PAUL HASTINGS
STAY CURRENT
A CLIENT ALERT FROM PAUL HASTINGS

April 2015

Key Trends in BSA/AML Compliance: Heightened Regulatory Expectations as Industry Growth Presents New Challenges

BY THE GLOBAL BANKING AND PAYMENT SYSTEMS PRACTICE

As the Federal Banking Agencies ("FBAs")[1] continue to sharpen and focus supervisory attention on enforcement of the Bank Secrecy Act ("BSA") and U.S. anti-money laundering ("AML") laws, banks are facing new and difficult regulatory, supervisory, and compliance challenges. Importantly, these developments have been accompanied by a marked uptick in BSA/AML enforcement activity by the FBAs and the Financial Crimes Enforcement Network ("FinCEN"). Highlighting this renewed emphasis, in August 2014, FinCEN issued an advisory emphasizing its expectations for financial institutions' BSA/AML compliance programs, including: engagement and accountability of financial institution management and directors; allocation of sufficient compliance staffing and related resources; sharing of relevant compliance related information across business units; competent and independent testing of an institution's BSA/AML compliance program, as well as periodic updates to address emerging issues and trends; and an enterprise-wide understanding of the critical role of BSA/AML reporting requirements.[2]

Perhaps more significantly, since 2012, the FBAs and FinCEN have brought a number of high profile supervisory and enforcement actions involving BSA/AML compliance issues against financial institutions, including banks and nonbanks.[3] A closer review of the enforcement activity since the beginning of 2014 reveals that the FBAs have not only increased their attention on and heightened their expectations for BSA/AML compliance for banks and thrifts, but have also expanded their focus to impose enforcement actions against a broader range of institutions, as well as individual officers of financial institutions. There is no reason to think that this activity will stop at the boardroom; in fact, the regulators have made clear their expectations for director accountability of the bank's critical compliance programs.

The emphasis on BSA/AML compliance is continuing into 2015, with a notable focus on certain hot-button issues including cryptocurrency, cybersecurity, and innovative payment technologies, such as mobile payments. The regulatory focus on these areas raises new issues for banks, including how to balance increased BSA/AML compliance obligations with monetary costs to the bank, as well as for nonbank institutions—specifically, with respect to the increasingly important role nonbank BSA/AML service providers play in the rapidly expanding footprint of the banking and financial services industry both domestically and internationally.

Recent BSA/AML Enforcement Activity

In 2014, the FBAs continued to emphasize their expectation that financial institutions establish and implement robust BSA/AML compliance programs.[4] The FBAs' heightened focus on identifying and addressing deficiencies in BSA/AML compliance programs has resulted in significant enforcement actions, including the imposition of substantial civil money penalties ("CMPs") by the FBAs and FinCEN. Among the more notable enforcement actions highlighting the FBAs' interest in and attention to BSA/AML issues, the FBAs pursued the following actions against national banks:

- In June 2014, the Office of the Comptroller of the Currency ("OCC") entered a consent order for a $500,000 CMP with a national bank based on deficiencies identified in its BSA/AML compliance program.[5] According to the OCC, during the period from 2010 to 2012 the bank, among other things, failed to (1) conduct adequate risk assessments and customer due diligence; (2) establish and implement an adequate suspicious activity monitoring system; (3) conduct adequate independent testing of its BSA/AML compliance program; and (4) provide the necessary resources and training to its BSA staff. In particular, the OCC alleged that the bank had failed to identify compliance program deficiencies and properly identify high-risk customers, resulting in the failure to timely file approximately 670 suspicious activity reports ("SARs").

- In a January 2014 agreement with FinCEN, the U.S. Attorney's Office for the Southern District of New York, and the OCC, a large national bank paid $2.05 billion to settle civil liability claims based on alleged willful violations of the BSA and the failure to report suspicious transactions arising out of a long-standing multi-billion dollar fraudulent investment scheme.[6] Under the terms of the settlement, for a number of years, bank employees had identified suspicious repeated round-dollar transactions between two prominent clients but did not file any SARs with law enforcement, even after another bank involved in the transactions filed a SAR and closed down an account owned by one of the clients. Exacerbating the situation, between 2006 and 2008, the bank conducted due diligence reviews on an investment fund and several feeder funds and identified several red flags for fraud, including: (1) investment performances that appeared too good to be true, (2) lack of transparency in investment and trading activity, (3) use of a small, unknown auditor, and (4) repeated refusal by the investment fund to fully comply with due diligence review requests. Despite the red flags, the bank failed to report its concerns to its AML personnel or to notify FinCEN, as required by law, and despite the filing of suspicious activity reports by employees at a foreign branch filed with their host country's regulator, which was known by the bank's U.S.-based AML compliance officers. FinCEN criticized the bank's failure to report these suspicious activities in light of the bank's redemption of its own investments in the suspicious funds.

- In a similar settlement with the OCC in January 2014, another bank agreed to pay a $500,000 CMP to the OCC as a result of BSA/AML compliance program deficiencies.[7] The OCC alleged that the bank's compliance department lacked resources and expertise, failed to provide for independent testing for BSA compliance, conducted inadequate risk assessments, and failed to implement an adequate suspicious activity monitoring system. The OCC also criticized the bank's internal audit review for its failure to identify the compliance program's deficiencies, which, after conducting a look back, resulted in the filing of 110 new SARs and 172 supplemental SARs.

The level of interest and enforcement activity has not abated in 2015, with the following action already noted:

- In February 2015, the OCC and FinCEN entered a consent order for a $1.5 million CMP with a community bank based on BSA violations as a result of failure to detect and adequately report suspicious transactions—the transactions involved millions of dollars in illicit proceeds from a judicial corruption scheme.[8] According to FinCEN, the bank failed to identify significant red flags, including: (1) a 2007 law enforcement subpoena submitted against individuals and entities involved in the transactions, (2) repeated round-dollar transactions, often occurring on a single day, and (3) abnormal activity volume compared to account balances. FinCEN specifically criticized the bank's failure to review for risk the accounts and documents of the individuals and entities identified in the subpoena. Another critical factor was that the bank waited two years—after the leaders of the fraud had pled guilty to criminal offenses—before filing SARs regarding the suspicious activity that totaled approximately $6.3 million.

In addition to these more typical actions involving banks, the FBAs also imposed CMPs for BSA/AML violations against a number of nonbank financial institutions, as well as individual officers. These include:

- In March 2015, the OCC and FinCEN entered a consent order for a $75,000 CMP against a money service business ("MSB") and its owner and AML compliance officer based, among other things, on willful violations of the BSA's compliance program and reporting requirements.[9] The MSB conducted check cashing services, but failed to implement an adequate AML program. The agencies alleged that the MSB lacked adequate internal controls, failed to conduct independent compliance reviews, and failed to adequately train appropriate personnel. Specifically, the company's AML compliance program lacked procedures for employees to follow when customers presented checks to be cashed for greater than $10,000 as well as procedures for verifying the accuracy of currency transaction reports ("CTRs"). Moreover, the MSB's employee training failed to address procedures related to check cashing and was conducted infrequently, with new employees not receiving training for many years. Additionally, the company and its AML officer filed CTRs late, and not at all for a period of more than two years.

- In January 2015, FinCEN and the U.S. Securities and Exchange Commission ("SEC") assessed a $20 million CMP against a securities broker-dealer for BSA violations.[10] The agencies alleged that, during the period from 2008 through May 2014, the securities broker-dealer failed to establish and implement an adequate AML program, conduct adequate due diligence on customers, and comply with requirements under Section 311 of the USA PATRIOT Act. In particular, FinCEN identified 16 customers who had engaged in suspicious patterns of trading involving penny stocks, which the security broker-dealer failed to report. The security broker-dealer also failed to conduct adequate due diligence and monitor a foreign financial institution customer that it had deemed "high risk."

- In December 2014, FinCEN assessed a $1 million CMP against the former Chief Compliance Officer ("CCO") of an MSB for his failure to ensure the MSB complied with the AML provisions of the BSA.[11] Additionally, the U.S. Attorney's Office for the Southern District of New York, acting as FinCEN's representative, filed a complaint seeking to enforce the CMP and to ban the CCO from employment in the financial industry. According to FinCEN, the CCO willfully

violated the BSA requirements to implement an effective AML compliance program and to report suspicious activity. While serving as CCO, the individual oversaw the MSB's fraud department, which received thousands of complaints from consumers who had been defrauded by agents of the MSB. FinCEN specifically alleged that the CCO failed to: (1) establish a policy for disciplining agents suspected of involvement in fraud or money laundering, (2) terminate agents known by the MSB to be engaged in fraud or money laundering, (3) ensure timely filing of SARs, (4) ensure effective audits of suspected agents were conducted, and (5) ensure the MSB performed adequate due diligence. According to FinCEN, the CCO violated his obligations as CCO, which allowed criminals to defraud thousands of innocent customers—many of whom were elderly—and launder the proceeds of such funds.

- A month earlier, in November 2014, FinCEN assessed a $300,000 CMP against a small credit union based on alleged BSA violations.[12] Notably, the credit union had only five employees and $4 million in assets. However, the credit union contracted with a third party vendor and MSB to provide services and subaccounts to 56 MSBs during the period 2009 to 2014. The 56 MSBs were not members of the credit union, were located in high-risk jurisdictions, and produced over $1 billion in transaction volume through outgoing wire transfers. During the period, the credit union failed to implement an adequate BSA compliance program and, instead, relied on the third-party vendor to conduct its required due diligence on MSBs. FinCEN cited the credit union's deficient BSA compliance program—inadequate internal controls, lack of independent testing, insufficient training, failure to designate an appropriate BSA compliance officer, and systemic reporting failures—as exposing the U.S. financial system to significant risks of money laundering and terrorist financing.

- In another settlement several months earlier, a MSB and its president/owner agreed to pay a $10,000 CMP to FinCEN for alleged violations of the BSA.[13] The president/owner served as the MSB's compliance officer, despite her lack of knowledge and experience with respect to the BSA. As a result, the MSB failed to develop an effective compliance program. Of particular concern, FinCEN noted that the MSB's inadequate policies, procedures, and internal controls failed to confirm the identities of consumers, monitor for suspicious transactions, identify currency transactions exceeding certain monetary values, provide sufficient training, or create adequate records. Additionally, the president/owner never conducted a BSA/AML risk assessment of the MSB and failed to conduct independent testing of the MSB's compliance program for a period of over six years.

Key Trends Emerging in BSA/AML Enforcement and Compliance

These recent enforcement actions highlight the ongoing expectation of the FBAs, FinCEN, and state regulators that financial institutions implement and maintain robust BSA/AML compliance programs that are appropriately tailored to the institution's risk profile. This high level of regulatory scrutiny is likely to continue for the foreseeable future, with key developments emerging to reflect the growth of—and significant changes to—the financial services industry in areas such as mobile and other emerging payment systems, continued reliance and dependence on service providers, and rapidly increasing cybersecurity risks. Based on last year's actions, financial institutions should understand and remain current on the following enforcement trends:

Increased Focus on MSBs, Including Cryptocurrency Companies

Although the FBAs have always had the authority, for purposes of the BSA and FinCEN's implementing regulations, to regulate and bring enforcement actions against a broad range of financial institutions, historical enforcement actions typically focused on banks and, occasionally, their third party service providers. Notably, 2014 marked an expansion in the regulators' increasing focus on nonbank financial institutions, such as MSBs and securities broker-dealers. Although the enforcement actions taken against MSBs in 2014 generally involved system due diligence, risk monitoring, and reporting failures, the actions also highlight the increased risks and heightened regulatory scrutiny surrounding MSBs.

Since the enactment of the USA PATRIOT Act in 2001, regulatory supervision and enforcement actions have increasingly scrutinized potential money laundering activities, and MSBs have been perceived as higher-risk customers in the wake of these developments. Due to concerns with regulatory scrutiny, uncertainty of regulatory expectations, the risks presented by various types of MSB accounts, and the costs and burdens associated with maintaining MSB accounts,[14] many banks have limited MSBs' access to banking products and services. In response to this "de-risking" of bank MSB operations, the FBAs have recently taken steps to clarify that banks should not be discouraged from working with and serving MSBs, but should have appropriate risk mitigation measures in place to do so.[15]

A similar approach may be taking shape with respect to the cryptocurrency industry. With the continued expansion of the industry, cryptocurrency companies and financial institutions providing products and services to those in the industry are likely to face increased regulatory scrutiny. For example, in July 2014, the New York State Department of Financial Services ("NYDFS") proposed to develop a regulatory licensing framework for virtual currency businesses.[16] Under the proposed framework, licenses would be required for businesses engaged in: (1) receiving or transmitting virtual currency on behalf of consumers; (2) securing, storing, or maintaining custody or control of such virtual currency on the behalf of customers; (3) performing retail conversion services; (4) buying and selling virtual currency as a customer business; or (5) controlling, administering, or issuing a virtual currency.[17] Such licenses would be required, among other things, to maintain robust AML compliance programs that, at a minimum, provide internal controls to ensure ongoing compliance with applicable BSA/AML laws and regulations, provide for independent testing, designate a qualified individual for coordinating and monitoring day-to-day compliance, and provide ongoing training to appropriate personnel.[18] To date, four other states—Hawaii, Idaho, Vermont, and Washington—actively license, regulate, and oversee the transmission of virtual currency. Two additional states—California and North Carolina—are in the process of or considering doing so.

As the cryptocurrency industry grows, state and federal banking regulators will be certain to increase their scrutiny of bank practices related to cryptocurrency customers, and/or follow New York's efforts to impose licensure and industry-specific BSA/AML requirements on the cryptocurrency industry.

Innovative Payment Technologies May Present a Challenge to the FBAs

As the payment systems industry continues its rapid growth, innovative and emerging payment technologies and new market participants will present new regulatory challenges and issues for the FBAs, FinCEN, state regulators, and law enforcement.

In particular, as nonbank companies such as telecommunications providers begin to offer new payment systems to their consumers, the FBAs and other regulators will not only need to understand these technologies, but also grapple with their role as regulators to the financial services industry. In most cases, the FBAs have supervisory and examination authority over industry participants

pursuant to the Bank Service Company Act; however, in some cases the FBAs' regulatory jurisdiction may be unclear. Innovations in payment technologies, like the development of mobile wallets and other mobile payment systems, have resulted in an overlap of financial and telecommunication regulatory schemes. Mobile payment services, in particular, are currently subject to oversight by the FCC with respect to mobile carrier standards and competition, the FTC with respect to consumer protection and identity fraud, and the FBAs with respect to consumer protection and banking regulations, including BSA/AML compliance.[19] Although it is generally understood that the FBAs' regulations and laws applicable to payment methods (credit, debit, prepaid, and ACH) govern these mobile payments, uncertainty remains with respect to coverage and liability responsibilities.[20] Unlike traditional banking products that allow financial institutions to control much of a transaction, "mobile payments require the coordinated and secure exchange of payment information over several unrelated entities,"[21] many of which have not previously been subject to the FBA's oversight and supervision.

In addition to the challenge of converging telecommunication and financial regulatory schemes, mobile payments present increased risks of money laundering and financing of terrorism activities. For example, criminals have increased access to a consumer's banking account by stealing a mobile phone with inadequate security or hacking a wireless network that transfers the financial data for such account. The continued growth of the mobile payments industry is requiring the FBAs to determine which technologies to supervise, how to supervise such technologies, and which technologies are more appropriately and effectively regulated by other agencies (i.e., the FCC or FTC).

Implications for Community Banks

As highlighted by FinCEN's imposition of a CMP on a small credit union in April 2014, every financial institution is expected to establish a BSA/AML compliance program commensurate with the institution's risk level, regardless of the institution's size or staffing. Financial institutions must carefully consider the risks associated with their customers and lines of business to determine what resources are required to adequately monitor BSA/AML risks. Importantly, smaller financial institutions must walk a fine line between heightened regulatory expectations requiring robust compliance programs, and managing the typically higher costs of such compliance programs. And this is not only a financial resources issue; some banks have faced regulatory criticism due to skyrocketing compliance costs. Typically, it is not uncommon for a small community bank's earnings to suffer as a result of such costs. The enhanced scrutiny on BSA/AML compliance for small financial institutions and increased regulatory expectations present the very real risk that small financial institutions may effectively be supervised out of the market. This is an issue with which the FBAs and other regulators are aware and continuously trying to address, but for which there are no ready solutions.

Oversight of Third Party Vendors

The FBAs have made clear that reliance on third party service providers for due diligence will not be sufficient to satisfy regulatory expectations. While financial institutions may appropriately outsource aspects of their BSA/AML compliance programs to third party compliance vendors, financial institutions and their officers will ultimately be held responsible for the institution's BSA/AML compliance program. It is critical that institutions using third party vendors take appropriate measures to oversee vendors' ongoing activities and operations on behalf of the bank, as well as to implement additional checks and controls within the institution to oversee and ensure compliance on a real-time basis.

Cybersecurity

FBAs are increasingly considering a financial institution's cybersecurity measures as part of the institution's BSA/AML compliance obligations. In a March 2, 2015 speech by OCC Comptroller Curry before the Institute of International Bankers, Comptroller Curry noted "the goals of BSA/AML and cybersecurity are increasingly converging. Terrorists, drug cartels, and cybercriminals all have a need to generate cash and move money, and it would seem that many of them would share some of the same goals. There are lessons to be learned from our decades-long experience in BSA enforcement that can be applied to the cybersecurity area, and vice versa."[22] Clearly, this is a time in which financial institutions of all sizes should be expecting increased FBA supervision of their cybersecurity measures, including as an ongoing part of both their supervisory safety and soundness and regulatory compliance examinations.

Focus on Individual Accountability[23]

Financial institutions and their staff must also be aware of and vigilant with respect to understanding the scope and nature of enforcement actions that could be brought directly against individual officers and directors for institutional BSA/AML compliance failures. As highlighted in several of the enforcement actions discussed above, the FBAs may hold individual officers accountable for compliance program deficiencies, regardless of whether the officers serve at national banks with significant experience and compliance resources, at small insured institutions, or at relatively new MSBs or other nonbank entities.

In addition to these enforcement actions, the Comptroller raised the issue of senior management "oversight accountability" for BSA/AML compliance, suggesting that financial institutions should be required to establish "clear lines of accountability that make it possible to hold senior executives responsible for serious compliance breakdowns that lead to BSA program violations."[24] State regulators appear to be adopting a similar approach. For example, NYDFS Superintendent Benjamin Lawsky has stated that "fines—while often necessary—are not sufficient to deter misconduct on Wall Street … We must also work to impose individual accountability, where appropriate, and clearly proven, on specific bank employees that engaged in wrongdoing."[25] NYDFS put its theory into action last year, requiring a bank, as part of a settlement agreement for violating U.S. sanctions and anti-money laundering rules, to terminate 13 officers and discipline 45 employees found responsible for or complicit with the bank's alleged misconduct.[26]

Action Plan for Financial Institutions

Given the increasingly complex BSA/AML compliance landscape, it is critical for banks and nonbank financial firms to develop and implement an action plan to address the heightened regulatory scrutiny and program risks presented with BSA/AML compliance. This requires an enterprise-wide review and assessment of BSA/AML risk, regardless of the size and complexity (or lack thereof) of a financial institution's operations. At a minimum, an action plan should include the following:

- ***Ensure a Strong Top-Down Compliance Culture.*** Involvement by bank senior officers and directors in understanding and overseeing a financial institution's BSA/AML compliance program is a key element of an effective program. Directors must be active participants in reviewing and overseeing an institution's compliance function and activities. Boards of directors should consider building BSA/AML compliance measures into the performance criteria for senior bank and business unit managers, ensuring that responsibility for oversight is assumed at the highest levels of the organization. This should include implementing clearly

defined channels for reporting compliance deficiencies, and conducting thorough board reviews of BSA/AML compliance lapses to assess program weaknesses and determine whether additional board action may be warranted to address compliance program deficiencies. Implementing a strong compliance culture at all levels of the organization will help to ensure that employees recognize that compliance is a top priority.

- ***Committing Sufficient Personnel and Technological Resources, While Avoiding Excessive Overhead Costs.*** As discussed above, there has been increased tension between financial institutions' BSA/AML compliance obligations and the need to keep overhead costs appropriate for the size of the institution. A financial institution must be able to demonstrate to regulators that it has committed the necessary resources—and is willing and able to invest additional resources, as appropriate—to establish and maintain a robust BSA/AML compliance program, including investments in technology, staff, training, and monitoring capabilities. The cost of committing adequate resources up-front will produce benefits in terms of reduced risk exposure and potential remedial costs and fines for failing to take the necessary actions to achieve and maintain BSA/AML compliance.

- ***Focus on Cybersecurity.*** In addition to maintaining updated information technology ("IT") software and programs, management and boards should ensure adequately trained staffing to monitor and supervise these processes and programs. Examiners will typically probe IT systems and back-end analytical departments to ensure that case management processes for unique or unusual transactions are supported by reasonable financial intelligence.

- ***Risk Management.*** Regulators will continue to examine financial institutions with a focus on ensuring that senior management and boards of directors have taken the time to identify the particular risks posed by a financial institution's business model and designed a BSA/AML compliance program that addresses such risks. Institutions should consider reviewing and updating their internal controls as necessary to address new and increased risks associated with particular industries and customers.

- ***Effective Detection and Reporting.*** Effective transaction monitoring and detection systems should be deployed and sufficiently staffed by trained personnel. While the particulars of a financial institution's detection and reporting system will be based on its size and BSA/AML risk profile, senior management should ensure that a financial institution's BSA and SARs policies are clear, precise and leave limited discretion to lower-level employees, which will promote consistent and timely filing. In addition to general BSA/AML training provided to all employees, financial institutions should consider additional training targeted at certain business units that pose higher risks and should make sure that such units are appropriately designed and equipped to detect and report suspicious activities related to heightened BSA/AML risks.

- ***Smaller Financial Institution Risks.*** Smaller financial institutions should identify particular lines of business or geographic regions that pose higher risks, and ensure such risks are specifically reflected and addressed in their BSA/AML compliance program, policies, and procedures. For example, an institution may not have a significant foreign presence, but may engage in issuing prepaid cards, supporting cash intensive businesses, have significant mobile banking platforms, and/or may serve particular groups of high-risk customers, all of which increase the institution's overall BSA/AML risk profile.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Atlanta

Todd W. Beauchamp
1.404.815.2154
toddbeauchamp@paulhastings.com

Chris Daniel
1.404.815.2217
chrisdaniel@paulhastings.com

Erica Berg Brennan
1.404.815.2294
ericaberg@paulhastings.com

Heena A. Ali
1.404.815.2393
heenaali@paulhastings.com

Kevin P. Erwin
1.404.815.2312
kevinerwin@paulhastings.com

Meagan E. Griffin
1.404.815.2240
meagangriffin@paulhastings.com

Diane Holden
1.404.815.2326
dianeholden@paulhastings.com

London

Ben Regnard-Weinrabe
+44 020 3023 5185
benregnardweinrabe@paulhastings.com

Nikki Johnstone
+44 020 3023 5112
nikkijohnstone@paulhastings.com

Miah Ramanathan
+44 020 3023 5178
miahramanathan@paulhastings.com

Palo Alto

Cathy S. Bedya
1.650.320.1824
cathybeyda@paulhastings.com

San Francisco

Thomas P. Brown
1.415.856.7248
tombrown@paulhastings.com

Stan Koppel
1.415.856.7284
stankoppel@paulhastings.com

Ryan M. Decker
1.415.856.7237
ryandecker@paulhastings.com

Molly E. Swartz
1.415.856.7238
mollyswartz@paulhastings.com

Paul M. Schwartz
1.415.856.7090
paulschwartz@paulhastings.com

Washington, D.C.

V. Gerard Comizio
1.202.551.1272
vgerardcomizio@paulhastings.com

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Lawrence D. Kaplan
1.202.551.1829
lawrencekaplan@paulhastings.com

Gerald S. Sachs
1.202.551.1975
geraldsachs@paulhastings.com

Alexandra L. Anderson
1 202 551 1969
alexandraanderson@paulhastings.com

Laura E. Bain
1.202.551.1828
laurabain@paulhastings.com

Ryan A. Chiachiere
1.202.551.1767
ryanchiachiere@paulhastings.com

Katie A. Croghan
1.202.551.1849
katiecroghan@paulhastings.com

Lauren Kelly D. Greenbacker
1.202.551.1985
laurenkellygreenbacker@paulhastings.com

Amanda Kowalski
1.202.551.1976
amandakowalski@paulhastings.com

---

[1] The FBAs are the Office of the Comptroller of the Currency ("OCC"), the Federal Deposit Insurance Corporation ("FDIC"), and the Board of Governors of the Federal Reserve System ("FRB").

[2] *See* Financial Crimes Enforcement Network, FIN-2014-A007, *Advisory to U.S. Financial Institutions on Promoting a Culture of Corporate Compliance* (August 11, 2014) ("Advisory"), *available at* http://fincen.gov/statutes_regs/guidance/pdf/FIN-2014-A007.pdf.

[3] For purposes of the BSA and FinCEN implementing regulations, a "financial institution" includes: banks, trust companies, U.S. agencies or branches of foreign banks, credit unions, and thrifts; brokers or dealers in securities or commodities

and investment companies; currency exchangers, issuers, redeemers, or cashiers of travelers checks, checks, money orders, or similar instruments; insurance companies; dealers in precious metals, stones, or jewels; pawnbrokers and loan or finance companies; money transmitters; and certain casinos or gaming establishments. See 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).

[4] Paul Hastings previously detailed the rise in BSA/AML and OFAC enforcement activity targeted at depository institutions in the Paul Hastings Client Alert titled *AML/BSA and OFAC Compliance—Higher Stakes and Greater Consequences for Banks* (March 2013), *available at* http://www.paulhastings.com/docs/default-source/PDFs/stay-current---bsaaml-and-ofac-compliance-higher-stakes-and-greater-consequences-for-banksdf36df6923346428811cff00004cbded.pdf.

[5] *See* OCC EA 2014-094, AA-EC-2014-60 (June 26, 2014), *available at* http://www.occ.gov/static/enforcement-actions/ea2014-094.pdf.

[6] *See* FinCEN Matter No. 2014-1 (January 7, 2014), *available at* http://www.fincen.gov/news_room/ea/files/JPMorgan_ASSESSMENT_01072014.pdf.

[7] *See* OCC EA 2014-006, AA-EC-2013-11 (January 14, 2014), *available at* http://www.occ.gov/static/enforcement-actions/ea2014-006.pdf.

[8] *See* FinCEN number 2015-03 (February 27, 2015), *available at* http://www.fincen.gov/news_room/ea/files/FNCB_Assessment.pdf.

[9] See FinCEN number 2015-03 (February 27, 2015), *available at* http://www.fincen.gov/news_room/ea/files/FNCB_Assessment.pdf.

[10] *See* Press Release, FinCEN (January 27, 2015), *available at* http://www.fincen.gov/news_room/nr/html/20150127.html.

[11] *See* Press Release, FinCEN (December 18, 2014), *available at* http://www.fincen.gov/news_room/nr/pdf/20141218.pdf.

[12] *See* Press Release, FinCEN (November 25, 2014), *available at* http://www.fincen.gov/news_room/nr/html/20141125.html.

[13] *See* FinCEN Matter No. 2014-03 (April 23, 2014), *available at* http://www.fincen.gov/news_room/ea/files/NMCE%20Assessment.pdf.

[14] *See* OCC Acting Comptroller Julie L. Williams, Testimony before Committee on Banking, Housing, and Urban Affairs of the U.S. Senate at 12 (April 26, 2005).

[15] *See* Cohen Speech; *see also* FinCEN Statement.

[16] *See* Press Release, NYDFS (July 17, 2014), *available at* http://www.dfs.ny.gov/about/press2014/pr1407171.html.

[17] *See* Press Release, NYDFS (July 17, 2014), *available at* http://www.dfs.ny.gov/about/press2014/pr1407171.html.

[18] *See* Section 200.15 of proposed BitLicense Regulatory Framework (February 25, 2014), *available at* http://www.dfs.ny.gov/legal/regulations/revised_vc_regulation.pdf; *see also* Press Release, NYDFS (July 17, 2014), available at http://www.dfs.ny.gov/about/press2014/pr1407171.html.

[19] *See* Federal Reserve Bank of Atlanta, *The U.S. Regulatory Landscape for Mobile Payments* (July 25, 2012).

[20] *See* Federal Reserve Bank of Atlanta, *The U.S. Regulatory Landscape for Mobile Payments* (July 25, 2012).

[21] *See* FDIC, *Supervisory Insights—Winter 2012—Mobile Payments: An Evolving Landscape* (January 3, 2013), *available at* https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin12/mobile.html.

[22] 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.

[23] For additional detail on the growing threat of enforcement actions targeted at individual financial institution officers and directors for institutional violations of law, please see the recently issued Paul Hastings Client Alert titled *Getting Personal—Financial Regulators Warn of New Era of Individual Responsibility* (April 2014), *available at* http://www.paulhastings.com/docs/default-source/PDFs/getting-personal-financial-regulators-warn-of-new-era-of-individual-responsibility.pdf.

[24] Thomas J. Curry, *Remarks Before the Association of Certified Anti-Money Laundering Specialists* (March 17, 2014), *available at* http://www.occ.gov/news-issuances/speeches/2014/pub-speech-2014-39.pdf.

[25] Press Release, New York Department of Financial Services (November 18, 2014), *available at* http://www.dfs.ny.gov/about/press2014/pr1411181.htm.

[26] Press Release, New York Department of Financial Services (June 30, 2014), *available at* http://www.dfs.ny.gov/about/press2014/pr1406301.htm.