain countries and industries from conducting commerce using the U.S. dollar, depressing global trade flows and straining global development.[3] The regulators also fear that the migration of transactions to unregulated financial systems could, paradoxically, undermine authorities' efforts to prevent financial crime and the financing of terrorist activity.[4] U.S. regulators continued to stress that current regulations and supervisory expectations do not require de-risking. Both U.S. and international standard-setting bodies have also begun to identify specific regulations and policies that lead to de-risking behavior, and have announced plans to modify these as necessary. The preliminarily successful legal challenge lodged by payday lenders claiming to have been affected by de-risking could also be motivating regulators' efforts to address the phenomenon. We discuss first this legal challenge and then turn to regulatory developments in 2015 related to de-risking, first with U.S. regulators and then with standard-setting bodies.

1. Challenges to Regulators

On September 25, 2015, the U.S. District Court for the District of Columbia declined to dismiss a complaint by a group of payday lenders claiming that informal guidance provided to banks by the Federal Deposit Insurance Corporation (the "FDIC"), the Office of the Comptroller of the Currency (the "OCC") and the Board of Governors of the Federal Reserve System (the "Federal Reserve") had placed pressure on those banks to exit relationships with their payday lender customers. The payday lenders argued that this harmed them by depriving them of access to the banking services necessary to do business.[5] The court held that the plaintiffs had sufficiently stated a claim that the defendant regulator had deprived them of

their constitutional right to due process. This case suggests a potential avenue for constitutional challenge of regulatory policy that some believe has led to de-risking in certain areas.

2. Reactions of U.S. Regulators and Treasury

Several U.S. regulators have maintained that their current policies do not encourage de-risking and urged institutions to instead improve risk management and controls and evaluate customers individually, rather than exiting business lines or otherwise engaging in de-risking. Speaking before a congressional committee, Martin Gruenberg, Chairman of the FDIC, highlighted the risks attendant to doing business with third-party payment processors ("TPPPs") stating that the FDIC "intended to ensure that institutions perform the due diligence, underwriting and ongoing monitoring necessary to mitigate the risks to their institutions."[6] The FDIC's position was repeated in its most recent annual report, stating: "[I]nsured institutions that properly manage customer relationships are neither prohibited nor discouraged from providing services to any customer operating in compliance with applicable law."[7] The OCC publicly shared this position: in a meeting of the Association of Certified Anti-Money Laundering Specialists in Manhattan, James F. Vivenzio, Senior Counsel for BSA/AML of the OCC, stated that the OCC is not pushing banks to cut off high-risk businesses such as online payday lenders from banking services.[8]

The Treasury Department has also clarified its policies and urged institutions not to engage in de-risking. In attempting to dispel criticisms that the Treasury Department had created a zero-tolerance regulatory regime with respect to illicit finance, David S. Cohen, Under Secretary for Terrorism and Financial Intelligence, stated: "The risk-based approach we expect of financial institutions does *not* imply a zero-tolerance regulatory regime. We recognize that it is not possible or practical for a financial institution to prevent every single potentially illicit transaction that flows through it. The Bank Secrecy Act requires that financial institutions establish and implement Anti-Money-Laundering/Combating the Financing of Terrorism ("AML/CFT") programs reasonably designed to detect, prevent, and report suspicious activity."[9] He also stated that recent regulatory actions "were not taken because of minor mistakes," but in response to "egregious cases" where banks deliberately broke the law and had significant fundamental AML and counter-terrorist financing failings. Adam Szubin, Acting Under Secretary for Terrorism and Financial Crimes, recently defined de-risking narrowly as "instances in which a financial institution seeks to avoid perceived regulatory risk by indiscriminately terminating, restricting, or denying services to broad classes of clients, without case-by-case analysis or consideration of mitigation options." He also stated that the current AML/CFT standards do not create a "zero tolerance, zero failure, or zero risk" system.[10] In addition, although the Treasury Department has been working to combat regional de-risking by consulting closely with central bank officials in the Gulf and Latin American regions, Acting Under Secretary Szubin stressed that the U.S. "will not dilute or roll back [its] AML/CFT standards, despite calls from some quarters to do so."[11]

While such statements have been important in clarifying that regulators do not intend for industry participants to exit entire business lines, but rather intend them to take a risk-based approach to managing the risk posed by particular groups of clients, there is still a perception that the threat of enforcement actions with severe negative implications for an institution must be taken seriously, and that clearer guidance is needed to lessen the de-risking phenomenon.

3. FATF's Efforts

In addition to discouraging institutions from engaging in de-risking, regulators have begun to consider how to modify policies and regulations to reduce the incentives motivating de-risking activity. The Financial Action Task Force (the "FATF") has been active on this front. As a result of its June plenary meeting, the FATF issued a statement identifying several specific policy areas in which FATF will work in cooperation with other regulators to improve standards and guidance in order to combat de-risking.[12] At its October plenary meeting, FATF confirmed that it and its associated financial regulators will maintain the monitoring of de-risking activity and its effects as a priority.[13] FATF also announced that it had identified regulatory expectations particularly relevant to de-risking activity. These include expectations relating to identification and management of risk with respect to correspondent banking and remittances entities, and appropriate levels of customer due diligence. According to its summary of the October plenary meeting, FATF will work with regulators to clarify expectations in these areas and expects to complete this work in 2016.

In 2015, FATF also published several pieces of guidance to regulators intended to assist them in providing regulatory clarity and thereby reducing financial institutions' incentives to de-risk in specific sectors. These publications include FATF's Guidance for a Risk-Based Approach to Virtual Currencies, designed to assist national-level regulators to develop appropriate AML/CFT laws and regulations applicable to virtual currency payment products and services.[14] The guidance is largely a tailored application of FATF's Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services, issued in 2013.[15] In 2015, FATF also published Guidance for a Risk-Based Approach: Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement, which encourages regulators and supervisors to ensure that financial institutions are taking a risk-based approach to implementing AML/CFT measures that is aimed at managing—not avoiding—risks.[16] For additional virtual currency developments, please see Part VI.

4. FSB's Efforts

The Financial Stability Board (the "FSB") has also announced plans to address de-risking. On November 6, 2015, the FSB issued a report discussing the problem of de-risking with respect to correspondent banking.[17] As discussed below, correspondent banking is an area that has received continued emphasis by regulators and has consequently experienced the de-risking phenomenon in a prominent way. The FSB has begun to consult with regulators and industry representatives to

understand the full extent of, and determine how to address, the issue, and has identified several areas in which regulators must clarify their expectations. These include:

- The level of customer due diligence necessary in higher-risk scenarios;
- The expectations for dealing with "high-risk jurisdictions" and the extent to which a "high-risk" designation affects all respondent banks in a jurisdiction that has been so identified; and
- The level of due diligence expected from correspondent banks, including whether building additional trust in local supervision could remove the respondent bank's correspondents' need to duplicate tasks such as reviewing the AML/CFT compliance efforts of a respondent bank.

The FSB has also identified areas in which regulators could modify their policies to encourage efficient risk-mitigating behavior in the correspondent-banking sector. These include, most notably:

- Incentivizing the use of good judgment by correspondent banks;
- Allowing for the use of information-sharing facilities by banks in a way that helps banks to meet regulatory expectations while satisfying data protection requirements; and
- Allowing for sharing customer information in a manner which meets regulatory expectations while complying with data protection and privacy laws.

To date, no action has been taken.

B. CORRESPONDENT BANKING

One area of customer-based risk that regulators continued to emphasize in 2015 was correspondent banking. Correspondent banking is generally considered by U.S. regulators to be higher risk because it allows a third-party bank to process transactions for its own customers through a U.S. financial institution that itself has no relationship with those customers. This continued emphasis was seen in several of 2015's significant enforcement actions by federal banking agencies. Consistent with prior actions, these actions focused on the application of due diligence and other BSA/AML requirements to foreign affiliates and branches. One notable example is the multi-agency resolution by Commerzbank AG and its New York branch ("Commerzbank New York") of potential civil and criminal liability for violations of, among other things, the International Emergency Economic Powers Act ("IEEPA") and the BSA. According to the settlement documents, one "significant failure" in Commerzbank New York's BSA/AML program was its failure to adequately monitor correspondent banking transactions, including by conducting due diligence on Commerzbank affiliates and branches. Commerzbank New York also did not assign risk ratings to its branches and affiliates. According to the settlement documents, this prevented Commerzbank New York from effectively monitoring correspondent banking transactions with its affiliates and, coupled with a lack of communication among Commerzbank entities, resulted in failures to file suspicious activity reports ("SARs"). For additional information about the Commerzbank settlement, please refer to our prior memorandum to clients.

Other relevant enforcement actions in 2015 include the Federal Reserve's June 2015 cease and desist order against Bank of the Orient, as well as the Federal Reserve Bank of New York's and DFS's June 2015 action against Cooperatieve Centrale Raiffeisen-Boerenleenbank B.A. ("Rabobank") and Rabobank's New York branch and the Federal Reserve of New York's and DFS's July 2015 action against China Construction Bank Corporation ("CCB") and CCB's New York branch. These actions, much like the Commerzbank settlement, generally include provisions addressing correspondent banking accounts maintained for foreign affiliates and/or branches and, like the Commerzbank actions, require the subject institution to treat its foreign affiliates/branches no differently than an unaffiliated bank.

U.S. regulators and law enforcement also emphasized in 2015 the need for U.S. branches of foreign banks to maintain or ensure their own access to due diligence information regarding customers of their foreign affiliates that are engaging in transactions through a correspondent banking account at the U.S. branch. For example, both the DOJ and the DFS criticized Commerzbank New York for maintaining correspondent accounts for foreign Commerzbank branches and affiliates without being able to access due diligence information about the customers of those branches and affiliates.[18] Although the DOJ's DPA with Commerzbank acknowledged that "the BSA does not require a financial institution to conduct due diligence of its customer's customers," the DOJ also emphasized that the financial institution is required to detect and report suspicious activity and that this is accomplished, in part, through due diligence on correspondent banking transactions, including by requesting information from the foreign affiliate correspondents. Although Commerzbank New York made such requests, those foreign affiliates consistently did not respond to those requests in a reasonable manner, and the DOJ's DPA suggested the U.S. branch therefore was not able to satisfy its obligations to detect and report suspicious activity.

C. OPERATION CHOKE POINT

"Operation Choke Point" is an enforcement initiative of the DOJ intended to stop banks and payment processors from providing financial services to merchants that are suspected of consumer fraud. The DOJ has not officially announced the termination of Operation Choke Point but issued its last subpoena under the initiative in August 2013.[19]

Bank customers affected by de-risking activity have alleged that the DOJ's Operation Choke Point strategy includes convincing bank regulators to encourage banks to terminate relationships with customers in industries carrying high risk of consumer fraud, such as the payday lending industry.[20] The industry's negative reaction[21] to this perceived DOJ strategy resulted in the FDIC's issuing of guidance that encouraged banks to take a risk-based approach to BSA compliance and stressed that the FDIC and other banking regulators do not impose a zero-tolerance regime.[22] Industry reaction may have also contributed to the House of Representatives' passage on February 4, 2016 of a bill intended to end Operation Choke Point by prohibiting a federal banking agency from formally or informally suggesting, requesting, or ordering a depository institution to terminate either a specific customer account, or group of

customer accounts, or otherwise restrict or discourage the depository institution from entering into or maintaining a banking relationship with a specific customer or group of customers, unless: (1) the agency has a material reason to do so, and (2) the reason is not based solely on reputation risk.[23] While analysts believe that the bill has little chance of passing in the Senate, the passage of this bill reveals that this program continues to receive attention from policy makers.[24]

Although not designed to identify and prosecute BSA/AML and OFAC violations specifically, Operation Choke Point has given rise to fines for failure to file SARs as required by the BSA. On March 10, 2015, CommerceWest Bank ("CommerceWest") entered into civil and criminal settlements with the DOJ in which it agreed to a $4.9 million monetary resolution, a deferred prosecution agreement in which it admitted to a willful violation of the BSA, and a permanent injunction requiring reforms to its fraud detection and prevention practices relating to TPPPs and certain merchants.[25] One of the allegations on which this settlement was based was a failure to file SARs with respect to the visibly suspicious conduct of a TPPP, despite the existence of several "red flags." The TPPP had been presenting remotely created checks on behalf of its merchant clients, many of whom experienced abnormally high return rates of 50%, including significant numbers of unauthorized transactions. In addition, other banks notified CommerceWest that the TPPP may have been facilitating fraud. As evidenced by the experience of CommerceWest, the Operation Choke Point initiative could increase the likelihood that a failure to file SARs, whether in connection with potential fraud or with potential violations of AML/CFT regulations, will be detected and serve as the basis for large fines.

II. ENFORCEMENT

As we observed earlier, more than 28 percent of the public enforcement actions by the federal banking regulators against financial institutions in 2015 addressed BSA/AML and/or OFAC sanctions concerns, leaving no doubt that BSA/AML and OFAC sanctions compliance continue to be areas of significant enforcement risk. We highlight below several notable developments and observations in enforcement in 2015, beginning with observations that apply across sectors and in both the BSA/AML and OFAC sanctions contexts. These cross-sector developments should be borne in mind by any institution facing enforcement measures to resolve BSA/AML or OFAC sanctions compliance concerns. We then turn to enforcement developments that are specific to the securities sector, the casino sector and the daily fantasy sports sector. We conclude with enforcement developments specific to OFAC sanctions.

A. CROSS-SECTOR DEVELOPMENTS

1. Individual Accountability

One notable enforcement-related observation in 2015 that applies across sectors and in both the BSA/AML and OFAC contexts is the continued focus on holding individuals accountable in corporate cases. In 2015, federal and state banking regulators, as well as the DOJ, the Financial Industry

Regulatory Authority ("FINRA") and the SEC, continued to emphasize the importance of holding individuals accountable in cases of corporate wrongdoing, including with respect to BSA/AML and OFAC sanctions compliance failings. This emphasis was seen in the public remarks of high-level officials from government agencies and self-regulatory organizations, a new DOJ policy, new DFS regulations, and the agencies' and FINRA's public enforcement actions. We also note a recent development in the ongoing litigation against the former Chief Compliance Officer ("CCO") of MoneyGram. As we mentioned in our prior memorandum to clients, in December 2014, the DOJ (on behalf of FinCEN) filed a criminal complaint against the former CCO seeking a $1 million penalty and an order enjoining the CCO from participating in the conduct of the affairs of any U.S. financial institution.[26] On January 8, 2016, the CCO's motion to dismiss the complaint was denied, with the court rejecting his argument that the statutory BSA/AML compliance program requirement, 31 U.S.C. § 5318(h), only applies to financial institutions, and not to individuals.

We anticipate that efforts by regulators and law enforcement to hold individual directors, officers and employees accountable for corporate wrongdoing will continue, if not intensify, in 2016, including a potential increase in the volume of actions against individuals and a ratcheting up of penalties sought against individuals such as prohibitions against future employment in the banking sector, civil monetary penalties and even criminal sanctions. As observed previously, BSA/AML and OFAC compliance are areas rife with complexities and are constantly undergoing change. If compliance officers and others with expertise in these areas perceive an increased personal risk for corporate missteps, the individuals best suited to handle BSA/AML-related challenges may decide that the risks outweigh the rewards. This could create an environment where only the largest and most well-heeled institutions can find qualified individuals to serve, and even large institutions may face difficulties given the perception that they entail a higher risk of potential BSA/AML violations.

a. Remarks on Individual Accountability

On February 25, 2015, Benjamin M. Lawsky, Superintendent of the DFS, delivered remarks addressing Wall Street accountability after the financial crisis and the prevention of money-laundering.[27] While acknowledging that the DFS does not have the authority to bring criminal prosecutions, Lawsky reported that the DFS had taken "a number of actions to expose and penalize misconduct by individual senior executives—including all the way up to the C-Suite, when appropriate." Lawsky explained that these actions include requiring senior executives to resign as part of enforcement actions and banning certain individuals from participating in the operations of DFS-regulated institutions. "[R]eal deterrence, in our opinion, means a focus not just on corporate accountability, but on individual accountability," stated Lawsky.

Federal regulators and self-regulatory organizations likewise emphasized the importance of holding individuals accountable for their actions. For example, FINRA's 2015 Regulatory and Examination

Priorities Letter, published on January 6, 2015, contained references to individuals involved in misconduct at regulated firms, cautioning that "[f]irms must protect their culture against individual bad actors" and emphasizing that FINRA's mission encompasses "shutting down bad practices and bad actors at the earliest possible time."[28] On March 12, 2015, Mary Jo White, Chair of the SEC, stated in remarks that "in the enforcement arena, the most effective deterrent is strong enforcement against responsible individuals, especially senior executives. In the end, it is people, not institutions, who engage in unlawful conduct."[29] She added that "the greatest disincentive for wrongdoing occurs when people believe that their own liberty, reputations and livelihoods are on the line and they recognize that real, personal consequences will follow from their misconduct." In remarks on June 1, 2015, Stanley Fischer, Vice Chairman of the Federal Reserve, highlighted several "major lessons learned" from the economic crises of the last 20 years.[30] According to Fischer, the principle that the private sector would manage risk efficiently and effectively "did not work out as predicted" and a possible reason is that "incentives are misaligned. One sees massive fines being imposed on banks. One does not see the individuals who were responsible for some of the worst aspects of bank behavior, for example in the Libor and foreign exchange scandals, being punished severely. Individuals should be punished for any misconduct they personally engaged in."

More broadly, in 2015, federal regulators emphasized the importance of cultural reform across the banking industry. For example, on November 5, 2015, the Federal Reserve Bank of New York hosted a conference entitled "Reforming Culture and Behavior in the Financial Services Industry."[31] During the event, Bill Dudley, the President of the Federal Reserve Bank of New York, and Christine Lagarde, Managing Director of the International Monetary Fund, spoke to industry leaders about the importance of personal integrity and accountability, encouraged bankers to consider their "broader social obligations" and challenged the industry to establish a reputation of trust.

b. DOJ Policy

Perhaps most significant, on September 10, 2015, Sally Quillian Yates, Deputy Attorney General of the United States, delivered remarks addressing individual liability in matters of corporate wrongdoing and announcing a new policy applicable to the DOJ's prosecutors and civil litigators.[32] The policy, documented in a September 9, 2015 memo from Yates, lists six "key steps" DOJ attorneys are to take in order to determine whether and to what extent individuals should be held accountable for corporate misconduct.[33] On November 16, 2015, Yates delivered remarks further discussing the policy and announcing that the DOJ would that day be "taking a big step forward" in implementing the policy into the "everyday work" of DOJ attorneys by issuing revisions to the United States Attorney's Manual (the "USAM").[34] Yates emphasized that the DOJ does not revise the USAM "all that often" and, when it does, "it's for something important"—when the DOJ wants to make clear that a policy is "at the heart" of what all DOJ attorneys do and that certain principles are "embedded" in DOJ culture. Further details on the DOJ's

policy and revisions to the USAM may be found in our previous memoranda to clients available here and here.[35]

c. DFS Regulation

Also significant, on December 1, 2015, the DFS published a proposed regulation requiring senior compliance officers at financial institutions chartered or licensed under the New York Banking Law (a "NY Financial Institution") to make an annual certification as to their institution's compliance with new transaction monitoring and filtering program requirements. This type of certification, if implemented, would present material additional personal risk for these BSA/AML compliance officers and would potentially further exacerbate reported difficulties in hiring and retaining qualified senior compliance officers.[36] The DFS's proposed regulation is discussed in greater detail in section III.A.2.

d. Public Actions

In addition to public declarations and revised policies, regulators and prosecutors have continued to take concrete steps in 2015 toward holding individuals accountable, in particular as part of high-profile corporate compliance investigations and enforcement actions.[37] The first such action in 2015 was the March 12, 2015 global settlement with Commerzbank AG (discussed in greater detail in section I.B) to address BSA/AML and OFAC compliance failures.[38] As part of that action, the Federal Reserve precluded Commerzbank from reemploying the individuals involved in the past actions or retaining them as consultants or contractors and required Commerzbank to continue to provide "substantial assistance" to the Federal Reserve in connection with its investigations of whether separate actions should be taken against individuals. The DFS required Commerzbank to terminate specific employees. As is common for DOJ actions, the DOJ required Commerzbank to cooperate with the DOJ in any ongoing investigation of current or former officers, directors, employees and agents of Commerzbank.

Less than two months later, on May 11, 2015, the Federal Reserve announced that it was barring five former private bankers and senior managers of Credit Suisse, AG, Zurich, Switzerland ("Credit Suisse") from employment in the U.S. banking industry.[39] The ban followed a 2011 indictment of the five individuals for assisting in the evasion of federal income taxes and the related 2014 global settlement with Credit Suisse. As part of the 2014 settlement, the Federal Reserve stated that it was continuing to investigate individuals and required Credit Suisse to terminate and not reemploy individuals who had been indicted.[40] The May 11, 2015 announcement is notable because it represents one avenue the Federal Reserve may pursue in holding individuals employed by foreign banks accountable for misconduct.[41]

On October 20, 2015, Crédit Agricole S.A. and its subsidiary, Crédit Agricole Corporate and Investment Bank, agreed to pay, collectively, a total of $787.3 million and enter into various settlement agreements with respect to apparent violations of U.S. sanctions programs. Much like the Federal Reserve's actions

against Commerzbank and Credit Suisse, the action against Crédit Agricole[42] prohibits the bank from re-employing individuals involved in the apparent sanctions violations or retaining them as consultants or contractors, and requires the bank to assist in ongoing investigations of individuals. The DFS's consent order requires Crédit Agricole to terminate a specific employee.

Less than a month later, on November 4, 2015, the Federal Reserve and DFS announced a total of $258 million in penalties against Deutsche Bank AG to address apparent violations of law related to U.S. sanctions. The Federal Reserve and DFS actions included similar provisions aimed at holding individuals accountable for misconduct.

While the actions against Crédit Agricole and Deutsche Bank included provisions aimed at holding individuals accountable for corporate misdeeds, neither included bans from employment in the U.S. banking industry, as found in the May 2015 Credit Suisse settlement.

2. Judicial Review of Settlements

Another notable enforcement-related observation in 2015 that applies across sectors and in both the BSA/AML and OFAC contexts is the potential for increased judicial scrutiny of settlements. On February 5, 2015, Judge Richard J. Leon of the United States District Court for the District of Columbia rejected a proposed Deferred Prosecution Agreement[43] ("DPA") between the DOJ and Fokker Services, B.V. ("Fokker") arising from admitted violations of U.S. sanctions laws. Citing the district court's "supervisory powers" and responsibility to "consider the public as well as the defendant," Judge Leon concluded that the agreement was "grossly disproportionate to the gravity of [Fokker's] conduct in a post-9/11 world" and that approval of the DPA would "undermine the public's confidence in the administration of justice and promote disrespect for the law." Judge Leon found fault with the DPA for a variety of reasons, including the relatively low monetary penalty amount ($21 million, consisting of the amount of illegal revenues), consisting only of disgorgement of revenues, the fact that no individuals would be prosecuted for their conduct, and the lack of an independent monitor to review remedial actions.

On appeal, the government argued, among other things, that Judge Leon exceeded his authority by rejecting the DPA and that judicial scrutiny of settlement agreements jeopardizes the government's ability to come to agreements with other defendants in the future. (The appeal remains pending at the time of this memorandum).[44]

Judge John Gleeson of the Eastern District of New York also has actively overseen a DPA between HSBC bank and the DOJ for AML and sanctions violations by HSBC. In 2013, Judge Gleeson asserted limited supervisory authority over approving or disapproving of deferred prosecution agreements that was greater than the authority that had previously been exercised by judges, although he did ultimately approve of the agreement.[45] In January 2016 Judge Gleeson ordered that a third-party compliance

monitor's report filed under seal in connection with the deferred prosecution agreement be redacted and unsealed.[46]

It remains to be seen whether judicial scrutiny of, and supervision over, the Fokker and HSBC agreements mark the beginning of a broader trend towards increased scrutiny of DPAs and similar court-approved settlement agreements.[47] However, each example lends a degree of uncertainty to any settlement with the government that requires court approval.

3. Waivers and Collateral Consequences

A third enforcement-related observation in 2015 that applies across sectors and in both the BSA/AML and OFAC contexts relates to the indirect consequences of BSA/AML and OFAC sanctions settlements, including with respect to securities and labor laws and regulations ("collateral consequences"). As discussed in our 2014 year-end review, as the severity of civil and criminal sanctions for BSA/AML and OFAC sanctions violations increases, the potential that collateral consequences also may result increases. These collateral consequences may be mitigated or eliminated by formal waivers issued by regulators. In 2015 there were indicia that it is becoming increasingly difficult for financial institutions to secure such waivers.

We discuss here two significant 2015 cases in which the SEC and the U.S. Department of Labor ("DOL") issued waivers that highlight this problem. We also discuss briefly waiver-related guidance issued by the SEC. The cases and guidance serve as a caution to institutions that the prospects of a waiver should not be taken for granted when deciding whether to voluntarily agree to an enforcement action that may carry collateral consequences. Indeed, the practice of granting waivers to corporate bad actors has garnered significant negative attention from some politicians, dissenting regulators and the media, who argue that waivers do not hold corporations accountable for their misconduct and eliminate the deterrent value of enforcement actions, and lawmakers are increasingly showing interest in this area. For example, one legislative proposal would require the SEC to "implement a more rigorous, fair, and public process" before waiving certain disqualifications in the securities laws.[48] It seems unlikely the debate over waivers of collateral consequences will be resolved in the immediate future. It is advisable for institutions contemplating a settlement to consider possible collateral consequences in advance and to ensure a plan is in place to manage such consequences.

a. Oppenheimer

On January 27, 2015, the SEC and FinCEN issued a cease and desist order and assessed civil money penalties, disgorgement, and interest of $10 million against Oppenheimer & Co. Inc. ("Oppenheimer"), a full-service broker-dealer, for violations of the BSA and securities laws.[49] On the same day, the SEC issued an order granting a waiver to Oppenheimer from the "bad actor" automatic disqualification under Rule 506(d) of Regulation D.[50] The disqualification renders a "safe harbor" exemption for private offerings

unavailable if an issuer has been the subject of specified enforcement actions, but the SEC may waive the disqualification upon a showing of good cause if the disqualification is not necessary under the circumstances. Oppenheimer had requested that the SEC waive disqualification resulting from the SEC and FinCEN actions in light of its commitments to make various changes to policies and procedures.

Commissioner Kara M. Stein and now former Commissioner Luis A. Aguilar dissented from the SEC's decision to grant the waiver,[51] citing a "long and unfortunate history of regulatory failures" and a "wholly failed compliance culture" at Oppenheimer. According to Commissioners Aguilar and Stein, the SEC could have sent "a clear message that there are meaningful consequences for firms that repeatedly and deliberately flout applicable laws and rules," but instead "turn[ed] a blind eye to [Oppenheimer's] repeated violations."

b. SEC Guidance

On March 13, 2015, in the aftermath of the SEC's decision on Oppenheimer's request for a waiver, the SEC's Division of Corporation Finance issued guidance regarding the factors that it considers when acting on requests for waivers of the "bad actor" automatic disqualification and various other disqualifications under Rules 505 and 506 and Regulation A. These factors include: (1) the identity of the individuals responsible for the misconduct; (2) the duration of the misconduct; (3) the remedial steps taken to address the misconduct and (4) the impact on the issuer or third parties, such as investors, clients or customers, if the waiver is denied. According to the guidance, the SEC will also consider whether the applicant has met its burden to show good cause, whether the conduct involved a criminal conviction or scienter-based violation, and whether the violation involved the offer and sale of securities, among other factors. The guidance also cautions that "[i]f warning signs were disregarded or the tone at the top of the party seeking the waiver condoned, encouraged or did not address the misconduct . . . these factors would weigh against granting a waiver." The subjective nature of these factors does little to clarify the circumstances that would merit a waiver of securities-related collateral consequences.

c. Credit Suisse

On October 1, 2015, following a 2014 guilty plea and sentencing for its role in helping U.S. taxpayers engage in tax evasion, Credit Suisse was granted an exemption from DOL allowing the institution to continue providing asset management services to U.S. retirement plans as a Qualified Professional Asset Manager ("QPAM").[52] In granting the exception, DOL emphasized that the misconduct underlying the criminal conviction did not involve Credit Suisse's affiliated or related QPAMs and imposed a number of conditions on Credit Suisse, notably that Credit Suisse inform its asset management clients of the criminal conviction, develop and implement a training program, be subject to an annual independent audit, and separate the investment and compliance operations of Credit Suisse QPAMs from the rest of Credit Suisse. These conditions go further than those imposed in previous DOL exemptions, and reflect the

continued pressure on DOL to take a tough stance on asset managers affiliated with an institution that has engaged in conduct that violates U.S. law.

4. Other Notable Actions

Three other notable actions occurred in 2015. In July, the FDIC and California Department of Business Oversight ("CDBO") issued a consent order against Banamex USA ("BUSA"), an indirect subsidiary of Citigroup. In October, the OCC issued a consent order against U.S. Bank National Association based on deficiencies in the bank's overall BSA/AML compliance program, and in November the OCC did the same with respect to Wells Fargo Bank, National Association.[53]

Other notable actions not yet mentioned include the OCC's April 2015 consent order for a civil money penalty against Lone Star National Bank, and the June 2015 actions by the DOJ, the FDIC and FinCEN against Bank of Mingo.

B. INDUSTRY-SPECIFIC DEVELOPMENTS

1. Securities Industry

In 2015, the SEC unambiguously signaled its intent to pursue enforcement actions against broker-dealers for BSA violations. Early in the year, SEC Enforcement Director Andrew Ceresney remarked that a "disturbingly large" number of securities firms filed zero SARs over "extended periods of time," raising questions about their compliance with their BSA obligations,[54] and that, while the SEC has historically pursued BSA violations in the context of enforcement matters involving other securities laws violations, "the incidence of SAR reporting suggests there is a need to pursue standalone BSA violations to send a clear message to the industry about the need for compliance." In more recent remarks on June 18, 2015, Director Kevin W. Goodman of the SEC's Office of Compliance Inspections and Examinations ("OCIE") elaborated on the focus of its approach to examining the AML programs, customer identification programs, and suspicious activity reporting of broker-dealers.[55]

The SEC's joint action with FinCEN against Oppenheimer in January 2015 reflects this enforcement emphasis.[56] In that action, the regulators levied $20 million in civil money penalties against Oppenheimer, representing the "largest civil money penalty ever against a broker-dealer for AML failures." The conduct at issue principally involved Oppenheimer's failure to detect and report suspicious activity related to penny stocks, which FinCEN described as typically "low-priced, thinly traded and highly speculative," and vulnerable to being used in unlawful transactions. According to FinCEN, there were various "red flags" that pointed to the need to undertake a systematic review of high-risk clients and transactions and potentially to file SARs, which Oppenheimer failed to do. Those "red flags" included, among others, penny stocks for which no registration statement was in effect for the sale, and customers who repeatedly deposited penny stocks in large blocks, many in paper certificate form, sold them shortly

thereafter and then immediately transferred the proceeds out of their account. Additional discussion concerning the settlement may be found in our AML & Sanctions Watchlist.[57]

FINRA has brought similar actions against its member firm broker-dealers. For instance, on December 21, 2015, FINRA fined Cantor Fitzgerald & Co. ("Cantor Fitzgerald") $6 million and ordered disgorgement of approximately $1.3 million in commissions in connection with the firm's unlawful sales of billions of unregistered microcap securities.[58] The firm was also sanctioned for failing to have an adequate supervisory or AML program in place that was tailored to detect "red flags" or suspicious activity connected to the firm's microcap activity. In keeping with recent trends seeking to impose individual accountability for corporate violations, two of Cantor Fitzgerald's executives were suspended and fined for their supervisory failures relating to such activity. Additional discussion concerning the settlement may be found in our memorandum to clients.[59]

2. Casino Industry

In 2015, FinCEN executed multiple enforcement actions against casinos and highlighted the casino industry in public remarks. Of FinCEN's ten public actions in 2015, three were against casinos,[60] including a $75 million civil money penalty against Hong Kong Entertainment (Overseas) Investments, Ltd. d/b/a Tinian Dynasty Hotel & Casino in June 2015—FinCEN's largest penalty against a casino for BSA violations. As recently as November 2015, Jennifer Shasky Calvery, the director of FinCEN, spoke about trends in BSA compliance and enforcement in the casino sector.[61] In June 2015, Associate Director of Enforcement Stephanie Brooker discussed a number of issues relevant to BSA compliance in the casino sector, in part highlighting key themes of FinCEN's enforcement approach, including individual accountability and heightened scrutiny of repeat offenders.[62]

3. Daily Fantasy Sports

Another area of increasing concern to FinCEN is the daily fantasy sports industry. In late 2015, Director Shasky Calvery reportedly stated that the daily fantasy sports industry "purports to have large volumes of funds moving through it" and that "[l]ike anything else, we will keep our eye on it."[63] Dealing with daily fantasy sports operators may carry implications for financial institutions with respect to their obligations to file SARs and general AML compliance obligations, as well as raise concerns under the Unlawful Internet Gambling Enforcement Act of 2006. Financial institutions that deal with the daily fantasy sports industry should be aware of the specific risks posed by that industry and ensure that their controls are designed to address those risks.

Daily fantasy sports operators have also drawn increased scrutiny from state authorities. In November 2015, the Office of the New York State Attorney General ("NYAG") served cease and desist letters on FanDuel, Inc. and DraftKings, Inc., determining that the companies' operations constituted illegal gambling.[64] On November 17, 2015, the NYAG commenced actions against the two companies before

the Supreme Court of the State of New York for New York County, seeking to enjoin the companies from doing business in New York due to repeated statutory violations of New York laws against illegal sports gambling. On December 11, 2015, the court granted the injunctions, finding that the NYAG had a "greater likelihood of success on the merits."[65] The injunctions have been stayed pending the companies' appeal of the Supreme Court's decision. Other states have also banned or regulated the operation of daily fantasy sports, and some state attorney generals have challenged the legality of daily fantasy sports.

It is unclear whether these developments pose legal risks for entities in the payments industry (such as credit card lenders and payment processors) that service daily fantasy sports operators. Some industry players have taken prophylactic action. On January 29, 2016, Vantiv Inc. reportedly notified its clients that it would stop processing transactions related to daily fantasy sports on February 29, 2016.[66] On February 5, 2016, Citigroup reportedly indicated that it would block debit and credit card payments by New York state residents to FanDuel and DraftKings.[67] Processing the transactions of daily fantasy sports operators presents unique risks to financial entities. Financial entities should therefore perform appropriate due diligence and take a risk-based approach to their relationships with daily fantasy sports operators.

C. OFAC SANCTIONS-SPECIFIC DEVELOPMENTS

In 2015, banking regulators and law enforcement continued to take action against institutions for the apparent circumvention of OFAC sanctions by using non-transparent payment methods, such as removing relevant information from payment messages or using cover payments or alternative payment methods. Indeed, in several OFAC sanctions-related enforcement actions highlighted in this memorandum, regulators and/or law enforcement faulted the subject bank for using non-transparent methods to facilitate the processing of U.S. dollar transactions involving sanctioned countries and/or specially designated nationals ("SDNs"). The settlement documents in the Crédit Agricole actions faulted the bank for removing information about sanctioned entities from payment messages sent from an ordering customer's financial institution through correspondent banks to a beneficiary customer's financial institution (so-called "wire stripping") and for using separate inter-bank payment messages (so-called "cover payments") that were presented in a way that prevented correspondent banks from obtaining any information about the ordering and beneficiary customers.[68] The DFS consent order against Deutsche Bank indicated that the bank had employed wire stripping and cover payments as well as instructed customers to use notes and code words to trigger special processing by bank staff to hide sanctions relationships.[69] Similarly, the settlement documents in the Commerzbank actions faulted Commerzbank for using various non-transparent payment methods to facilitate the processing of U.S. dollar transactions involving sanctioned countries and SDNs, including wire stripping and cover payments, as well as allowing the use of Commerzbank-issued checks in lieu of wire payments and instructing sanctioned

clients in methods for evading U.S. sanctions.[70] The use of non-transparent payment methods appears very likely to be a continuing area of interest going forward.[71]

Here, we discuss several additional actions against institutions for OFAC sanctions violations that are remarkable for other reasons: they expound a new theory of "facilitation," articulate limitations on receiving credit for voluntary self-disclosure, and highlight the critical importance of ensuring that screening systems are operating properly and are kept up-to-date.

1. "Facilitation" Through Business Decisions and Business Support

In a "landmark case" announced by the DOJ in March 2015, Schlumberger, a non-U.S. wholly owned subsidiary of Schlumberger Ltd. ("Schlumberger"), also a non-U.S. corporation and one of the largest oilfield services organizations in the world, pled guilty to conspiring to violate the IEEPA by facilitating the provision of oilfield services to customers in Iran and Sudan through Schlumberger's drilling and measurements business segment, which was headquartered in Texas. As a part of the plea agreement, Schlumberger paid approximately $232.7 million in criminal penalties, including a $155.2 million criminal fine, which constituted the largest criminal fine (but not total penalty) to date in connection with an IEEPA prosecution.[72] The violations asserted by the DOJ were based substantially on a "facilitation" theory premised on business decisions and business support from the United States of conduct by non-U.S. entities within the corporate organization that related to sanctioned countries (in this case, Iran and Sudan).[73] At the time, OFAC did not take parallel action. However, in an August 2015 announcement alleging facts similar to those alleged by the DOJ, OFAC stated that it had determined that a finding of violation with respect to Schlumberger "was the appropriate administrative response," particularly in light of the "parallel criminal case and the substantial criminal fine and forfeiture."

For additional information concerning the actions against Schlumberger, please refer to our AML & Sanctions Watchlist and our memorandum to clients.[74]

2. Failure to Obtain Credit for Voluntary Self-Disclosure

On August 27, 2015, OFAC announced that UBS AG ("UBS") had agreed to pay approximately $1.7 million to settle alleged violations of the Global Terrorism Sanctions Regulations by processing transactions related to securities held in custody in the United States for or on behalf of an individual UBS customer in Switzerland designated by OFAC.[75] Prior to the customer's designation in 2001, UBS in Zurich opened accounts for the customer that were used to engage in investments in different markets. Although UBS placed blocks and restrictions on the customer's account after its designation by OFAC (and other jurisdictions, including Switzerland), which prohibited the client from withdrawing or transferring funds outside of UBS, UBS continued to engage in investment-related activity on behalf of the customer, including processing U.S. Dollar securities-related transactions to or through the United States. UBS considered these transactions to be "internal transfers" and the securities transactions never generated

any alerts in UBS's systems used for screening external transfers. The only aspect of the securities transactions that contained the clients' name were internal entries allocating transfers in the clients' various accounts. In March 2008, a U.S. custodian identified that certain securities were beneficially owned by the sanctions-target client, and filed a blocked property report with OFAC. In November 2012, following removal of the client from the Swiss sanctions list, UBS elected to close the customer's accounts. During the process of initiating wire transfers to another financial institution to effect close-out of the client's position, UBS's sanctions filter generated alerts against the customer's name as an individual on OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List"). OFAC did not afford UBS credit for voluntarily self-disclosing those violations to OFAC. OFAC concluded that these "were not voluntary self-disclosures within the scope of OFAC's [regulations] because they were substantially similar to another apparent violation of which OFAC was already aware." In keeping with past OFAC practice,[76] this case demonstrates that an institution may not receive credit for self-disclosing violations that are uncovered in an investigation of violations that were not self-disclosed if those transactions are substantially similar to those under investigation.

This enforcement action also highlights the importance of financial institutions taking appropriate measures to ensure compliance with all applicable sanctions when they have operations or otherwise conduct business in multiple jurisdictions that have implemented sanctions against particular persons (individuals or entities) or countries, and raises awareness regarding the sanctions obligations for foreign financial institutions, including those that purchase, sell, transfer or otherwise transact in U.S. securities, or that process transactions to or through the United States.

3. Screening System Failures

At least two OFAC sanctions-related enforcement actions in 2015 highlight the importance of ensuring that screening systems are operating properly and are kept up to date with OFAC's changes to sanctions programs and designated persons.

In March 2015, OFAC announced that PayPal, Inc. ("PayPal") had agreed to pay over $7.6 million to settle alleged violations of sanctions programs administered by OFAC.[77] In addition to allegedly failing to use screening technology and procedures to identify potential involvement of U.S. sanctions targets in transactions that PayPal processed, OFAC asserted that PayPal's automated interdiction filter was not "working properly" for approximately six months and failed to alert on certain prohibited transactions. When the filter eventually alerted on these transactions, PayPal staff allegedly failed to comply with the company's internal policies and procedures, causing PayPal not to block the account or report it to OFAC for over four years. For additional information on this enforcement action, please refer to our memorandum to clients.[78]

In October 2015, OFAC announced a finding of violation against BMO Harris N.A. ("BMO Harris"), as the successor to Marshall and Ilsley Bank ("M&I Bank"),[79] in connection with M&I Bank's processing of funds

transfers for the purpose of paying for Iranian-origin carpets in violation of 31 C.F.R. § 560.204. M&I on-boarded the carpet producer as a customer in 2009, when the importation into the United States of Iranian-origin carpets was permitted under a general license, and M&I Bank put the name of the customer in its false hit list. However, when OFAC revoked the pertinent general license in September 2010, M&I did not remove the customer from the false hit list and continued to process payments involving the customer. As noted by OFAC, the action against BMO Harris highlights the risks associated with failing to implement proper procedures and controls to ensure that internal proprietary sanctions lists are properly reviewed following changes to the SDN List and/or to the sanctions programs administered by OFAC. The action also highlights the necessity that companies screen both transactions and customers as part of their OFAC compliance regimes.

III. BSA/AML REGULATORY DEVELOPMENTS

A. PROPOSED AML REGULATIONS TO BROADEN SCOPE OF APPLICATION OF AML REQUIREMENTS

1. FinCEN's Proposed AML Rules for Investment Advisers

On September 1, 2015, FinCEN published a notice of proposed rulemaking (the "Proposed AML Rule"),[80] requiring certain "large" investment advisers (*i.e.*, advisers that have $100 million or more in regulatory assets under management) that are registered or required to be registered with the SEC (the "Covered RIAs") to establish AML programs and file SARs with FinCEN pursuant to the BSA.

The Proposed AML Rule was long expected by the industry as it effectively replaces two previous proposals that FinCEN withdrew in 2008—a 2003 proposal that would have imposed AML requirements on a narrower category of advisers and a 2002 proposal that would have required unregistered investment companies to establish AML programs.[81] Although the Proposed AML Rule comes as no surprise, the scope of the Proposed AML Rule has nonetheless generated significant industry comment.

First, the Proposed AML Rule would subject a broad range of investment advisers to the AML program and SAR-filing requirements because it covers all large RIAs. It includes, for example, private fund advisers, subadvisers, non-U.S. advisers (with respect to their U.S. operations) and investment advisers to registered investment companies. In addition, in the preamble, FinCEN notes the possibility of expanding the Proposed AML Rule to cover certain advisers that are exempt from registration with the SEC and state-regulated investment advisers.[82] Several commenters have requested FinCEN to exclude non-U.S. RIAs from the scope of the Proposed AML Rule, noting that the proposed coverage of such RIAs may violate the jurisdictional limits of the BSA and may subject non-U.S. RIAs to conflicting or duplicative regulatory requirements across jurisdictions.[83]

Second, the Proposed AML Rule would extend to all advisory activities of the Covered RIAs. A number of commenters have argued that some of these advisory services are provided in relation to activities or accounts that generally do not pose a high risk of engaging in money-laundering activities—for example, investment advisory activities for accounts held for publicly traded companies and pension plans.[84]

The Proposed AML Rule would make three significant changes to the regulatory expectations imposed on RIAs:

- It would include Covered RIAs within the definition of "financial institution" in the BSA regulations, thus requiring Covered RIAs to comply with several obligations generally applicable to financial institutions under the BSA (*e.g.*, filing currency transaction reports ("CTRs") and keeping records relating to the transmittal of funds);
- It would require Covered RIAs to develop and implement a written AML program and file SARs with FinCEN; and
- It would delegate to the SEC the authority to examine Covered RIAs for compliance with the Proposed AML Rule.

Consistent with the approach reflected in the USA PATRIOT Act, the Proposed AML Rule is designed to allow Covered RIAs to develop a risk-based AML program rather than imposing a "one-size-fits-all" requirement.

The AML program must be approved in writing by the board of directors of the Covered RIA. The proposed requirements for the AML program are consistent with those applicable to other financial institutions, and would require a Covered RIA, at a minimum, to:

- Establish and implement policies, procedures, and internal controls based upon the Covered RIA's assessment of the money-laundering or terrorist financing risks associated with its business;
- Designate an officer of the Covered RIA responsible for implementing and monitoring the operations and internal controls of the AML program;
- Provide ongoing training for appropriate employees (and for the employees of any agent or third-party service provider) in BSA requirements that is tailored to the particular employees; and
- Provide for periodic independent testing of the AML program by the employees of the Covered RIA or its affiliates or by unaffiliated service providers to ensure that the program complies with the Proposed AML Rule and functions as designed.

Although FinCEN is not currently proposing to apply a customer identification program requirement or customer due diligence requirements, FinCEN anticipates addressing both of these issues with respect to Covered RIAs in subsequent rulemakings.

Consistent with SAR filing requirements for other financial institutions, the Proposed AML Rule would require a Covered RIA to report, on a confidential basis, any suspicious transaction that is conducted or attempted by, at, or through the Covered RIA and that involves or aggregates at least $5,000 in funds or other assets, within 30 days after the Covered RIA becomes aware of the suspicious transaction. The

new SAR filing requirement applies to transactions initiated after the implementation of an AML program required by the Proposed AML Rule. However, Covered RIAs may and will be encouraged to begin filing SARs as soon as practicable on a voluntary basis upon the issuance of the final rule.

In addition to concerns regarding the scope of investment advisers and advisory activities covered by the Proposed AML Rule, commenters have asked FinCEN, among other things, to remove a requirement that a Covered RIA assess the AML risks not only of its fund clients, but also of any investors in such funds. Commenters have sought the removal of this "look-through" requirement, noting that an RIA may not have access to information about fund investors, particularly given the highly intermediated nature of the fund business.

2. New York Department of Financial Services Issues Proposed Transaction Monitoring and Filtering Program Requirements and Annual Senior Compliance Officer Certification

On December 16, 2015, the DFS published its proposed regulation (the "Proposed Regulation") in the New York State Register, setting forth for NY Financial Institutions the specific attributes of a transaction monitoring and filtering program to ensure compliance with applicable federal BSA/AML laws and regulations and OFAC sanctions.[85] The proposed attributes of the transaction monitoring and filtering programs extend well beyond formal regulatory requirements published by federal authorities, but are generally consistent with regulatory expectations reflected in the Federal Financial Institutions Examination Council's ("FFIEC") BSA/AML Examination Manual[86] and recent enforcement actions by the federal banking agencies and FinCEN for banks and branches of foreign banks.[87]

Most notably, in keeping with the general trend in the enforcement context of emphasizing personal accountability, the Proposed Regulation, as drafted, would introduce an annual certification requirement for senior compliance officers, which poses an unprecedented element of risk for these officers, including the risk of criminal penalties (as drafted). The Proposed Regulation, including the form of certification, would require the senior compliance officer to certify that the transaction monitoring and filtering program requirements are satisfied. The certifying officer would face potential criminal penalties in the event of an "incorrect" or "false" certification. Although the Proposed Regulation refers to "incorrect" or "false" certifications without qualification, the proposed form of certification includes a qualifier that the information provided is to the officer's "best knowledge." At the same time, however, the Proposed Regulation does not explicitly provide an "intent" standard for the imposition of criminal penalties.

Additional discussion concerning the Proposed Regulation may be found in our memorandum to clients.[88]

The effective date of the Proposed Regulation would be immediate on final issuance and would apply to all "state fiscal years" beginning April 1, 2016. The comment period has been extended to March 31, 2016.

B. OTHER REGULATORY MEASURES TO ADDRESS MONEY-LAUNDERING CONCERNS

1. FinCEN Targets Areas of Money-Laundering Concern with Geographic Targeting Orders

This year, FinCEN issued two Geographic Targeting Orders ("GTOs"), and renewed and broadened a 2014 GTO,[89] imposing certain requirements on non-financial institutions to address specific areas of money-laundering concern. Under the BSA and implementing Treasury regulation,[90] FinCEN has authority to issue GTOs that impose additional reporting and recordkeeping requirements on one or more domestic financial institutions or non-financial trades or businesses in a geographic area, with the potential for civil or criminal penalties against the targeted business and its officers, directors, employees or agents for non-compliance. To issue such an order, FinCEN is required to find that reasonable grounds exist to conclude that the GTO is necessary to carry out the purposes of the BSA and prevent evasion. Though FinCEN has used GTOs in the past, it has employed this tool with greater frequency in recent years, issuing two GTOs in 2014, two in 2015 and two in the first month of 2016 alone.[91] Although the GTO requirements have been imposed on non-financial institutions, they should also be used as a guide by financial institutions of areas of increased risk or regulatory focus, which may warrant enhanced due diligence of companies within scope of the GTOs.

This year's GTOs include the following:

- On April 21, 2015, FinCEN issued a GTO that requires approximately 700 exporters of electronics (including cell phones) located near Miami, Florida, including any of their agents, subsidiaries, and franchises, to record and report to FinCEN additional information on certain transactions involving cash and certain negotiable instruments.[92] The GTO was issued as a result of law enforcement investigations, which revealed that many of these businesses were being exploited as part of sophisticated TBML schemes in which drug proceeds in the United States were being used to pay for goods that were shipped to South America and sold for local currency, which was ultimately transferred to drug cartels. TBML has been an area of increased FinCEN focus since at least 2010, when FinCEN released an advisory to financial institutions on filing SARs regarding TBML.[93] Additional discussion concerning this GTO may be found in our memorandum to clients.[94]
- On July 13, 2015, FinCEN issued a GTO requiring check cashers in certain areas of southern Florida[95] to temporarily enhance the identification requirements for customers cashing Federal tax refund checks. The GTO is intended to combat the increase in "stolen identity tax refund fraud." Typical schemes of concern to FinCEN involve criminals filing fraudulent tax returns after stealing a victim's identity and then cashing the refund checks at local check cashers using fake identification to evade law enforcement. FinCEN, the IRS, and the U.S. Attorney's Office for the Southern District of Florida are particularly concerned that identity thieves are attempting these schemes outside of tax-filing season to catch financial institutions off guard and slip through their anti-money-laundering controls. The GTO will therefore cover a time period in which the proportion of fraudulent tax refund transactions is high compared to the relatively low total volume of transactions. The GTO requires check cashers in Miami-Dade and Broward counties to obtain and record, at the time of the transaction, additional identifying information about customers cashing tax refund checks over $1,000.[96] Additional discussion concerning this GTO may be found in our AML & Sanctions Watchlist.[97]

2. FinCEN Proposes Special Measures Against an Andorran Bank While Withdrawing Similarly Proposed Special Measures Against Lebanese Canadian Bank SAL

FinCEN again this year proposed[98] special measures against an institution—Banca Privada d'Andorrà ("BPA")—that the Treasury proposed to designate as a foreign financial institution of primary money-laundering concern. As is commonly the case, the preliminary finding by the Treasury and the issuance of the proposed special measures alone had very severe consequences for BPA. Although BPA's shareholders are fighting this designation—filing suit against FinCEN in the U.S. District Court for the District of Columbia seeking rescission of FinCEN's notice of finding and setting aside the proposed rulemaking—as usual, the impact was immediate. In BPA's case, for example, several banks quickly froze BPA's correspondent bank accounts, BPA's Spanish business filed for bankruptcy, and its Panamanian and Andorran units were seized by local regulators. Following these developments, on February 19, 2016, FinCEN announced that it was withdrawing its findings and proposed rulemakings regarding BPA after having determined that it no longer posed a money-laundering threat to the U.S. financial system, in light of the suspension of its business operations. The court is now considering whether BPA's claims challenging the withdrawn notice of findings and the notice of proposed rulemaking can proceed or are now moot.

FinCEN's ability to use special measures was successfully challenged by FBME Bank Ltd, a Tanzanian bank with significant operations in Cyprus ("FBME") that obtained a preliminary injunction against a FinCEN final rule imposing special measures against it.[99] A day before the final rule was scheduled to take effect, the U.S. District Court for the District of Columbia granted FBME's motion for a preliminary injunction,[100] noting that (i) FinCEN had provided insufficient notice to FBME of the unclassified, non-protected information on which FinCEN relied during the rulemaking proceedings; and (ii) FinCEN had failed to adequately consider at least one alternative to the special measure it sought to impose. Following this ruling, in November 2015, FinCEN re-opened all aspects of the FBME final rule for comment. Well before the court's ruling, however, the Central Bank of Cyprus had effectively taken over the management of FBME and had appointed an administrator to run FBME. In December 2015, the Central Bank of Cyprus revoked the license for FBME's Cyprus branch and imposed fines on FBME for failure to comply with AML requirements. Notwithstanding these developments in FBME's particular case, however, it is as yet unclear whether, and to what extent, FinCEN will review or change its rulemaking procedures for special measures.

In any event, the court's finding in FBME's case only speaks to FinCEN's rulemaking process, not the basis on which FinCEN issues proposed special measures in the first place. The court also placed on record its disinclination to "second guess FinCEN's exercise of its broad discretion in finding that FBME pose[d] a primary money-laundering concern, or its resulting imposition of the . . . special measure."

The limited nature of the FBME ruling makes it unlikely that it will apply to special measures proposed against other institutions. In many cases, the initial designation by itself is likely to have serious consequences for financial institutions. For example, this year, FinCEN withdrew its Notice of Proposed Rulemaking ("NPRM") seeking to impose special measures against Lebanese Canadian Bank SAL ("LCB") because the bank no longer exists as a foreign financial institution.[101] On September 20, 2011, seven months after FinCEN's NPRM, the Lebanese central bank and monetary authority, the Banque du Liban, revoked LCB's banking license and delisted LCB from its registry of banks. Subsequently, LCB's former shareholders sold LCB's assets and liabilities to another financial institution.

IV. SANCTIONS REGULATORY DEVELOPMENTS

A. INTRODUCTION

Unlike in previous years, where sanctions program developments have largely consisted of the expansion of existing sanctions or the issuance of new ones, in 2015, most attention was focused on the easing of sanctions on Cuba and Iran, taking into account the declaration in early 2016 of "Implementation Day" for the Joint Comprehensive Plan of Action (the "JCPOA")[102]—historic actions, given that both countries effectively have been subject to comprehensive sanctions for many years. However, despite the popularity of sanctions relief in the press and otherwise, in fact the relief is limited. At present, both sanctions programs continue to place broad restrictions on U.S. persons' ability to engage with Iran and Cuba and, as shown above, enforcement has remained a priority. Nonetheless, with the majority of U.S. secondary sanctions against Iran lifted (albeit subject to certain terms and conditions), and the lifting of most E.U. and U.N. sanctions and the Iran-related sanctions of many other jurisdictions, many non-U.S. persons potentially could decide to engage in business with Iran that was avoided when sanctions were more prevalent. Even so, those persons must ensure that the transactions are not subject to U.S. jurisdiction.

In 2015, the United States implemented new sanctions programs for Venezuela and Burundi, both of which target "bad actors" (for more information on the Venezuela sanctions program, please see our memorandum to clients and AML & Sanctions Watchlist post),[103] and a third program designed to address malicious cyber-enabled activities conducted outside of the United States that threaten the national security, foreign policy or economic health of the United States (for more information on cybersecurity-related sanctions, please see section V.A). In addition, the Hizballah International Financing Prevention Act of 2015, which aims to curtail funding of Hizballah's activities by raising the possibility of secondary sanctions for foreign financial institutions that knowingly conduct business with Hizballah by restricting or eliminating their access to U.S. correspondent or payable-through accounts, became law.

Following an active year in 2014, in 2015 OFAC issued no new sanctions with respect to Russia's role in the destabilization and annexation of the Crimea region of Ukraine. However, OFAC issued several

general licenses authorizing certain Crimea-related activities and also issued guidance to further define the scope of sanctions and to deter attempts to circumvent the sanctions.

Finally, we note that in the United Kingdom, Her Majesty's Treasury ("HMT") has indicated that it will focus on increased implementation and awareness of financial sanctions through the establishment of an Office of Financial Sanctions Implementation ("OFSI") within HMT. Although HMT representatives have stated that OFSI will not be focused on enforcement, the UK 2015 Summer Budget also contains plans to enact legislation increasing penalties for non-compliance. It remains to be seen whether this increased focus will result in significant additional risk associated with sanctions compliance in the United Kingdom.

The discussion below highlights developments that we believe are most likely to have a significant impact on financial institutions.

B. IRAN

With respect to Iran, the possibility of relief in 2015[104] has given way to real, although limited, U.S. sanctions relief in 2016, ahead of what was widely considered the likely timeframe. The comprehensive solution was announced on July 14, 2015 in the JCPOA in which the P5+1 agreed to suspend and eventually eliminate certain E.U., U.N. and U.S. nuclear-related sanctions against Iran in exchange for Iran's demonstrating that it is using its nuclear program exclusively for peaceful purposes. The JCPOA, however, does not permit any substantial additional dealings between Iran and U.S. persons or transactions subject to U.S. jurisdiction. Thus, U.S. persons continue to be subject to broad and comprehensive restrictions on trade, investment, and dealings with Iran. Even with relief of the secondary sanctions, non-U.S. persons must observe the terms and conditions of that relief, and still may violate U.S. law if they engage in transactions with Iran that are subject to U.S. jurisdiction, such as U.S. dollar transactions involving Iran that are cleared in the United States by U.S. financial institutions. OFAC has published guidance and frequently asked questions explaining in detail the extent of sanctions relief and its effects on various types of entities and activities.[105]

1. United States

On Implementation Day, the United States suspended, but did not permanently terminate, most secondary sanctions applicable to various sectors of Iran's economy, subject to certain terms and conditions. These include, most notably, a suspension of secondary sanctions for engaging in financial and banking transactions with the Central Bank of Iran or financial institutions of Iran and most other specified Iranian financial institutions (but excluding certain institutions such as Ansar Bank, Mehr Bank, and Bank Saderat), the National Iranian Oil Company, Naftiran Intertrade Company and the National Iranian Tanker Company. In addition to relaxing secondary financial sanctions, the United States suspended most other secondary sanctions, including those relating to underwriting, insurance, and reinsurance, the energy and petrochemical sectors, the shipping, shipbuilding and port sectors, gold and

other precious metals industries, software and industrial metals industries, the automotive sector, and trade in nuclear-related commodities. In addition, many, but not all, Iranian persons were removed from U.S. sanctions designations lists.

A number of secondary sanctions remain, including:

- Significant transactions with any Iran-related SDN or any SDN designated in connection with Iranian proliferation of weapons of mass destruction or support for international terrorism, or the Islamic Revolution Guard Corps and its designated agents or affiliates; and
- Sale, supply, or transfer to or from Iran of graphite, raw or semi-finished metals such as aluminum and steel, coal, and software for integrating industrial processes if sold, supplied or transferred to an end-user that is an SDN or for an end use that includes military or ballistic missile programs of Iran or with Iranian nuclear activities inconsistent with the JCPOA.

In addition to lifting secondary sanctions, on Implementation Day, OFAC issued General License H that in effect reverses the extension of the obligation to comply with the U.S.-imposed trade and investment sanctions to U.S.-owned or -controlled non-U.S. entities, subject to significant conditions and exceptions that can complicate the utility of the license. Chief among these are that no U.S. person may facilitate the transactions, including the U.S. parent entity, subject to very limited exceptions (such as for certain IT-shared services); no SDN may be involved in the transaction; the transaction, if it were conducted in the United States, may not violate any other OFAC sanctions program; and the ban on direct or indirect export and re-export of goods and services from the United States to Iran remains in place.

OFAC also has issued a general license to allow the import to the United States of Iranian-origin carpets and foodstuffs, including caviar and pistachios. In addition, OFAC released the Commercial Aircraft Statement of Licensing Policy, creating a framework for the exportation of civil aircraft, parts, and associated services to Iran if the licensed items and services are used exclusively for commercial passenger aviation (but not exports to SDNs).

2. European Union

The European Union has suspended the vast majority of its nuclear-related sanctions including restrictions applicable to E.U. persons with respect to certain transactions with Iran in the financial, banking, insurance, oil and gas, petroleum, shipping and shipbuilding and other transport industries; trade in gold and other precious metals; banknotes and coinage.[106] However, a number of sanctions remain in force involving sanctions targeted at human rights abuses.

C. CUBA

With respect to Cuba, limited easing of the Cuban embargo occurred throughout 2015. In January and September 2015, and again in January 2016, OFAC made a number of revisions to the Cuban Asset Control Regulations ("CACR") designed to implement the policy changes announced by President Obama on December 17, 2014 of further empowering and engaging the Cuban people, and increasing U.S.

persons' ability to interact with Cuban persons.[107] Although these revisions have eased certain elements of the Cuban embargo, particularly in the areas of travel, telecommunications, remittances, certain financial services and support for the Cuban people, the changes are incremental and the broad-based Cuban embargo remains in place. Transactions between the United States, or persons subject to U.S. jurisdiction, and Cuba generally remain prohibited unless otherwise authorized or exempt. The changes do authorize financial institutions to process additional types of transactions involving Cuba, but these transactions generally are restricted to those in which the underlying activity is also permitted. The relaxations permitting new activities are generally intended to facilitate interaction and information-sharing between U.S. and Cuban individuals, rather than to facilitate commerce and build broad commercial ties between the United States and Cuba. Despite the Obama administration's policy shift, those undertaking activity in reliance on the new authorizations must take care to ensure that their activity strictly conforms to the terms and conditions of the regulations, which are very detailed and technical.

Although travel for tourist activities continues to be prohibited by the CACR, OFAC amended the CACR to ease the regulatory burden associated with travel to Cuba for permitted reasons. Among other changes, OFAC generally licensed certain types of travel to, from or within Cuba that previously could only be conducted after receiving specific permission from OFAC. With the amendments, there are now 12 generally licensed categories of travel to Cuba.[108] OFAC also expanded the scope of permitted "travel-related transactions" that may be conducted during permitted travel to, from or within Cuba. Most important for financial institutions, OFAC's amendments enable travelers to use U.S. credit and debit cards in Cuba for authorized expenses, and financial institutions are permitted to enroll merchants to process those transactions. Financial institutions subject to U.S. jurisdiction are permitted to engage in all transactions incident to the processing and payment of credit cards, debit cards, stored value cards, checks, drafts, travelers' checks and similar instruments used or negotiated in Cuba by any person engaging in authorized "travel-related transactions" in Cuba.[109] Financial institutions are permitted to rely on the traveler when determining whether an individual's travel is authorized for purposes of processing Cuba travel-related transactions, unless the financial institution knows or has reason to know that the travel is not authorized.[110]

In addition, OFAC's revisions to the CACR include the issuance of a general license which permits U.S. depository institutions to establish and maintain correspondent accounts at financial institutions in Cuba, provided the accounts are used only for transactions authorized under the CACR.

OFAC also implemented changes that affect how U.S. depository institutions treat wire transfers involving Cuba or a Cuban national. Previously, U.S. depository institutions were required to block all payments in which Cuba or a Cuban national had an interest (i.e., freeze the funds and keep them in a segregated account until otherwise instructed by OFAC), to the extent such payments were not otherwise authorized by or exempt from the CACR. OFAC issued a new general license authorizing U.S. depository

institutions to reject, instead of block, such funds transfers that originate and terminate outside the United States, provided that neither the originator nor the beneficiary is a person subject to U.S. jurisdiction, and provided that prohibited officials of the Cuban government or prohibited members of the Cuban Communist Party do not have an interest in the transfer.[111] The general license also authorizes U.S. depository institutions to process funds transfers in which Cuba or a Cuban national have an interest that originate and terminate outside the United States, provided that neither the originator nor the beneficiary is a person subject to U.S. jurisdiction and provided that the funds transfer would be authorized under the CACR if the originator or beneficiary were a person subject to U.S. jurisdiction.[112]

On January 16, the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") issued Cuba sanctions-related revisions to the Export Administration Regulations ("EAR"), which regulate the transfer of U.S.-origin "dual-use" goods and services (i.e., goods or services that have both civilian purposes and potential military applications).[113] The new BIS regulations generally complement OFAC's revisions by relaxing the EAR's licensing regime in areas similar to those relaxed by OFAC.

On May 29, 2015, the U.S. Department of State announced that it rescinded Cuba's designation as a State Sponsor of Terrorism.[114] Although rescission of the designation has no immediate effect on OFAC's Cuba-related sanctions, it allows for the easing of other restrictions related to the provision of foreign assistance to the government of Cuba and the export of munitions, goods and technology to Cuba. In its announcement, however, the Department of State made clear that "the United States [still] has significant concerns and disagreements with a wide range of Cuba's policies and actions," although these concerns "fall outside the criteria relevant to the rescission of a State Sponsor of Terrorism designation." Nonetheless, rescission of the designation is important, and may be relevant for issuers required to file reports with the U.S. Securities and Exchange Commission ("SEC"). The staff of the SEC has reviewed filings, and has issued comment letters, regarding disclosure of dealings with state Sponsors of Terrorism in the past.

On September 18, OFAC and BIS announced additional changes to the CACR and EAR.[115] Among other changes, OFAC's revisions allow certain additional persons subject to U.S. jurisdiction, such as authorized travelers and U.S. persons authorized to maintain a physical presence in Cuba, as described below, to open and maintain bank accounts in Cuba for authorized purposes. The revisions permit certain additional financial transactions, including removing the limit on donative remittances to Cuban nationals other than prohibited officials from the Cuban Government or the Cuban Communist Party, unblocking previously blocked remittances and certain previously blocked funds transfers, and permitting persons subject to U.S. jurisdiction to receive remittances in the United States from most Cuban nationals, wherever located.[116] OFAC's revisions to the CACR also authorize all persons subject to U.S. jurisdiction to provide goods and services to Cuban nationals who are individuals that are located in a

third country, and allow certain U.S. persons, such as news bureaus and providers of telecommunications and Internet-based services, to establish a physical presence in Cuba.

Despite the liberalization of certain portions of the Cuban sanctions regime, a general ban on trade and investment, and in dealings in property in which a Cuban national has an interest, remains in place. Transactions between the United States, or persons subject to U.S. jurisdiction, and Cuba remain generally prohibited unless authorized or exempt.[117] As noted above, the changes announced by OFAC in 2015 are in the nature of authorizations on permissions, are limited in nature, and application therefore is very detailed and technical. Despite the Obama administration's policy of engagement with Cuba, care must be taken to ensure that any activity undertaken in reliance on the new authorizations strictly conforms to the applicable terms and conditions.

D. UKRAINE/RUSSIA AND CRIMEA REGION

Although no new Ukraine-related/Russia sanctions were issued, OFAC issued several general licenses authorizing certain Crimea-related activities and issued guidance regarding the scope of existing sanctions.[118] For more information on Ukraine/Russia-related sanctions imposed in 2014, see our memorandum to clients.[119]

1. General Licenses

In 2015 OFAC issued general licenses allowing U.S. persons, including financial institutions, to engage in specified transactions with individuals in the Crimea region of Ukraine. Subject to certain restrictions, General License No. 6 authorizes U.S. persons to send and receive, and U.S. financial institutions to process, funds transfers that are noncommercial, personal remittances to or from the Crimea region of Ukraine or for or on behalf of an individual ordinarily resident in the Crimea region of Ukraine,[120] even if there is no U.S. person acting as the remitter or beneficiary.[121] U.S. financial institutions processing such transfers may rely on the originator of the remittance in determining whether the funds transfer complies with the terms of the license, as long as the transferring institution does not know or have reason to know that the funds transfer is not authorized.

OFAC also issued a general license authorizing the operation of an account in a U.S. financial institution for an individual ordinarily resident in the Crimea region of Ukraine, other than an individual whose property and interests are blocked, as long as the transactions processed through the account: (i) are of a personal nature, and not for use in supporting or operating a business; (ii) do not involve transfers directly or indirectly to the Crimea region of Ukraine or for the benefit of individuals ordinarily resident in Crimea unless the transfers are authorized by General License No. 6; and (iii) are not otherwise prohibited.[122]

Additional licenses issued in 2015 authorize certain transactions related to telecommunications and mail,[123] and the exportation or reexportation from the United States or by U.S. persons of services

incident to the exchange of personal communications over the Internet to persons in the Crimea region of Ukraine.[124]

2. Circumvention Guidance

On July 30, OFAC issued a Crimea Sanctions Advisory to highlight some of the practices that have been used to circumvent or evade U.S. sanctions involving Crimea.[125] The evasive practices included a pattern or practice of repeatedly omitting address information for originators or beneficiaries ordinarily resident in Crimea from Society for Worldwide Interbank Financial Telecommunication ("SWIFT") messages and the obfuscation of references to Crimea in trade transactions and associated agreements and documentation. In addition, some parties may list Crimean counterparties on financial and trade documents as being located in Russia, since Russia claims sovereignty over the Crimea region of Ukraine, making it more difficult for U.S. financial institutions to identify trade involving that region.

OFAC recommends that U.S. persons and persons conducting business in or through the United States adopt the following measures to mitigate these patterns or practices:

- Ensure that transaction-monitoring systems include appropriate search terms corresponding to major geographic locations in Crimea, and not simply references to "Crimea";
- Request additional information from parties (including financial institutions, corporate entities and individuals) that have previously violated or attempted to violate U.S. sanctions on Crimea; and
- Clearly communicate U.S. sanctions obligations to international partners when discussing OFAC sanctions compliance expectations with correspondent banking and trade partners.

3. Sectoral Sanctions Guidance

Finally, OFAC issued FAQs clarifying how the prohibitions on extension of credit to entities subject to the Ukraine/Russia-related sectoral sanctions (the "SSI entities") apply in the context of letters of credit and contractual payment terms. Under Directives 1, 2 and 3,[126] issued under E.O. 13662, U.S. persons and persons in the United States are prohibited from transacting in, providing financing for, or otherwise dealing in new debt with an SSI entity if the debt has a maturity period longer than 90 days (for Directives 1 and 3) or 30 days (for Directive 2). FAQ 395 clarified that, in the case of letters of credit, the restrictions apply when the SSI entity is the *applicant* or the *issuing bank* (although extensions of credit under a letter of credit with a tenor of less than 30 or 90 days, as applicable, are not prohibited). U.S. persons may deal in (including acting as the advising or confirming bank or as the applicant) or process transactions under a letter of credit in which an entity subject to Directive 1, 2 or 3 is the *beneficiary*.[127] These actions would not violate the Directives because the "subject letter of credit does not represent an extension of credit" to the SSI entity.

FAQ 419 focused on the Directives' restrictions on debt in the context of contractual payment terms in transactions involving the sale of goods to an SSI entity, the provision of services to and subscription arrangements involving SSI entities or progress payments for long-term projects. OFAC stated the debt

restrictions would apply to such transactions and, if the payment terms exceed 30 or 90 days, as applicable, such payment terms "generally constitute[] a prohibited dealing in debt of the SSI entity."[128]

V. CYBERSECURITY

Cybersecurity continued to be an area of focus of the Obama administration, legislators, regulators and standard-setting bodies, and this focus is likely to increase in light of the steady stream of reported data breaches and other cyber-related crimes. In response to a number of recent high-profile cyber attacks initiated outside the United States, including the November 2014 release of confidential data belonging to Sony Pictures Entertainment, the president and U.S. regulators have adopted a number of measures to address cyber crime, including the use of sanctions to deter and punish those committing or attempting to commit cyber-related crimes. Although regulators are focusing on cyber-preparedness and the incorporation of cybersecurity considerations into the AML frameworks of individual institutions, there is also recognition that the response to cyber threats will need to be broad-based.

A. SANCTIONS

On January 2, 2015, President Obama authorized additional sanctions against North Korea and the Workers' Party of North Korea (the "Workers' Party") in response to the November 2014 release of confidential data belonging to Sony Pictures Entertainment.[129] Executive Order 13687 (E.O. 13687) authorized the Treasury Department to add individuals and entities tied to the North Korean government or the Workers' Party to the SDN list, and suspended the entry of such individuals in the United States, if non-U.S. citizens. On the same day, OFAC designated three entities and 10 individuals as SDNs.[130]

On April 1, the president issued Executive Order 13694 ("E.O. 13694") authorizing asset-blocking sanctions against persons found to have engaged in or supported significant malicious cyber-enabled activities.[131] As noted by President Obama upon initiation of the program, "cyber threats pose one of the most serious economic and national security challenges to the United States, and my Administration is pursuing a comprehensive strategy to confront them."

Under the order, the Secretary of the Treasury is authorized to designate as SDNs individuals and entities determined to be responsible for or complicit in certain cyber-enabled activities outside the United States that pose a significant threat to the national security, foreign policy, economic health or financial stability of the United States. The Executive Order is intended to address cyber-enabled activities that harm or compromise critical infrastructure, disrupt computers or computer networks, or misappropriate funds, information or trade secrets, but that may be beyond the reach of other authorities available to the U.S. government because of jurisdictional or other issues.

Also on April 1, OFAC issued a set of related FAQs.[132] Among other things, the FAQs clarify that the measures in the order are directed against significant malicious cyber-enabled activities that have the

purpose or effect of causing specific enumerated harms, and are not designed to prevent or interfere with legitimate cyber-enabled academic, business or non-profit activities. The FAQs specifically provide that E.O. 13694 is not intended to interfere with or target:

- Legitimate activities to ensure and promote the security of information systems, such as penetration testing and other methodologies, or to prevent or interfere with legitimate cyber-enabled activities undertaken to further academic research or commercial innovation as part of computer security-oriented conventions, competitions or similar "good faith" events;
- Legitimate network defense or maintenance activities performed by computer security experts and companies as part of the normal course of business on their own systems or systems they are otherwise authorized to manage; and
- Victims of malicious cyber-enabled conduct, including the unwitting owners of compromised computers.

According to Secretary Jacob Lew, "[t]he Treasury Department is committed to protecting the U.S. financial system from a range of state and non-state actors." While the new authority under E.O. 13694 is a "powerful tool," the Treasury "intend[s] to use this authority carefully and judiciously against the most serious cyber-threats to protect" critical U.S. infrastructure.[133] To date, no individuals or entities have been targeted for sanctions under the authority of E.O. 13694.

On December 31, 2015, OFAC issued regulations implementing E.O. 13694, including the executive order's asset-blocking provisions.[134] The regulations contemplate specific and general licenses, including those related to the provision of legal services. OFAC intends to supplement the new rules with a more comprehensive set of regulations, which may include additional interpretive and definitional guidance and additional general licenses and statements of licensing policy.[135]

B. REGULATORY RESPONSES TO CYBER THREATS

The FFIEC has continued to take a leadership role in the financial institution community in developing a coordinated approach to cyber threats, as reflected in its publication of cybersecurity priorities for 2015, which included a Cybersecurity Assessment Tool, released in June, designed to help institutions "identify their risks and determine their cybersecurity preparedness" over time by comparing the institution's cybersecurity risk profile with its "maturity level" (*i.e.*, the effectiveness of its cybersecurity controls and risk management) in several categories.[136] The FFIEC's priorities also include developing information sharing mechanisms among financial institutions, as well as with law enforcement. This initiative will be enhanced by the recent passage of the Cybersecurity Act of 2015 (the "Cybersecurity Act"), which generally shields private entities that share and receive cybersecurity-related information from civil, regulatory and antitrust liability if the sharing activity is conducted in accordance with the terms of the Cybersecurity Act.

Regulators also continued to explore the nexus between cybersecurity and BSA/AML in 2015. In a March speech to the Institute of International Bankers, Comptroller of the Currency Thomas J. Curry highlighted

that "the goals of BSA/AML and cybersecurity are increasingly converging" and noted that "[t]errorists, drug cartels, and cybercriminals all have a need to generate cash and move money . . . ."[137] These statements were echoed in a June report in which the OCC identified cybersecurity as a "top supervisory concern" and stated that the rapid pace of technological change presents a significant risk in banks' BSA/AML efforts.[138]

In October, FinCEN introduced a new category of "Cyber-related" SARs in its annual review of aggregated SAR-filing activity from the previous year in light of the increasing prevalence of cyber-related incidents.[139] The cyber-related category includes SARs filed in connection with any online banking fraud, unauthorized Internet transaction, email hack, unauthorized online transfer, email compromise, online bill pay fraud, online gambling, mobile banking fraud, online wire, cyber banking, online banking internal transfer, phishing email, computer intrusion or email fraud.[140]

Finally, several regulators and commentators recently have emphasized that a key tool in minimizing BSA/AML and cybersecurity threats will be to increase information-sharing across banks and have endorsed statutory safe harbors for banks that file SARs and share information about bad actors and financial crimes with one another.[141] As noted, this initiative likely will be furthered by the December 18 adoption of the Cybersecurity Act and the subsequent release by the U.S. Department of Homeland Security of guidance regarding the sharing of information relating to potential cyber threats between the private sector and the government.

VI. VIRTUAL CURRENCIES

Virtual currencies remained a hot topic in 2015 with an increased intersection with BSA/AML. In the United States, developments included the first state-level comprehensive regulatory framework for firms engaging in virtual currency businesses, the promulgation of a model framework for regulating virtual currency activities at the state level, and other state-level developments. The DFS continues to pursue virtual currency regulation, having published its final BitLicense rules in June 2015 and approved the first BitLicense application in September.[142] Certain of these developments involve the imposition of new BSA/AML requirements. Also in 2015, various federal agencies, including FinCEN, issued rulings and enforcement actions clarifying the application of federal regulations to firms dealing in virtual currencies. Virtual currency regulation has similarly drawn attention internationally, as reflected in the June 2015 FATF release, Guidance for a Risk-Based Approach to Virtual Currencies.[143]

A. THE EVOLVING REGULATORY FRAMEWORKS

1. FinCEN

Leading up to 2015, FinCEN provided various regulatory guidance relating to virtual currencies, including guidance issued on March 18, 2013 on the application of FinCEN regulations to administrators,

exchangers and users of virtual currencies and administrative rulings relating to that guidance.[144] On August 14, 2015, FinCEN issued an administrative ruling regarding the applicability of MSB regulations under the BSA to an unnamed company that holds precious metals in custody for its customers and issues digital proofs of custody ("digital certificates") that can be linked to the customers' wallets on the bitcoin blockchain ledger.[145] FinCEN found that the company was an administrator of the digital certificates, which constituted commodity-backed virtual currency. As a consequence (and also based on an unrelated finding that the company was a dealer in precious metals, precious stones or jewels), FinCEN ruled that the company was a money transmitter subject to FinCEN's MSB regulations under the BSA and therefore required to register with FinCEN and comply with certain BSA requirements. In reaching this decision, FinCEN noted that the company could not rely on the exemption afforded to companies that "accept[] and transmit[] funds solely for the purpose of effecting a *bona fide* purchase or sale of the real currency or other commodities for or with a customer" because by issuing a freely transferable digital certificate of ownership to a customer, the company was allowing unrestricted transfer of value to other customers and third parties and was "no longer limiting itself to the type of transmission of funds" necessary to the execution of a currency or commodity sale.

2. New York State

On June 3, 2015, the DFS announced the release of its final BitLicense rules for regulating virtual currency firms, including virtual currency exchanges, and on September 22, 2015, the DFS announced the approval of its first BitLicense application from Circle Internet Financial, a virtual currency firm, that already had a state money-transmission license.[146] The rules set forth AML compliance provisions for licensees, including AML program, customer identification program, SAR filing and other reporting and recordkeeping requirements, which are analogous to the federal AML rules.[147] Elements of these rules that have attracted industry concern include:

- Unlike the New York Banking Law, these rules do not explicitly state that compliance with applicable federal AML requirements will constitute compliance with the AML requirements under the BitLicense rules.
- These final BitLicense rules may apply to licensees that are not subject to federal AML rules. For instance, the rules provide that licensees that are not subject to a federal SAR requirement must still file SARs with the DFS on a form prescribed by the DFS. However, the DFS rules regarding SARs differ from the federal rules in important ways; for example, the DFS rules do not provide the filer with safe harbor from civil liability.
- The rules also provide that licensees involved in virtual currency transactions that do not have a federal currency transaction reporting requirement must notify the DFS of such transactions.
- The new BitLicense rules require the application of enhanced due diligence to accounts maintained for non-U.S. persons and non-U.S. licensees in order to detect money-laundering activity,[148] as well as a prohibition on the maintenance of any relationships with foreign shell companies.

Subsequent to the release of the final BitLicense rules, it was reported that a number of bitcoin companies ceased operations in New York in light of the costs of applying for a BitLicense and various other concerns, including the perceived difficulty of the application process.[149]

3. Other States

Other states are taking or considering steps to develop a framework for regulating virtual currency businesses. On September 15, 2015, the Conference of State Bank Supervisors ("CSBS") issued a Model Regulatory Framework to promote consistent regulatory regimes for virtual currency activities among states.[150] The Model Regulatory Framework contains provisions relating to compliance with federal and state laws, including BSA/AML compliance. The Model Regulatory Framework provides that states should require virtual currency service providers to verify the identities of all service users, including all individuals that use a virtual currency service to transfer money via the blockchain. By contrast, the BitLicense rules promulgated by the DFS prior to the finalization of the Model Regulatory Framework require licensees to record "the identity and physical addresses of the party or parties to the transaction that are customers or accountholders of the Licensee and, to the extent practicable, any other parties to the transaction."

On June 19, 2015, Governor Daniel Malloy of Connecticut signed into law H.B. No. 6800,[151] which clarifies that money transmitter applicants must specify whether their services will include virtual currency. Other states, such as California, Pennsylvania and North Carolina, have also been active in considering legislation for the regulation of virtual currency businesses.[152] It is expected that AML compliance requirements will be included as part of these.

4. FATF

In June 2015, FATF published the Guidance for a Risk-Based Approach to Virtual Currencies ("VC Guidance"). The non-binding VC Guidance addresses virtual currency payment products and services ("VCPPS"), focusing primarily on the AML/CFT risks raised by entities that are "points of intersection" where "[virtual currency] activities intersect with the regulated fiat currency financial system." These points of intersection include convertible virtual currency exchangers ("convertible VC nodes"). The VC Guidance explains the application of the risk-based approach to AML/CFT measures in the virtual currency context, building on the Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services issued by FATF in 2013 and clarifying the application of FATF's international standards on combating money-laundering and the financing of terrorism and proliferation (the "FATF Recommendations"), published by FATF in 1990 and most recently revised in 2012, to convertible VC nodes.[153]

The VC Guidance discusses how certain of the FATF Recommendations apply to countries and competent authorities, with a focus on identifying and mitigating risks associated with convertible virtual

currencies, applying licensing and registration requirements, implementing effective supervision, providing effective and dissuasive sanctions and facilitating regulatory cooperation. The VC Guidance also explains how certain of the FATF Recommendations should apply to convertible VC nodes and examines current obstacles to their application in practice. Finally, the VC Guidance surveys the risk-based approaches taken and expected to be taken by governments around the world.

B. ENFORCEMENT ACTIONS

During 2015, virtual currency businesses became the target of regulatory enforcement actions by the Commodities Futures Trading Commission ("CFTC"), DOJ, FinCEN and SEC.

The regulatory enforcement actions by the CFTC related to Commodity Exchange Act ("CEA") violations, including the first statement by the CFTC that bitcoin and virtual currencies are commodities under the CEA.[154] With respect to AML specifically, in several speeches, FinCEN has highlighted its supervisory expectations for virtual currencies. On May 6, 2015, in her keynote address at the West Coast AML Forum, FinCEN director Shasky Calvery indicated that FinCEN had been working closely with IRS BSA examiners to launch "a series of supervisory examinations of businesses in the virtual currency industry" and that FinCEN will continue to "use [its] supervisory and enforcement authorities to appropriately penalize non-compliance and drive compliance improvements."[155] On November 16, 2015, at the ABA/ABA Money Laundering Enforcement Conference in Washington, D.C., Director Shasky Calvery repeated these comments, reinforcing the message that FinCEN's supervisory examinations of the virtual currency industry are an ongoing priority.[156]

The fruits of FinCEN's efforts are reflected in the first enforcement action FinCEN has taken against a virtual currency exchange, which was taken concurrently with the DOJ. On May 5, 2015, Ripple Labs Inc. ("Ripple") and its subsidiary XRP II LLC ("XRP II") entered into a consent to the assessment of a civil money penalty with FinCEN in the amount of $700,000,[157] to be partially satisfied by a $450,000 forfeiture imposed as part of a settlement agreement with the DOJ,[158] to settle potential civil and criminal liability in connection with violations of the BSA. According to the statement of facts and violations,[159] to which Ripple and XRP II admitted as part of the settlement, Ripple sold convertible virtual currency known as "XRP" without having registered with FinCEN as an MSB, despite FinCEN's March 18, 2013 guidance clarifying that virtual currency exchangers and administrators constitute "money transmitters" and must therefore register as MSBs with FinCEN. In addition, Ripple (and XRP II after it replaced Ripple as a seller of XRP in July 2013) failed to maintain an appropriate AML program or file required SARs. Under the settlement documents, Ripple and XRP II consented to a remedial framework,[160] agreeing to migrate the virtual currency wallet service Ripple Trade to an MSB registered with FinCEN, to implement an effective AML program and to ensure their compliance with the funds transfer rule, including 31 C.F.R. 1010.410 (the "Travel Rule"). In addition, Ripple and XRP II agreed to conduct a three-year look-back to

review transactions and attempted transactions for suspicious activity and committed to implement transaction-monitoring enhancements to the Ripple protocol.[161]

Subsequent to the enforcement action, Ripple suspended all account sign-ups on Ripple Trade until further notice,[162] and then announced that Ripple Trade would be discontinued in early 2016.[163] For additional information, please refer to the related post on our AML & Sanctions Watchlist.[164]

Finally, the SEC brought criminal charges against two virtual currency-mining companies and their founder, for the first time characterizing sales of "Hashlets" (shares in the returns from virtual currency mining operations) as investment contracts, and thus securities, subject to the anti-fraud provisions in the Securities Act and Securities Exchange Act of 1934.[165]

* * *

Copyright © Sullivan & Cromwell LLP 2016

ENDNOTES

1 *See, e.g.*, remarks of Adam Szubin, Acting Under Secretary for Terrorism and Financial Crimes, at the ABA/ABA Money Laundering Enforcement Conference (Nov. 16, 2015), *available at* https://www.treasury.gov/press-center/press-releases/Pages/jl0275.aspx; "FATF Takes Action to Tackle De-Risking" (Oct. 23, 2015), *available at* http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-action-to-tackle-de-risking.html.

2 *Id.*

3 *Id.*

4 "Report To The G20 On Actions Taken To Assess And Address The Decline In Correspondent Banking," Financial Stability Board (Nov. 6, 2015), *available at* http://www.financialstabilityboard.org/wp-content/uploads/Correspondent-banking-report-to-G20-Summit.pdf.

5 *Community Fin. Services Ass'n. of America et al.* v. *Fed. Deposit Insurance Corp.*, D.D.C. Case No. 14-CV-953 (Sept. 25, 2015), *available at* http://business.cch.com/BANKD/CFSA-v-FDIC-MemorandumOpinion-09252015.pdf.

6 Remarks of Martin J. Gruenberg, Chairman of the FDIC, before the U.S. House of Representatives Financial Services Committee Subcommittee on Oversight and Investigations, Washington, D.C. (Mar. 24, 2015), *available at* https://fdic.gov/news/news/speeches/spmarch2415.html.

7 "Federal Deposit Insurance Corporation 2014 Annual Report" (Mar. 4, 2015), *available at* https://www.fdic.gov/about/strategic/report/2014annualreport/2014AR_Final.pdf.

8 Evan Weinberger, "OCC Won't Issue Anti-Money Laundering Recommendations," Law360 (Jan. 26, 2015), *available at* http://www.law360.com/articles/615111/occ-won-t-issue-anti-money-laundering-recommendations.

9 Remarks of Under Secretary for Terrorism and Financial Intelligence David S. Cohen at the Treasury Roundtable on Financial Access for Money Services Businesses (Jan. 13, 2015), *available at* https://www.treasury.gov/press-center/press-releases/Pages/jl9736.aspx.

10 Remarks of Adam Szubin, Acting Under Secretary for Terrorism and Financial Crimes, at the ABA/ABA Money Laundering Enforcement Conference (Nov. 16, 2015), https://www.treasury.gov/press-center/press-releases/Pages/jl0275.aspx.

11 Remarks of Adam Szubin, Acting Under Secretary for Terrorism and Financial Crimes, at the ABA/ABA Money Laundering Enforcement Conference (Nov. 16, 2015), https://www.treasury.gov/press-center/press-releases/Pages/jl0275.aspx.

12 "Drivers for 'de-risking' go beyond anti-money laundering/terrorist financing" (June 26, 2015), *available at* http://www.fatf-gafi.org/publications/fatfrecommendations/documents/derisking-goes-beyond-amlcft.html.

13 "FATF Takes Action to Tackle De-Risking" (Oct. 23, 2015), *available at* http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-action-to-tackle-de-risking.html.

14 "Guidance for a Risk-Based Approach: Virtual Currencies" (June 2015), *available at* http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

15 "Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services" (June 2013), *available at* http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-npps-2013.html.

16 "Guidance For A Risk-Based Approach: Effective Supervision And Enforcement By AML/CFT Supervisors Of The Financial Sector And Law Enforcement" (Oct. 2015), *available at*

http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-effective-supervision-and-enforcement.html.

17 "Report To The G20 On Actions Taken To Assess And Address The Decline In Correspondent Banking," Financial Stability Board (Nov. 6, 2015), *available at* http://www.financialstabilityboard.org/wp-content/uploads/Correspondent-banking-report-to-G20-Summit.pdf.

18 Deferred Prosecution Agreement, *United States of America* v. *Commerzbank AG and Commerzbank AG New York Branch* Criminal No. [_____] (March 12, 2015), *available at* http://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/12/commerzbank_deferred_prosecution_agreement_1.pdf; Consent Order Under New York Banking Law §§ 39 and 44, *In the Matter of Commerzbank AG, Commerzbank AG New York Branch* (March 12, 2015), *available at* http://www.dfs.ny.gov/about/ea/ea150312.pdf.

19 Letter dated July 7, 2015 to Hon. Blaine Luetkemeyer, U.S. House of Representatives, from G. Bradley Weinsheimer, Deputy Counsel, U.S. Dep't of Justice Office of Professional Responsibility regarding "OPR Inquiry Regarding Operation Choke Point" (stating "[t]he last FIRREA subpoena issued under Operation Choke Point was issued in August 2013"), *available at* http://big.assets.huffingtonpost.com/ChokePointOPRReport.pdf.

20 *Community Fin. Services Ass'n. of America et al.* v. *Fed. Deposit Insurance Corp.*, D.D.C. Case No. 14-CV-953 (Sept. 25, 2015), *available at* http://business.cch.com/BANKD/CFSA-v-FDIC-MemorandumOpinion-09252015.pdf.

21 "FDIC, Fed Must Face Payday Lenders' 'Choke Point' Lawsuit" (Sep. 25, 2015), http://www.bloomberg.com/news/articles/2015-09-25/fdic-fed-must-face-payday-lenders-choke-point-lawsuit.

22 "Statement on Providing Banking Services," FIL-5-2015 (Jan. 28, 2015), https://www.fdic.gov/news/news/financial/2015/fil15005.pdf.

23 114 H.R. 766, *available at* https://www.congress.gov/114/bills/hr766/BILLS-114hr766rh.pdf.

24 *See* "House Passes Bill to Curb 'Operation Choke Point,'" The Hill (Feb 2, 2016), *available at* http://thehill.com/policy/finance/268223-house-passes-bill-to-curb-operation-choke-point.

25 "CommerceWest Bank Admits Bank Secrecy Act Violation and Reaches $4.9 Million Settlement with Justice Department" (Mar. 10, 2015), http://www.justice.gov/opa/pr/commercewest-bank-admits-bank-secrecy-act-violation-and-reaches-49-million-settlement-justice; Consent Decree, *United States of America* v. *Commercewest Bank*, C.D.C. Case No. CV-15-00379 (Mar. 10, 2015), *available at* http://www.justice.gov/file/347431/download; Deferred Prosecution Agreement; Attachments, *United States of America* v. *CommerceWest Bank*, C.D.C. Case No. SACR15-00025 (Mar. 10, 2015), *available at* http://www.justice.gov/file/348996/download.

26 "2014 Year-End Review of U.S. BSA/AML and Sanctions Developments and Their Importance to Financial Institutions" (Jan. 29, 2015), *available at* https://www.sullcrom.com/siteFiles/Publications/SC_Publication_2014_Year_End_Review_of_US_BSA_AML_and_Sanctions_Developments.pdf.

27 *See* "Superintendent Lawsky's Remarks on Financial Regulation in New York City at Columbia Law School" (Feb. 25, 2015), *available at* http://www.dfs.ny.gov/about/speeches/sp150225.htm.

28 FINRA, 2015 Regulatory and Examination Priorities Letter (Jan. 6, 2015), *available at* http://www.finra.org/industry/2015-exam-priorities-letter. The 2016 Regulatory and Examinations Priorities Letter states that FINRA will focus on "whether supervisors are effective role models of firm culture" as an indicator of how firm culture affects compliance- and risk-management

practices. FINRA, 2016 Regulatory and Examinations Priorities Letter (Jan. 5, 2016), *available at* http://www.finra.org/sites/default/files/2016-regulatory-and-examination-priorities-letter.pdf.

29 *See* "Understanding Disqualifications, Exemptions and Waivers Under the Federal Securities Laws" (Mar. 12, 2015) *available at* http://www.sec.gov/news/speech/031215-spch-cmjw.html.

30 Remarks by Vice Chairman Stanley Fischer at the International Monetary Conference, Toronto, Canada (Jun 1, 2015), *available at* http://www.federalreserve.gov/newsevents/speech/fischer20150601a.htm.

31 "Reforming Culture and Behavior in the Financial Services Industry: Workshop on Progress and Challenges" (Nov. 19, 2015), *available at* https://www.newyorkfed.org/medialibrary/media/newsevents/events/banking/2015/culture_workshop_summary_2015.pdf.

32 Remarks by Sally Quillian Yates, Deputy Attorney General, at New York University School of Law Announcing New Policy on Individual Liability in Matters of Corporate Wrongdoing (Sept. 10, 2015), *available at* http://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-new-york-university-school.

33 *See* "Individual Accountability for Corporate Wrongdoing" (Sept. 9, 2015), *available at* http://www.justice.gov/dag/file/769036/download.

34 *Id.*; Remarks by Sally Quillian, Deputy Attorney General, at American Banking Association and American Bar Association Money Laundering Enforcement Conference (Nov. 16, 2015), *available at* http://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-american-banking-0.

35 "New Justice Department Guidance on Individual Accountability: Analysis of the Justice Department's New Guidance on Individual Liability in Matters of Corporate Wrongdoing" (Sept. 14, 2015), *available at* https://www.sullcrom.com/new-justice-department-guidance-on-individual-accountability; and "Justice Department Releases New Prosecution Policies: United States Attorneys' Manual Revised to Incorporate Recently Announced Policies on Individual Liability and Cooperation in Corporate Prosecutions" (Nov. 18, 2015), *available at* https://www.sullcrom.com/new-justice-department-policies-on-corporate-prosecutions.

36 A recent article noted that "[a] round three dozen senior bank-compliance executives left their jobs in 2015, three times the number of a year earlier," and that "most of those were in positions overseeing anti-money-laundering or financial crime." *The Wall Street Journal*, "Now in the Cross Hairs: Compliance Officers" (Feb. 5, 2016).

37 For a past example of such an action, see Cease and Desist Order Issued Upon Consent, *In the Matter of BNP Paribas S.A.* (June 30, 2014), *available at* http://www.federalreserve.gov/newsevents/press/enforcement/enf20140630a1.pdf. Federal agencies also executed enforcement actions targeted directly against individuals. For example, on September 14, 2015, the OCC levied a civil money penalty against the Chief Executive Officer of a bank, in part for failure to take appropriate action regarding that bank's failure to file CTRs. Stipulation and Consent Order, *In the Matter of Douglas Ulrich* (September 14, 2015), available at http://www.occ.gov/static/enforcement-actions/ea2015-104.pdf. During the course of 2015, FINRA also levied fines against individuals in several enforcement actions, such as in actions against Aegis Capital Corp. and Mercator Associates, LLC. Order Accepting Offer of Settlement, *Department of Enforcement* v. *Aegis Capital Corp. et al.* (Aug. 3, 2015), *available at* https://www.finra.org/sites/default/files/Aegis_Capital_Corp_Smulevitz_McKenna.pdf; Order Accepting Offer of Settlement, *Department of Enforcement v. Mercator Associates, LLC and Fabrizio David Lentini* (Oct. 16, 2015), *available at* http://disciplinaryactions.finra.org/Search/ViewDocument/63617.

ENDNOTES (CONTINUED)

[38] *See* Federal Reserve Press Release (Mar. 12, 2015), *available at* http://www.federalreserve.gov/newsevents/press/enforcement/20150312b.htm.

[39] *See* Federal Reserve Press Release (May 11, 2015), *available at* http://www.federalreserve.gov/newsevents/press/enforcement/20150511a.htm.

[40] Similarly, in its May 20, 2015 actions against UBS AG, Barclays Bank PLC, Citigroup Inc., JPMorgan Chase & Co., Royal Bank of Scotland PLC, and Bank of America Corporation for unsafe and unsound practices in the foreign exchange markets, the Federal Reserve precluded the institutions from reemploying the individuals involved in the past actions or retaining them as consultants or contractors, and required the institutions to provide "substantial assistance" to the Federal Reserve in connection with its investigation of whether enforcement actions should be taken against individuals.

[41] On November 10, 2015, the Federal Reserve announced its decision denying one of the individuals' request to withdraw the Federal Reserve's action barring him from employment in the banking industry. *See* Federal Reserve Press Release (Nov. 10, 2015), *available at* http://www.federalreserve.gov/newsevents/press/enforcement/20151110a.htm.

[42] *See* Federal Reserve Press Release (Oct. 20, 2015), *available at* http://www.federalreserve.gov/newsevents/press/enforcement/20151020a.htm.

[43] *See* "Fokker Services B.V. Agrees To Forfeit $10.5 Million For Illegal Transactions With Iranian, Sudanese, And Burmese Entities—Company Will Pay Additional $10.5 Million In Parallel Civil Settlement" (June 5, 2014), *available at* http://www.justice.gov/usao-dc/pr/fokker-services-bv-agrees-forfeit-105-million-illegal-transactions-iranian-sudanese-and.

[44] The case is *U.S.* v. *Fokker Services BV*, 15-3016 and 15-3017, U.S. Court of Appeals for the District of Columbia Circuit.

[45] *See United States* v. *HSBC Bank USA, N.A. & HSBC Holdings PLC*, Memorandum and Order 12-CR-763 (E.D.N.Y. 2013), *available at* https://www.justice.gov/sites/default/files/usao-edny/legacy/2015/04/06/HSBC%20Memorandum%20and%20Order%207.1.13.pdf.

[46] "HSBC Case Tests Transparency of Deferred Prosecution Agreements" (Feb. 8, 2016), *available at* http://www.nytimes.com/2016/02/09/business/dealbook/hsbc-case-tests-transparency-of-deferred-prosecution-agreements.html?_r=0.

[47] *See, e.g.*, *United States* v. *Saena Tech Corp.*, No. CR 14-211, 2015 WL 6406266 (D.D.C. Oct. 21, 2015), in which Judge Emmet Sullivan, while approving a DPA, expressed skepticism regarding the government's use of DPAs in a domestic bribery case.

[48] *See, e.g.*, Discussion Draft of the Bad Actor Disqualification Act, U.S. House Committee on Financial Services, *available at* http://democrats.financialservices.house.gov/uploadedfiles/03.24.15_sec_discussion_draft_bill.pdf.

[49] *See* "SEC Charges Oppenheimer With Securities Law Violations Related to Improper Penny Stock Sales" (Jan. 27, 2015), *available at* http://www.sec.gov/news/pressrelease/2015-14.html; *see* "FinCEN Fines Oppenheimer & Co. Inc. $20 Million for Continued Anti-Money Laundering Shortfalls," (Jan. 27, 2015), *available at* https://www.fincen.gov/news_room/nr/html/20150127.html.

[50] *In the Matter of Oppenheimer & Co., Inc.*, Securities Act Release No. 9712 (Jan. 27, 2015), *available at* http://www.sec.gov/rules/other/2015/33-9712.pdf.

[51] SEC, Dissenting Statement in the Matter of Oppenheimer & Co., Inc. (Feb. 4, 2015), *available at* http://www.sec.gov/news/statement/dissenting-statement-oppenheimer-inc.html.

[52] *See* Notice of Exemption, *available at* https://www.federalregister.gov/articles/2015/10/02/2015-24919/notice-of-exemption-involving-credit-suisse-ag-hereinafter-either-credit-suisse-ag-or-the-applicant.

[53] Consent Order, *In the Matter of U.S. Bank National Association* (Oct. 23, 2015), *available at* http://www.occ.gov/static/enforcement-actions/ea2015-113.pdf; Consent Order, *In the Matter of Wells Fargo Bank, National Association* (Nov. 19, 2015), *available at* http://www.occ.gov/static/enforcement-actions/ea2015-125.pdf.

[54] Remarks of Andrew Ceresney, SEC Enforcement Director, at SIFMA's 2015 Anti-Money Laundering & Financial Crimes Conference (Feb. 25, 2015), *available at* http://www.sec.gov/news/speech/022515-spchc.html.

[55] "Anti-Money Laundering: An Often-Overlooked Cornerstone of Effective Compliance," Remarks of Kevin W. Goodman, National Associate Director, Broker-Dealer Examination Program, Office of Compliance Inspections and Examinations (Jun. 18, 2015), *available at* http://www.sec.gov/news/speech/anti-money-laundering-an-often-overlooked-cornerstone.html.

[56] *See* Order Instituting Administrative and Cease and Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933 and Section 15(b) and 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing Remedial Sanctions and a Cease and Desist Order, *In the Matter of Oppenheimer & Co., Inc.* (Jan. 27, 2015), *available at* http://www.sec.gov/litigation/admin/2015/33-9711.pdf; Assessment of Civil Money Penalty, *In the Matter of Oppenheimer & Co., Inc.* (Jan. 26, 2015), *available at* https://www.fincen.gov/news_room/ea/files/Oppenheimer_Assessment_20150126.pdf. In these enforcement actions, FinCEN found that Oppenheimer willfully violated the BSA by failing to (a) implement an adequate AML program, (b) conduct adequate due diligence on a foreign correspondent account, and (c) comply with requirements under the rules imposing Special Measures under Section 311 of the USA PATRIOT Act, while the SEC found that Oppenheimer willfully violated federal securities laws, including the requirement under Section 17(a) of the Securities Exchange Act of 1934 and Rule 17a-8 thereunder that Oppenheimer file SARs with FinCEN. These actions by the SEC and FinCEN are the latest in a series of actions against the company for AML program shortcomings. In December 2005, the New York Stock Exchange and FinCEN assessed Oppenheimer $2.8 million in civil money penalties and in August 2013 FINRA fined the company $1.4 million for BSA violations similar to those detailed by FinCEN and the SEC.

[57] "Recent Developments in BSA/AML" (Feb. 2, 2015), *available at* http://www.sullcrom.com/siteFiles/Publications/SC_Publication_Recent_Developments_in_BSA_AML_02_02_15.pdf.

[58] Financial Industry Regulatory Authority Letter of Acceptance, Waiver and Consent No. 2012034964301 re: Cantor Fitzgerald & Co., CRD No. 134 (Dec. 21, 2015), *available at* http://disciplinaryactions.finra.org/Search/ViewDocument/63881.

[59] "FINRA Fines Cantor Fitzgerald & Co. $6 Million for Selling Unregistered Microcap Shares, Related AML and Supervisory Violations" (Dec. 22, 2015), *available at* https://www.sullcrom.com/blogs-finra-fines-cantor-fitzgerald-and-co-s6-million-for-selling-unregistered-microcap-shares-related-aml-and-supervisory-violations.

[60] Assessment of Civil Money Penalty, *In the Matter of Trump Taj Mahal Associates, LLC, d/b/a Trump Taj Mahal Casino Resort Atlantic City, New Jersey* (March 6, 2015), *available at* https://www.fincen.gov/news_room/ea/files/20150302%20Assessment%20of%20Civil%20Money%20Penalty%20Trump%20Taj%20Mahal%20(post-approval%20by%20bankruptcy%20court).pdf. Assessment of Civil Money Penalty, *In the Matter of Hong Kong Entertainment (Overseas) Investments, Ltd. d/b/a Tinian Dynasty Hotel & Casino* (June 3, 2015), *available at* https://www.fincen.gov/news_room/ea/files/Tinian_Dynasty_Assessment.pdf; Assessment of Civil

ENDNOTES (CONTINUED)

Money Penalty, *In the Matter of Desert Palace, Inc. d/b/a Caesars Palace Las Vegas, Nevada* (November 6, 2015), *available at* https://www.fincen.gov/news_room/nr/files/Caesars_Palace_ASSESSMENT.pdf.

61 Remarks by Jennifer Shasky Calvery, Director of FinCEN at the ABA/ABA Money Laundering Enforcement Conference (Nov. 16, 2015), *available at* https://www.fincen.gov/news_room/speech/html/20151116.html.

62 Remarks of Stephanie Brooker, Associate Director of Enforcement of FinCEN at the 2015 Banking Secrecy Act Conference (Jun. 18, 2015), *available at* https://www.fincen.gov/news_room/speech/html/20150618.html.

63 Legal Sports Report, "Next Up For Daily Fantasy Sports: Clarification of Anti-Money Laundering Compliance" (Oct. 30, 2015), *available at* http://www.legalsportsreport.com/5717/dfs-anti-money-laundering-compliance/.

64 Notice to Cease and Desist and Notice of Proposed Litigation Pursuant to New York Executive Law § 63(12) and General Business Law § 349, *In the Matter of FanDuel, Inc.* (Nov. 10, 2015), *available at* http://ag.ny.gov/pdfs/Final_NYAG_FanDuel_Letter_11_10_2015_signed.pdf; Notice to Cease and Desist and Notice of Proposed Litigation Pursuant to New York Executive Law § 63(12) and General Business Law § 349, *In the Matter of DraftKings, Inc.* (Nov. 10, 2015), *available at* http://ag.ny.gov/pdfs/Final_NYAG_DraftKings_Letter_11_10_2015.pdf.

65 *New York* v. *DraftKings, Inc.* (N.Y. Sup. Ct. Dec. 11, 2015), *available at* https://www.nycourts.gov/press/Draftkings%20Inc%20and%20Fanduel%20Inc.pdf.

66 "Fantasy Sports Payment Firm May Opt Out" (Jan. 29, 2016), *available at* https://www.bostonglobe.com/business/2016/01/29/payment-processor-will-drop-daily-fantasy-sites-report-says/wUO6De3fD39YUL7RCnAeEL/story.html.

67 "Fantasy Sites Are Dealt New Rebuff by Citigroup" (Feb. 5, 2016), *available at* http://www.nytimes.com/2016/02/06/sports/fantasy-sports-draftkings-fanduel.html?_r=1.

68 Consent Order Under New York Banking Law §§ 39 and 44, *In the Matter of Crédit Agricole S.A., Crédit Agricole Corporate & Investment Bank New York Branch* (Oct. 15, 2015), *available at* http://www.dfs.ny.gov/about/ea/ea151019.pdf.

69 Consent Order Under New York Banking Law §§ 39 and 44, *In the Matter of Deutsche Bank AG, Deutsche Bank AG New York Branch* (Nov. 3, 2015), *available at* http://www.dfs.ny.gov/about/ea/ea151103.pdf.

70 Deferred Prosecution Agreement, *United States of America* v. *Commerzbank AG and Commerzbank AG New York Branch* (Mar. 12, 2015), *available at* https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/12/commerzbank_deferred_prosecution_agreement_1.pdf.

71 *See, e.g.*, Deferred Prosecution Agreement, *United States of America* v. *Commerzbank AG and Commerzbank AG New York Branch* Criminal No. [_____] (March 12, 2015), *available at* https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/12/commerzbank_deferred_prosecution_agreement_1.pdf; Consent Order Under New York Banking Law §§ 39 and 44, *In the Matter of Commerzbank AG, Commerzbank AG New York Branch* (March 12, 2015), *available at* http://www.dfs.ny.gov/about/ea/ea150312.pdf; Plea Agreement between Schlumberger Oilfield Holdings Ltd., the Office of the United States Attorney for the District of Columbia, and the National Security Division of the United States Department of Justice (Mar. 25, 2015), *available at* https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/25/schlumberger_plea_agreement.pdf; "UBS AG Settles Potential

ENDNOTES (CONTINUED)

Liability for Apparent Violations of the Global Terrorism Sanctions Regulations" (Aug. 27, 2015), *available at* https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20150827_ubs.pdf; Consent Order Under New York Banking Law §§ 39 and 44, *In the Matter of Crédit Agricole S.A. and Crédit Agricole Corporate and Investment Bank* (Oct. 20, 2015), *available at* http://www.dfs.ny.gov/about/ea/ea151019.pdf; "Crédit Agricole Corporate and Investment Bank Admits to Sanctions Violations, Agrees to Forfeit $312 Million" (Oct. 20, 2015), *available at* http://www.justice.gov/usao-dc/pr/cr-dit-agricole-corporate-and-investment-bank-admits-sanctions-violations-agrees-forfeit; Consent Order Under New York Banking Law §§ 39 and 44, *In the Matter of Deutsche Bank AG, Deutsche Bank AG New York Branch* (November 3, 2015), *available at* http://www.dfs.ny.gov/about/ea/ea151103.pdf.

72 "Schlumberger Oilfield Holdings Ltd. Agrees to Plead Guilty and Pay Over $232.7 Million for Violating US Sanctions by Facilitating Trade with Iran and Sudan" (Mar. 25, 2015), *available at* http://www.justice.gov/opa/pr/schlumberger-oilfield-holdings-ltd-agrees-plead-guilty-and-pay-over-2327-million-violating-us.

73 Plea Agreement between Schlumberger Oilfield Holdings Ltd., the Office of the United States Attorney for the District of Columbia, and the National Security Division of the United States Department of Justice (Mar. 25, 2015), *available at* https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/25/schlumberger_plea_agreement.pdf.

74 AML & Sanctions Watchlist, *available at* https://www.sullcrom.com/blogs/ofac; "Recent Developments in Sanctions Enforcement" (Apr. 8, 2015), *available at* https://www.sullcrom.com/siteFiles/Publications/SC_Publication_Recent_Developments_in_Sanctions_Enforcement.pdf.

75 "UBS AG Settles Potential Liability for Apparent Violations of the Global Terrorism Sanctions Regulations" (Aug. 27, 2015), *available at* https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20150827_ubs.pdf.

76 *See*, *e.g.*, Australia and New Zealand Banking Group, Ltd. Settlement Agreement (Aug. 21, 2009), *available at* https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/anz_08242009.pdf; Credit Suisse AG Settlement Agreement (Dec. 16, 2009), *available at* https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/12162009.pdf.

77 "PayPal, Inc. Settles Potential Civil Liability for Apparent Violations of Multiple Sanctions Programs" (Mar. 25, 2015), *available at* https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20150325_paypal.pdf.

78 "Recent Developments in Sanctions Enforcement" (Apr. 8, 2015), *available at* https://www.sullcrom.com/siteFiles/Publications/SC_Publication_Recent_Developments_in_Sanctions_Enforcement.pdf.

79 OFAC Enforcement Action, BMO Harris Bank NA Receives a Finding of Violation Regarding Violations of the Iranian Transactions and Sanctions Regulations (Oct. 21, 2015), *available at* http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20151021_bmo_harris.pdf.

80 "Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers," 80 Fed. Reg. 52680 (Sept. 1, 2015), *available at* https://www.federalregister.gov/articles/2015/09/01/2015-21318/anti-money-laundering-program-and-suspicious-activity-report-filing-requirements-for-registered.

81 *See* "Withdrawal of the Notice of Proposed Rulemaking; Anti-Money Laundering Programs for Unregistered Investment Companies," 73 Fed. Reg. 65569 (Nov. 4, 2008); and "Withdrawal of the Notice of Proposed Rulemaking; Anti-Money Laundering Programs for Investment Advisers," 73 Fed. Reg. 65568 (Nov. 4, 2008).

ENDNOTES (CONTINUED)

82 FinCEN has also currently deferred a discussion as to whether commodity pools are covered by the Proposed AML Rule.

83 *See, e.g.*, "Investment Company Institute Comment Letter" (Nov. 2, 2015) at 7, *available* at https://www.ici.org/pdf/29461.pdf (paste in browser).

84 *See, e.g.*, "Financial Services Roundtable Comment Letter" (Nov. 2, 2015) at 4, *available at* http://fsroundtable.org/fsr-comment-on-application-of-anti-money-laundering-aml-rules-to-investment-advisers/.

85 *See* New York Department of Financial Services Superintendent's Regulations, Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications (Proposed Rule), I.D.-No.-DFS-50-15-00004-P, Part 504 of Title 3 NYCRR (Dec. 16, 2015).

86 *See* Bank Secrecy Act/Anti-Money Laundering Examination Manual, Federal Financial Institutions Examination Council, 60-80, 125-32, 142-54, 290-95 and App. R (2014), *available at* https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm.

87 *See* Consent Order, *In the Matter of U.S. Bank National Association* (Oct. 23, 2015), *available at* http://www.occ.gov/static/enforcement-actions/ea2015-113.pdf; Consent Order, *In the Matter of JPMorgan Chase Bank, N.A., JPMorgan Bank and Trust Company, N.A. and Chase Bank USA, N.A.* (Jan. 14, 2013), *available at* http://www.occ.gov/static/enforcement-actions/ea2013-002.pdf; Consent Order, *In the Matter of Citibank, N.A.* (Apr. 5, 2012), *available at* http://www.occ.gov/static/enforcement-actions/ea2012-052.pdf; Assessment of Civil Money Penalty, *In the Matter of Wachovia Bank, National Association* (Mar. 12, 2010), *available at* https://www.fincen.gov/news_room/ea/files/100316095447.pdf.

88 "New York DFS Proposed BSA/AML and Sanctions Requirements: New York Department of Financial Services Issues Proposed Transaction Monitoring and Filtering Program Requirements and Annual Senior Compliance Officer Certification" (Dec. 2, 2015), *available at* https://www.sullcrom.com/new-york-dfs-proposed-bsaaml-and-sanctions-requirements.

89 On August 11, 2014, FinCEN issued a GTO that requires enhanced cash reporting by armored car services and other common carriers of currency at the San Ysidro and Otay Mesa Ports of Entry in California. FinCEN renewed the GTO for an additional six-month period, beginning on February 8, 2015, which ended on August 7, 2015. FinCEN has since renewed the GTO again for common carriers in Southern California on August 8, 2015 for another six-month period, which will end on February 4, 2016, but this time broadened the GTO, making it also applicable to common carriers crossing the border at eight major ports of entry in Texas, which commenced on September 17, 2015 and will end on March 15, 2016. *See* FinCEN Press Release, "FinCEN and Mexican Counterpart Shine Spotlight on Cross-Border Cash Couriers: Geographic Targeting Order and Guidance Issued to Guard Against Misuse of Armored Cars" (Aug. 1, 2014), *available at* https://www.fincen.gov/news_room/nr/html/20140801.html; *see also* FinCEN Press Release, "FinCEN Renews Geographic Targeting Order (GTO) Requiring Enhanced Cash Reporting at the San Ysidro and Otay Mesa Ports of Entry in California" (Feb. 6, 2015), *available at* https://www.fincen.gov/news_room/nr/html/20150206.html; FinCEN Press Release, "FinCEN Renews and Broadens Geographic Targeting Orders on Border Cash Shipments in California and Texas" (Aug. 7, 2015), *available at* https://www.fincen.gov/news_room/nr/html/20150807.html.

90 *See* 31 U.S.C. § 5326(a); 31 C.F.R. § 1010.370 and U.S. Treasury Department Order 180-01.

91 *See supra* 4; *see also "*FinCEN and Mexican Counterpart Shine Spotlight on Cross-Border Cash Couriers" (Aug. 1, 2014), *available at* https://www.fincen.gov/news_room/nr/html/20140801.html; "FinCEN Issues Geographic Targeting Order Covering the Los Angeles Fashion District as Part of Crackdown on Money Laundering for Drug Cartels" (Oct. 2, 2014), *available at*

http://www.fincen.gov/news_room/nr/html/20141002.html; "FinCEN Targets Money Laundering Infrastructure with Geographic Targeting Order in Miami" (Apr. 21, 2015), *available at* (https://www.fincen.gov/news_room/nr/html/20150421.html; "FinCEN Combats Stolen Identity Tax Refund Fraud in South Florida with Geographic Targeting Order" (Jul. 13, 2015), *available at* https://www.fincen.gov/news_room/nr/html/20150713.html; and "FinCEN Takes Aim at Real Estate Secrecy in Manhattan and Miami" (Jan. 13, 2016), *available at* https://www.fincen.gov/news_room/nr/html/20160113.html.

92 "FinCEN Targets Money Laundering Infrastructure with Geographic Targeting Order in Miami" (Apr. 21, 2015), *available at* http://www.fincen.gov/news_room/nr/pdf/20150421.pdf.

93 "FinCEN Advisory to Financial institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering" (Feb. 18, 2010), *available at* https://www.fincen.gov/statutes_regs/guidance/pdf/fin-2010-a001.pdf. The May 2014 advisory identified several red flags to assist U.S. financial institutions in identifying and reporting suspicious funnel account and TBML activity. Financial institutions should continue to appropriately monitor for any red flags identified by FinCEN that may signify suspicious funnel account and TBML activity, and report such activity, as appropriate, on a SAR with FinCEN. The GTO's terms (other than with respect to recordkeeping) were effective for a six-month period, which commenced on April 28, 2015, and ended on October 25, 2015. The GTO was renewed by FinCEN on October 26, for an additional six-month period, which is set to end on April 23, 2016. FinCEN Press Release, "FinCEN Renews Geographic Targeting Order (GTO) Requiring Enhanced Reporting and Recordkeeping for Electronics Exporters Near Miami, Florida" (Oct. 25, 2015), *available at* https://www.fincen.gov/news_room/nr/html/20151023.html.

94 "Recent Developments in BSA/AML" (Apr. 22, 2015), *available at* https://www.sullcrom.com/siteFiles/Publications/SC_Publication_Recent_Developments_in_BSA_AML_4_22_15.pdf.

95 For purposes of the GTO, a "check casher" is defined by FinCEN's existing regulations. *See* 31 CFR 1010.100(ff)(2); "FinCEN Combats Stolen Identity Tax Refund Fraud in South Florida with Geographic Targeting Order" (Jul. 13, 2015), *available at* https://www.fincen.gov/news_room/nr/html/20150713.html. The term generally includes a person that accepts checks or monetary instruments in return for currency or other monetary instruments (or a combination of the two), in an amount greater than $1,000 for any person on any day in one or more transactions.

96 Check cashers subject to the GTO were required to comply with its requirements from August 3, 2015 through January 30, 2016 and retain the additional information for five years from the last date on which the GTO is in effect.

97 "FinCEN Combats Stolen Identity Tax Refund Fraud through Geographic Targeting Order for South Florida" (Jul. 14, 2015), *available at* https://www.sullcrom.com/blogs-fincen-combats-stolen-identity-tax-refund-fraud-through-geographic-targeting-order-for-south-florida.

98 FinCEN Notice of Finding That Banca Privada Is a Financial Institution of Primary Money Laundering Concern 80 Fed. Reg. 13464 (Mar. 10, 2015); *see* FinCEN Press Release, "FinCEN Names Banca Privada d'Andorrà a Foreign Financial Institution of Primary Money Laundering Concern" (Mar. 10, 2015), *available at* http://www.fincen.gov/news_room/nr/html/20150310.html.

99 *FBME Bank Ltd.* v. *Lew*, No. 1:15-cv-01270, 2015 WL 5081209 (D.D.C. Aug. 27, 2015).

100 *FBME Bank Ltd.* v. *Lew*, 2015 WL 5081209 (Aug. 27, 2015).

101 *See* Withdrawal of the Proposed Rulemaking Against Lebanese Canadian Bank SAL, 80 Fed. Reg. 60575 (Oct. 7, 2015), *available at* https://www.federalregister.gov/articles/2015/10/07/2015-24912/financial-crimes-enforcement-network-withdrawal-of-the-proposed-rulemaking-against-lebanese-canadian.

ENDNOTES (CONTINUED)

102 The JCPOA is the agreement entered into between China, France, Germany, Russia, the United Kingdom, the United States, the European Union and Iran to ensure that Iran's nuclear program will be exclusively peaceful. U.S. Department of State, "Joint Comprehensive Plan of Action," *available at* http://www.state.gov/e/eb/tfs/spi/iran/jcpoa/.

103 "U.S. Economic Sanctions—Recent Developments: President Prohibits Trade With and New Investment in the Crimea Region of Ukraine and Announces Changes to the Cuba Embargo; Congress Passes New Laws Authorizing New Ukraine-Related Sanctions and Targeted Sanctions Against Venezuelan Government Officials" (Dec. 24, 2014), *available at* https://www.sullcrom.com/us-economic-sanctions-recent-developments; "OFAC Issues Venezuela Sanctions Regulations" (Jul. 13, 2015), *available at* https://www.sullcrom.com/blogs-ofac-issues-venezuela-sanctions-regulations.

104 More information about the relief from Iran sanctions afforded prior to the implementation of the JCPOA can be found in our previous memorandum to clients. "2014 Year-End Review of U.S. BSA/AML and Sanctions Developments and Their Importance to Financial Institutions" (Jan. 29, 2015), *available at* https://sullcrom.com/siteFiles/Publications/SC_Publication_2014_Year_End_Review_of_US_BSA_AML_and_Sanctions_Developments.pdf.

105 U.S. Department of the Treasury & U.S. Department of State, "Guidance Relating To The Lifting Of Certain U.S. Sanctions Pursuant To The Joint Comprehensive Plan Of Action On Implementation Day" (Jan. 16, 2016), *available at* https://www.treasury.gov/resource-center/sanctions/Programs/Documents/implement_guide_jcpoa.pdf; "Frequently Asked Questions Relating to the Lifting of Certain Sanctions Under the Joint Comprehensive Plan of Action (JCPOA) on Implementation Day," *available at* https://www.treasury.gov/resource-center/sanctions/Programs/Documents/jcpoa_faqs.pdf.

106 "Information Note on E.U. Sanctions to be Lifted Under the Joint Comprehensive Plan of Action (JCPOA)" (Jan. 16, 2016), *available at* http://eeas.europa.eu/top_stories/pdf/iran_implementation/information_note_eu_sanctions_jcpoa_en.pdf.

107 31 C.F.R. 515.587.

108 31 C.F.R. § 515.560. The categories of travel for which a general authorization, subject to conditions and limitations, is now available include: (i) family visits; (ii) official business of the U.S. government, foreign governments, and certain intergovernmental organizations; (iii) journalistic activity; (iv) professional research and professional meetings; (v) educational activities; (vi) religious activities; (vii) public performances, clinics, workshops, athletic and other competitions, and exhibitions; (viii) support for the Cuban people; (ix) humanitarian projects; (x) activities of private foundations or research or educational institutes; (xi) travel related to the exportation, importation or transmission of information or informational materials; and (xii) travel related to certain authorized exportations with respect to U.S.-owned or -controlled foreign firms.

109 31 C.F.R. § 515.584(a). *See also* Frequently Asked Questions Related to Cuba 32-33.

110 Frequently Asked Questions Related to Cuba 54.

111 31 C.F.R. § 515.584(d)(1). *See also* Frequently Asked Questions Related to Cuba 36.

112 *See* 31 C.F.R. § 515.584(d)(2). *See also* Frequently Asked Questions Related to Cuba 36.

113 "Cuba: Providing Support for the Cuban People" (Jan. 16, 2015), *available at* https://www.federalregister.gov/articles/2015/01/16/2015-00590/cuba-providing-support-for-the-cuban-people.

ENDNOTES (CONTINUED)

114 "Rescission of Cuba as a State Sponsor of Terrorism" (May 29, 2015), *available at* http://www.state.gov/r/pa/prs/ps/2015/05/242986.htm.

115 "Publication of Updated Cuban Assets Control Regulations (CACR)" (Sept. 18, 2015), *available at* https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20150918.aspx; "Commerce and Treasury Announce Further Amendments to the Cuba Sanctions Regulations" (Sept. 18, 2015), *available at* https://www.commerce.gov/news/press-releases/2016/01/commerce-and-treasury-announce-further-amendments-cuba-sanctions.

116 31 C.F.R. 515.587.

117 *See* Frequently Asked Questions Related to Cuba 3, 56.

118 "Crimea-Region Sanctions" (May 28, 2015), *available at* https://www.sullcrom.com/blogs-crimea-region-sanctions; "Amendment of FAQs Regarding Trade Finance Involving SSIs Under Ukraine-Related Sanctions" (May 28, 2015), *available at* https://www.sullcrom.com/blogs-amendment-of-faqs-regarding-trade-finance-involving-ssis-under-ukraine-related-sanctions.

119 "2014 Year-End Review of U.S. BSA/AML and Sanctions Developments and Their Importance to Financial Institutions" (Jan. 29, 2015), a*vailable at* https://sullcrom.com/siteFiles/Publications/SC_Publication_2014_Year_End_Review_of_US_BSA_AML_and_Sanctions_Developments.pdf.

120 "General License No. 6 – Noncommercial, Personal Remittances Authorized" (Jan. 30, 2015), *available at* https://www.treasury.gov/resource-center/sanctions/Programs/Documents/eo13685_gl_6.pdf.

121 FAQ 453, *available at* https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx.

122 "General License No. 7 – Operation of Accounts Authorized" (Jan. 30, 2015), *available at* https://www.treasury.gov/resource-center/sanctions/Programs/Documents/eo13685_gl_7.pdf.

123 "General License No. 8 – Transactions Related to Telecommunications and Mail Authorized" (Jan. 30, 2015), *available at* https://www.treasury.gov/resource-center/sanctions/Programs/Documents/eo13685_gl_8.pdf.

124 "General License No. 9 – Exportation of Certain Services and Software Incident to Internet-Based Communications Authorized" (May 22, 2015), *available at* https://www.treasury.gov/resource-center/sanctions/Programs/Documents/ukraine_gl_9.pdf.

125 "Crimea Sanctions Advisory" (July 30, 2015), *available at* https://www.treasury.gov/resource-center/sanctions/Programs/Documents/crimea_advisory.pdf.

126 Directive 1 imposed sanctions on two entities from the financial sector, Directive 2 imposed sanctions on entities from the energy sector and Directive 3 imposed sanctions on entities from the defense and related materiel sector. The directives are available for download at https://www.treasury.gov/resource-center/sanctions/Programs/Pages/ukraine.aspx.

127 FAQ 395. The FAQ previously stated that "U.S. persons may advise or confirm a letter of credit issued on behalf of a non-sanctioned entity in which an entity subject to Directive 1, 2 or 3 is the beneficiary (*i.e.*, the exporter or seller of the underlying goods) because the subject letter of credit does not represent an extension of credit to the SSI entity."

128 FAQ 419.

129 Executive Order 13687 (Jan. 2, 2015), available at https://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea.

ENDNOTES (CONTINUED)

130 Press Release, Treasury Imposes Sanctions Against the Government of The Democratic People's Republic of Korea (Jan. 2, 2015), available at https://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx.

131 "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (Apr. 1, 2015), *available at* https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf.

132 "OFAC FAQs," *available at* https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx.

133 "Statement of Secretary Lew on the Executive Order Targeting Significant Malicious Cyber-Enabled Activities" (Apr. 1, 2015), *available at* https://www.treasury.gov/press-center/press-releases/Pages/jl10015.aspx.

134 "Cyber-Related Sanctions Regulations" (Dec. 30, 2015), *available at* https://www.treasury.gov/resource-center/sanctions/Programs/Documents/fr80_81752.pdf.

135 "Publication of Cyber-Related Sanctions Regulations" (Dec. 31, 2015), *available at* https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20151231.aspx.

136 "Cybersecurity Assessment Tool," *available at* https://www.ffiec.gov/cyberassessmenttool.htm.

137 Remarks by Thomas J. Curry, Comptroller of the Currency, Before the Institute of International Bankers (Mar. 2, 2015), *available at* http://www.occ.gov/news-issuances/speeches/2015/pub-speech-2015-32.pdf.

138 "Semiannual Risk Perspective" (Spring 2015), *available at* http://www.occ.gov/publications/publications-by-type/other-publications-reports/semiannual-risk-perspective/semiannual-risk-perspective-spring-2015.pdf.

139 "SAR Stats Technical Bulletin" (Oct. 2015), *available at* https://www.fincen.gov/news_room/rp/files/SAR02/SAR_Stats_2_FINAL.pdf.

140 *See id.* at 34.

141 *See, e.g.*, Remarks by Comptroller Thomas J. Curry to the Institute for International Bankers (Mar. 2, 2015), *available at* http://www.occ.gov/news-issuances/speeches/2015/pub-speech-2015-32.pdf. *See also* Testimony of John W. Carlson of the Financial Services Information Sharing and Analysis Center to the U.S. House of Representatives Committee on Financial Services (Jun. 24, 2015), *available at* https://www.fsisac.com/sites/default/files/news/JCarlson%20June%2024%20Testimony%20FINAL.pdf.

142 "NYDFS Announces Final BitLicense Framework for Regulating Digital Currency Firms" (Jun. 3, 2015), *available at* http://www.dfs.ny.gov/about/speeches/sp1506031.htm; "NYDFS Announces Approval of First BitLicense Application from a Virtual Currency Firm" (Sept. 22, 2015), *available at* http://www.dfs.ny.gov/about/press/pr1509221.htm.

143 "Guidance for a Risk-Based Approach to Virtual Currencies" (Jun. 2015), *available at* http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html.

144 "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (Mar. 18, 2013), *available at* https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

145 FinCEN Ruling, Application of FinCEN's Regulations to Persons Issuing Physical or Digital Negotiable Certificates of Ownership of Precious Metals (Aug. 14, 2015), *available at* https://www.fincen.gov/news_room/rp/rulings/html/FIN-2015-R001.html.

ENDNOTES (CONTINUED)

146 "NYDFS Announces Approval of First BitLicense Application from a Virtual Currency Firm" (Sept. 22, 2015), *available at* http://www.dfs.ny.gov/about/press/pr1509221.htm.

147 Entities exempt from the DFS's licensing requirements under its new BitLicense rules, to which the AML compliance provisions of the rules apply, include (1) any entity that is chartered under the New York Banking Law and approved by the DFS to engage in virtual currency business activity, and (2) merchants and consumers that utilize virtual currency solely for the purchase or sale of goods or services or for investment purposes. This latter provision is analogous to one of the exemptions to the definition of a money transmitter, as provided in 31 C.F.R. §1010.100(ff).

148 By contrast, federal regulations require enhanced due diligence on correspondent accounts maintained for a foreign bank in more limited circumstances, such as when the foreign bank operates under an offshore banking license, a banking license issued by certain foreign countries designated as non-cooperative by certain intergovernmental groups or organizations, or a banking license issued by a country designated by the Secretary of the Treasury as warranting special measures. *See* 12 C.F.R. § 1010.610(c).

149 "The Real Cost of Applying for a New York BitLicense," Coin Desk (Aug. 13, 2015), *available at* http://www.coindesk.com/real-cost-applying-new-york-bitlicense/; "New York Bitcoin Scene Divided As BitLicense Deadline Looms," Coin Desk (Aug. 7, 2015), *available at* http://www.coindesk.com/new-york-bitcoin-scene-divided-as-bitlicense-deadline-looms/.

150 "State Regulatory Requirements for Virtual Currency Activities – CSBS Model Regulatory Framework" (Sept. 15, 2015), *available at* https://www.csbs.org/regulatory/ep/Documents/CSBS-Model-Regulatory-Framework(September%2015%202015).pdf.

151 "An Act Concerning Mortgage Correspondent Lenders, The Small Loan Act, Virtual Currencies and Security Freezes on Consumer Credit Reports," Substitute for Raised H.B. No. 6800, Connecticut General Assembly, *available at* https://www.cga.ct.gov/2015/act/pa/2015PA-00053-R00HB-06800-PA.htm.

152 "An Act to Repeal Section 107 of the Corporations Code, and to add Section 2178 to, and to add Division 11 (commencing with Section 26000) to, the Financial Code, relating to currency," Assembly Bill No. 1326, California Legislature, *available at* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB1326; "Money Transmitter Act," House Bill No. 850, The General Assembly of Pennsylvania, *available at* http://www.legis.state.pa.us/CFDOCS/Legis/PN/Public/btCheck.cfm?txtType=PDF&sessYr=2015&sessInd=0&billBody=H&billTyp=B&billNbr=0850&pn=1029; "An Act to Enact the North Carolina Money Transmitters Act as Requested by the Office of the North Carolina Commissioner of Banks," H.B. 289, General Assembly of North Carolina, *available at* http://www.ncleg.net/Applications/BillLookUp/LoadBillDocument.aspx?SessionCode=2015&DocNum=1327&SeqNum=0.

153 FATF is an inter-governmental body whose mandate is to set standards and promote effective implementation of measures for combating various threats to the integrity of the international financial system, as well as to work with international stakeholders to identify national-level vulnerabilities. FATF published the FATF Recommendations in 1990 in order to combat the laundering of drug money. Since then, the FATF Recommendations have been revised and expanded. The FATF Recommendations set forth a framework for combating money-laundering and terrorist financing and are intended to be implemented by countries through measures adapted to their particular circumstances. The FATF Recommendations, together with their Interpretive Notes and applicable definitions in the Glossary, form the FATF Standards, which are required to be implemented by all FATF members and FATF-Style Regional Bodies. The 40 recommendations cover AML/CFT policies and coordination, money-laundering and confiscation,

terrorist financing and financing of proliferation, preventive measures, transparency and international cooperation.

154 On September 17, 2015, the CFTC announced a consent order against Coinflip, Inc. d/b/a Derivabit and its chief executive officer for violations of the Commodity Exchange Act (CEA) and regulations thereunder, finding for the first time that "Bitcoin and other virtual currencies are encompassed in the definition [of 'commodity' for purposes of the CEA] and properly defined as commodities." "CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering" (Sept. 17, 2015), *available at* http://www.cftc.gov/PressRoom/PressReleases/pr7231-15; Order Instituting Proceedings Pursuant to Sections 6(c) and 6(d) of the Commodity Exchange Act, Making Findings and Imposing Remedial Sanctions (Sept. 17, 2015), *available at* http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliporder09172015.pdf. The CFTC's finding is consistent with Chairman Timothy Massad's testimony before the U.S. Senate Committee on Agriculture, Nutrition & Forestry that "[d]erivative contracts based on a virtual currency represent one area within [the CFTC's] responsibility." The CFTC's finding seems to imply that the CFTC could initiate other types of actions, such as market manipulation enforcement actions, relating to virtual currencies. Testimony of Chairman Timothy Massad before the U.S. Senate Committee on Agriculture, Nutrition & Forestry (Dec. 10, 2014), available at http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6.

155 Remarks of Jennifer Shasky Calvery, Director of FinCEN, at the West Coast AML Forum (May 6, 2015), *available at* https://www.fincen.gov/news_room/speech/html/20150506.html.

156 Jennifer Shasky Calvery, Director of FinCEN, at the ABA/ABA Money Laundering Enforcement Conference (Nov. 16, 2015), *available at* https://www.fincen.gov/news_room/speech/html/20151116.html.

157 Assessment of Civil Money Penalty, *In the Matter of Ripple Labs Inc. and XRP II, LLC* (May 5, 2015), *available at* https://www.fincen.gov/news_room/nr/pdf/Ripple_Assessment.pdf.

158 Ripple Labs Inc. Settlement Agreement (May 5, 2015), *available at* http://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/05/05/settlement_agreement.pdf.

159 Statement of Facts and Violations, Attachment A to Ripple Labs Inc. Settlement Agreement (May 5, 2015), *available at* https://www.fincen.gov/news_room/nr/pdf/Ripple_Facts.pdf.

160 Remedial Framework, Attachment B to Ripple Labs Inc. Settlement Agreement (May 5, 2015), *available at* https://www.fincen.gov/news_room/nr/pdf/Ripple_Remedial_Measures.pdf.

161 A Ripple spokesperson subsequently clarified that the required changes have "nothing to do with the protocol itself" but rather refer to "monitoring tools" used to analyze publicly available transaction data. The Wall Street Journal, BitBeat: Day After FinCEN Bombshell, Ripple Labs Addresses Concerns (May 6, 2015), *available at* http://blogs.wsj.com/moneybeat/2015/05/06/bitbeat-day-after-fincen-bombshell-ripple-labs-addresses-concerns/.

162 "Why did this hot cryptocurrency company halt new account signups?" Fortune (Jul. 9, 2015), *available at* http://fortune.com/2015/07/09/ripple-halts-new-accounts/.

163 "Ripple Trade Closing, Replaced With Wallet and Trading Portal GateHub," Finance Magnates (Dec. 15, 2015), *available at* http://www.financemagnates.com/cryptocurrency/exchange/ripple-trade-closing-replaced-with-wallet-and-trading-portal-gatehub/.

ENDNOTES (CONTINUED)

164 "Ripple Labs Admits to Criminal BSA Violations in First Concurrent FinCEN/DOJ Action Against a Virtual Currency Exchanger; Director of FinCEN Discusses Virtual Currency Supervision and Other Concerns" (May 6, 2015), *available at* https://www.sullcrom.com/ripple-labs-admits-to-criminal-bsa-violations-in-first-concurrent-fincendoj-action.

165 "SEC Charges Bitcoin Mining Companies" (Dec. 1, 2015), *available at* https://www.sec.gov/news/pressrelease/2015-271.html; Complaint and Demand for Jury Trial, *SEC* v. *Homero Joshua Garza, GAW Miners, LLC and ZenMiner, LLC*, Case 3:15-cv-01760 (D. Conn. Dec. 1, 2015). According to the SEC's Complaint, the defendants conducted a Ponzi scheme, selling "far more computing power than they owned and dedicated to virtual currency mining" and paying back investors using "money that [the investors], and others, had invested."

The SEC did not specify the factors which led to its conclusion that Hashlets were investment contracts. According to the SEC's Complaint, investors bought Hashlets, which entitled them to "a share of the profits that GAW Miners and/or ZenMiner would purportedly earn by mining virtual currencies." Nonetheless, the SEC alleged that purchasers of Hashlets "had no right to receive any piece of computer hardware at the end of their Hashlet contract" and primarily "relied solely on the efforts of GAW Miners and/or ZenMiner to generate Hashlets' expected profits." These facts, among others, seem to correspond to the *Howey* factors for establishing an investment contract: "(1) an investment of money, (2) in a common enterprise, (3) with profits to come solely from the efforts of others." *Rossi* v. *Quarmley*, 604 Fed. Appx. 171, 173 (3d Cir. 2015) (internal quotations omitted); *SEC* v. *W. J. Howey Co.*, 328 U.S. 293 (1946).

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 800 lawyers on four continents, with four offices in the United States, including its headquarters in New York, three offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future related publications from Stefanie S. Trilling (+1-212-558-4752; trillings@sullcrom.com) in our New York office.

New York		
Nicolas Bourtin	+1-212-558-3920	bourtinn@sullcrom.com
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Elizabeth T. Davy	+1-212-558-7257	davye@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
Jared M. Fishman	+1-212-558-1689	fishmanj@sullcrom.com
C. Andrew Gerlach	+1-212-558-4789	gerlacha@sullcrom.com
Wendy M. Goldberg	+1-212-558-7915	goldbergw@sullcrom.com
Steven R. Peikin	+1-212-558-7228	peikins@sullcrom.com
Karen Patton Seymour	+1-212-558-3196	seymourk@sullcrom.com
Samuel W. Seymour	+1-212-558-3156	seymours@sullcrom.com
Donald J. Toumey	+1-212-558-4077	toumeyd@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com
Michael M. Wiseman	+1-212-558-3846	wisemanm@sullcrom.com
Washington, D.C.		
Eric J. Kadel, Jr.	+1-202-956-7640	kadelej@sullcrom.com
William F. Kroener III	+1-202-956-7095	kroenerw@sullcrom.com
Stephen H. Meyer	+1-202-956-7605	meyerst@sullcrom.com
Jennifer L. Sutton	+1-202-956-7060	suttonj@sullcrom.com
Andrea R. Tokheim	+1-202-956-7015	tokheima@sullcrom.com
Samuel R. Woodall III	+1-202-956-7584	woodalls@sullcrom.com