



## *Promoting a Culture of BSA/AML Compliance – FinCEN Ups the Ante*

BY [LAWRENCE KAPLAN](#), [MICHAEL HERTZBERG](#) & LAURA BAIN

Following several notable criminal and civil enforcement actions against financial institutions (“Financial Institutions”),<sup>1</sup> the Financial Crimes Enforcement Network (“FinCEN”) recently issued a regulatory advisory to emphasize certain critical elements of an effective Bank Secrecy Act (“BSA”) and anti-money laundering (“AML”) compliance program (the “Advisory”).<sup>2</sup> The Advisory focuses on effective steps that Financial Institutions and their leadership should take to “improve and strengthen organizational compliance with BSA/AML obligations.”<sup>3</sup> The enhanced focus on BSA/AML compliance by both FinCEN and each of the federal banking agencies (“FBAs”)<sup>4</sup> dictates that all Financial Institutions — from multinational bank holding companies to regional and community banks to non-bank financial services companies — should review and update, as appropriate, their BSA/AML compliance programs and policies to ensure they conform to the heightened regulatory expectations detailed in the Advisory.

### **FinCEN Advisory**

Critical elements that FinCEN expects Financial Institutions to incorporate in their BSA/AML compliance programs going forward, i.e., in addition to those proscribed by applicable BSA regulations,<sup>5</sup> include:

- *Leadership Engagement.* BSA compliance starts with a Financial Institution’s leadership, which may include its board of directors, senior executive management, owners and operators.<sup>6</sup> These individuals must ensure there is visible leadership support to create a “culture of compliance” at the Financial Institution.<sup>7</sup> FinCEN expects that an engaged leadership should receive periodic BSA/AML training tailored to their specific role, have an appropriate understanding of BSA/AML obligations and compliance so that the Financial Institution may effectively allocate resources to its BSA/AML function, and remain informed of the Financial Institution’s record of BSA/AML compliance.<sup>8</sup> Comptroller of the Currency Thomas Curry made similar comments in March 2013 when he identified “the strength of an institution’s compliance culture” as one of the critical ingredients to an effective BSA/AML compliance program.<sup>9</sup>
- *Compliance Not Sacrificed for Revenue Interests.* The governance structure of a Financial Institution should ensure that compliance staff has sufficient resources, authority and autonomy to implement a Financial Institution’s AML program, as well as the ability to independently take actions to address and mitigate risks that might arise from particular business lines and to file any necessary reports, such as Suspicious Activity Reports (“SARs”).<sup>10</sup> For example, the Advisory raises concerns that although money services

businesses (“MSBs”) often receive a significant percentage of their revenue from agents, if an MSB agent is found to be engaging in an activity that raises significant BSA/AML compliance risks (such as not observing contractually required Know-Your-Customer procedures), the MSB should be able to investigate and take action based on the results of the compliance investigation, regardless of the impact on revenue.<sup>11</sup>

- *Effective Information Sharing.* Financial Institutions should ensure that information relevant to BSA/AML compliance is shared across business units and, for larger Financial Institutions, affiliated entities.<sup>12</sup> This element is based upon several recent enforcements against Financial Institutions where a lack of effective information sharing with compliance staff was cited as a significant concern.<sup>13</sup> Examples of effective information sharing include a casino sharing significant customer information developed for marketing purposes with compliance staff, or a mutual fund providing relevant customer transaction information developed through a frequent trade monitoring program to BSA/AML compliance staff. At the same time, Financial Institutions must ensure that all shared information remains subject to applicable privacy safeguards.
- *Adequate Human and Technological Resources.* In addition to having a knowledgeable and competent BSA officer, as required by FinCEN and FBA regulations,<sup>14</sup> a Financial Institution should ensure that it devotes appropriate support staff and technological resources, such as automated transaction monitoring systems, to its BSA/AML compliance program based on its risk profile.
- *Independent and Competent Testing.* BSA/AML program testing is deemed to be effective where the party testing the program (external or internal) is “independent, qualified, unbiased and does not have conflicting business interests that may influence the outcome of the compliance program test.”<sup>15</sup> This permits a Financial Institution to locate and take appropriate corrective action where BSA/AML compliance deficiencies are identified.
- *Leadership Understanding of BSA Reporting.* All employees of a Financial Institution, from the Chairman of the Board to customer-facing staff, must understand what purpose BSA reports serve and how such information is used.<sup>16</sup> This requires training that demonstrates the value of such reports in confronting serious national security threats — including terrorist organizations, rouge nations, weapons of mass destruction proliferators and foreign corruption — as well as in supporting law enforcement priorities, such as combatting transnational criminal organizations and cyber-theft.<sup>17</sup>

## Recent BSA/AML Enforcement Activity

The FBAs have indicated a renewed focus on BSA/AML compliance after a slow-down in the aftermath of the 2008 financial crisis.<sup>18</sup> This renewed 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”) in some cases. Clearly, the Advisory is based, in part, upon the following recent enforcement actions:

- In June 2014, the OCC entered into a consent order for a CMP with a national bank based on deficiencies in the institution’s BSA/AML compliance program. Under the consent order, the bank agreed to pay a \$500,000 CMP based in part on inadequate independent testing of its BSA/AML compliance program and its failure to provide sufficient resources and training for its BSA compliance staff.<sup>19</sup>

- In January 2014, a national bank agreed to pay a \$500,000 CMP to the OCC in response to identified BSA/AML deficiencies in the bank's compliance program. According to the OCC, the bank's compliance department lacked resources and expertise, and failed to implement an adequate suspicious activity monitoring system or conduct adequate risk assessments. The OCC also criticized the bank's internal audit review for failing to identify the bank's compliance program deficiencies, which, upon conducting a look back, resulted in the bank filing 110 new SARs and 172 supplemental SARs.<sup>20</sup>
- In a similar settlement that same month with FinCEN, the U.S. Attorney's Office for the Southern District of New York, and the OCC, another bank paid \$2.05 billion to settle civil liability claims based on suspicious transactions that flowed through it but were not reported. For a period of more than 10 years the bank's employees had identified repeated round-dollar transactions between two clients but did not report these transactions to the bank's AML personnel. Additionally, between 2006 and 2008, the bank conducted due diligence reviews on an investment fund and several feeder funds, identifying several fraud red flags, but failed to report the red flags or concerns to its AML personnel and to notify FinCEN as required by law. Moreover, employees from a foreign branch filed suspicious activity reports with their host-country's regulator, but the bank's U.S. legal and investment bank compliance employees did not share this information with the bank's BSA officer or AML operations, or notify FinCEN. FinCEN criticized the bank's failure to report these suspicious activities to its compliance staff in light of the bank's investment in the suspicious funds for its own profit.<sup>21</sup>
- In September 2013, a bank consented to a \$4.1 million CMP issued by FinCEN and the OCC based on various BSA violations, alleging that the bank had "focused on revenue generation" from certain suspicious accounts "rather than the associated risks." In particular, the agencies alleged that the bank failed to ensure it had appropriate compliance staffing and adequate oversight over compliance responsibilities, resulting in the failure to timely file approximately 190 SARs.<sup>22</sup>
- In December 2012, in one of the most significant BSA/AML-related enforcement actions to date, the OCC and FRB entered into consent cease and desist orders and consent orders for CMPs of \$500 million and \$165 million, respectively, for BSA/AML violations by a national bank and its holding company and affiliates.<sup>23</sup> The multi-agency settlement also included \$1.9 billion in penalties against the bank and its holding company and affiliates levied by the OCC, the FRB, FinCEN, the Treasury Department's Office of Foreign Assets Control ("OFAC"), and the Department of Justice.<sup>24</sup> The OCC noted that the bank's BSA/AML program failed in identifying, monitoring, and reporting illicit financial activities, which had a direct impact on the ability of law enforcement to combat transnational criminal activity. Under the multi-agency settlement, the bank and its holding company agreed to undertake various remedial actions to implement the necessary internal controls, staff training, and resources to assess BSA/AML violations in high-risk transactions; establish and maintain a BSA/AML compliance committee that meets at least monthly; and implement an enterprise-wide BSA/AML compliance program.

## **Key Trends Regarding BSA/AML Enforcement and Compliance**

The Advisory and the recently publicized enforcement actions highlight several key BSA/AML compliance and enforcement trends facing Financial Institutions today, including:

### ***Regulating through Enforcement Actions***

While the Advisory serves as a helpful roadmap for Financial Institutions attempting to comply with current BSA/AML regulatory expectations, many critical details for effective BSA/AML compliance continue to be transmitted through examinations and, particularly, through enforcement proceedings. BSA/AML compliance officers should continue to review publicly-available enforcement actions to identify new trends and issues that regulators are highlighting.

### ***Deputizing Banks for BSA Enforcement***

While the Advisory is applicable to a broader universe of Financial Institutions than just depository institutions, the renewed focus of the FBAs on BSA/AML compliance should serve as a reminder to depository institution compliance staff that FBAs are focused on not just how an institution ensures compliance with its own activities, but also those of its clients and account holders.

### ***Focus on Individual Responsibility<sup>25</sup>***

Bankers and compliance staff should be particularly mindful of enforcement actions that could be directly targeted at individuals for institutional BSA/AML compliance failures. For example, in 2013 the U.S. Department of the Treasury, which administers FinCEN and the OFAC, announced its intention to hold individual bankers liable for wrongful acts that involve money laundering activities and to seek financial penalties against individuals culpable for implementing or orchestrating corporate acts that were at the heart of the wrongdoing.<sup>26</sup> Additionally, in February 2014, the Financial Industry Regulatory Authority fined both Brown Brothers Harriman \$8.0 million and its Global AML Officer \$25,000; the AML officer also was suspended for one month.<sup>27</sup> Similarly, in March 2014, the Comptroller of the Currency raised the issue in the context of AML actions, suggesting that senior bank managers should be held personally accountable for BSA risk management failures and deficiencies, especially when there is a conscious decision or deliberate action not to commit the requisite resources and expertise necessary to maintain an AML program that meets the requirements of law and/or the expectations of the regulators.<sup>28</sup> And it is not just federal regulators that are taking this view. The New York Department of Financial Services, an active enforcer in the AML context, is also now seeking personal accountability for bank officers and directors who bear responsibility for an institution's wrongful acts.<sup>29</sup>

### ***Effect on Corporate Activity***

The failure of a Financial Institution to comply with regulators' heightened BSA/AML compliance expectations may lead to substantial consequences beyond compliance costs or enforcement activity, and may impact the ability of management to carry out strategic corporate initiatives. For example, the pending acquisition of Hudson City Bancorp by M&T Bank Corp has been held up for more than two years due to FRB concerns over M&T's BSA/AML compliance program.<sup>30</sup>

## Action Plan for Financial Institutions

It is imperative for depository and non-depository Financial Institutions 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 Compliance Culture at the Top.** Involvement by bank senior officers and directors in understanding and overseeing a Financial Institution's BSA/AML compliance program is a key element of both the Advisory and recent BSA/AML enforcement actions taken against Financial Institutions. In addition to the periodic executive training and review noted by the Advisory, an institution's senior management and the board of directors should consider the following:
  - Building BSA/AML compliance measures into the performance criteria for senior bank and business unit managers. It is not solely the responsibility of the compliance function to be accountable for BSA/AML compliance; accountability and program oversight must be assumed by business unit management, with clear lines of communication established with senior management. In addition, directors must be active participants in reviewing and overseeing a Financial Institution's compliance function and activities.
  - Financial Institutions should also consider ways to ensure that responsibility for oversight is assumed at the highest levels of an organization, including imposing claw-back provisions for senior officers in the event that BSA/AML violations occur, to ensure senior management accountability for BSA/AML compliance.
  - Implementing clearly defined channels for informing the board of directors, a committee of the board, and/or senior management of potential compliance deficiencies to ensure the independence of senior compliance and/or BSA/AML compliance officials.
  - Conducting thorough board reviews of BSA/AML compliance lapses, including where the lapses were self-identifiable, to assess program weaknesses and determine whether additional board action may be warranted to address compliance program deficiencies.
- **Commit Sufficient Human and Technological Resources.** 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. While Financial Institutions are continually facing pressures to reduce overhead and expenses, particularly as revenue growth slows, BSA/AML compliance efforts should not be part of any planned cost-cutting measures. For example, following the imposition of CMPs on one of the banks referenced above, the Financial Institution reportedly increased spending on AML technology and processes by 900 percent, including hiring ten times as many staff dedicated to BSA/AML monitoring.<sup>31</sup> While such measures may not be necessary for Financial Institutions with BSA/AML compliant programs, Financial Institutions should expect to continue to fund and expand compliance capability where necessary and appropriate to do so. 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. At a minimum, employing an experienced and knowledgeable BSA officer and support staff, as appropriate,

is critical. In addition to maintaining updated IT software and programs, management and the board of directors of a Financial Institution should ensure adequately trained staffing to monitor and supervise these processes and programs. Examiners may 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 have designed a BSA/AML compliance program that addresses such risks. For example, a Financial Institution with a large foreign correspondent banking practice or a significant prepaid card presence should address risks particular to those lines of business in its BSA/AML programs, policies, and procedures. Depending on the business profile of the Financial Institution, this may also include customer-focused risk management activities. For example, a Financial Institution with an active customer base among local immigrants may have increased risks relating to remittance transfers and other outbound transactions.
- **Effective Detection and Reporting.** To ensure Financial Institutions are able to capture and report potentially illicit financial activity, 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 particular size and BSA/AML risk profile, senior management should ensure that a Financial Institution's BSA and SAR policies are clear, precise and leave limited discretion to lower-level employees, to promote consistent and timely filing. As noted in the FFIEC BSA/AML Examination Manual, where a Financial Institution "has an established SAR decision-making process, has followed existing policies, procedures and processes, and has determined not to file a SAR," the Financial Institution should not be criticized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith.<sup>32</sup> Additionally, a Financial Institution must ensure that SAR decisions are thoroughly documented and include the specific reason for filing or not filing a SAR.
- **Targeted Training.** In addition to general BSA/AML training provided to all employees, Financial Institutions should consider additional training targeted at certain business units. For example, given the emphasis in the Advisory on effective information sharing, specialized training could be provided to legal or security staff about what types of information developed or possessed by those departments would be relevant for BSA/AML compliance. Financial Institutions may also consider updating annual BSA/AML training to provide all employees with an understanding of how BSA reports are used to develop critical information to further law enforcement and national security interests.
- **Small 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, smaller Financial Institutions 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.

◇ ◇ ◇

# STAY CURRENT

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](mailto:toddbeauchamp@paulhastings.com)

Chris Daniel  
1.404.815.2217  
[chrisdaniel@paulhastings.com](mailto:chrisdaniel@paulhastings.com)

Heena A. Ali  
1.404.815.2393  
[heenaali@paulhastings.com](mailto:heenaali@paulhastings.com)

Erica Berg Brennan  
1.404.815.2294  
[ericaberg@paulhastings.com](mailto:ericaberg@paulhastings.com)

Kevin P. Erwin  
1.404.815.2312  
[kevinerwin@paulhastings.com](mailto:kevinerwin@paulhastings.com)

Meagan E. Griffin  
1.404.815.2240  
[meagangriffin@paulhastings.com](mailto:meagangriffin@paulhastings.com)

Diane M. Pettit  
1.404.815.2326  
[dianepettit@paulhastings.com](mailto:dianepettit@paulhastings.com)

## Palo Alto

Cathy S. Beyda  
1.650.320.1824  
[cathybeyda@paulhastings.com](mailto:cathybeyda@paulhastings.com)

## San Francisco

Thomas P. Brown  
1.415.856.7248  
[tombrown@paulhastings.com](mailto:tombrown@paulhastings.com)

Stanton R. Koppel  
1.415.856.7284  
[stankoppel@paulhastings.com](mailto:stankoppel@paulhastings.com)

Paul M. Schwartz  
1.415.856.7090  
[paulschwartz@paulhastings.com](mailto:paulschwartz@paulhastings.com)

## Washington, D.C.

V. Gerard Comizio  
1.202.551.1272  
[vgerardcomizio@paulhastings.com](mailto:vgerardcomizio@paulhastings.com)

Behnam Dayanim  
1.202.551.1737  
[bdayanim@paulhastings.com](mailto:bdayanim@paulhastings.com)

Lawrence D. Kaplan  
1.202.551.1829  
[lawrencekaplan@paulhastings.com](mailto:lawrencekaplan@paulhastings.com)

Laura Bain  
1.202.551.1828  
[laurabain@paulhastings.com](mailto:laurabain@paulhastings.com)

Ryan A. Chiachiere  
1.202.551.1767  
[ryanchiachiere@paulhastings.com](mailto:ryanchiachiere@paulhastings.com)

Katie A. Croghan  
1.202.551.1849  
[katiecroghan@paulhastings.com](mailto:katiecroghan@paulhastings.com)

Michael A. Hertzberg  
1.202.551.1797  
[michaelhertzberg@paulhastings.com](mailto:michaelhertzberg@paulhastings.com)

Amanda Kowalski  
1.202.551.1976  
[manadakowalski@paulhastings.com](mailto:manadakowalski@paulhastings.com)

<sup>1</sup> 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; 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).

<sup>2</sup> 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](http://fincen.gov/statutes_regs/guidance/pdf/FIN-2014-A007.pdf).

<sup>3</sup> *Id.* at 1.

<sup>4</sup> The relevant federal banking agencies are the Office of the Comptroller of the Currency (“OCC”), Board of Governors of the Federal Reserve System (“FRB”) and the Federal Deposit Insurance Corporation (“FDIC”).

<sup>5</sup> FinCEN and FBA regulations require a financial institution to have a written, board approved program that is reasonably designed to assure and monitor compliance with the BSA. The program must, at a minimum: (i) provide for a system of internal controls to assure ongoing compliance; (ii) provide for independent testing for compliance; (iii) designate an individual or individuals who have responsibility for overseeing or conducting compliance testing; and (iv) provide for appropriate training and monitoring of compliance. This publication is published solely for the interests of friends and clients of Paul Hastings LLP and should not be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership. Copyright © 2014 Paul Hastings LLP.

personnel. See, e.g., 12 C.F.R. §21.21(d)(3) (OCC); 12 C.F.R. §208.63(c)(3)(FRB); 12 C.F.R. §326.8(c)(3)(FDIC); 31 C.F.R. §1022(d)(3) (OCC); 31 C.F.R. § 1022.210 (MSBs); 31 C.F.R. § 1023.210 (Brokers-Dealers); 31 C.F.R. § 1024.210 (Mutual Funds); 31 C.F.R. § 1025.210 (Insurance Companies); 31 C.F.R. § 1026.210 (Commodities Brokers); 31 C.F.R. § 1028.210 (Operators of Credit Card Systems); 31 C.F.R. § 1029.210 (Loan or Finance Companies).

<sup>6</sup> Advisory at 2.

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

<sup>9</sup> See Comptroller of the Currency Thomas J. Curry, Remarks before the Institute of International Bankers (Mar. 7, 2013) (“Curry March 4 Speech”); see also Testimony of Comptroller of the Currency Thomas J. Curry before the Senate Committee on Banking, Housing and Urban Affairs (Mar. 7, 2013) (“Curry March 7 Testimony”).

<sup>10</sup> Advisory at 2.

<sup>11</sup> *Id.*

<sup>12</sup> *Id.* at 3.

<sup>13</sup> *Id.*

<sup>14</sup> See Footnote 5; Advisory at 3-4.

<sup>15</sup> *Id.* at 4.

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

<sup>18</sup> 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>.

<sup>19</sup> See OCC EA 2014-094, AA-EC-2014-60 (June 26, 2014), available at <http://www.occ.gov/static/enforcement-actions/ea2014-094.pdf>.

<sup>20</sup> See OCC EA 2014-006, AA-EC-2013-11 (January 14, 2014), available at <http://www.occ.gov/static/enforcement-actions/ea2014-006.pdf>.

<sup>21</sup> See FinCEN Matter No. 2014-1 (January 7, 2014), available at [http://www.fincen.gov/news\\_room/ea/files/JPMorgan\\_ASSESSMENT\\_01072014.pdf](http://www.fincen.gov/news_room/ea/files/JPMorgan_ASSESSMENT_01072014.pdf).

<sup>22</sup> See FinCEN Matter No. 2013-02 (September 24, 2013), available at [http://www.fincen.gov/pdf/SRVB\\_Assessment\\_092413.pdf](http://www.fincen.gov/pdf/SRVB_Assessment_092413.pdf).

<sup>23</sup> See OCC EA 2012-261, AA-EC-2012-140 (Dep’t of Treasury, Dec. 4, 2012), available at <http://www.occ.gov/static/enforcement-actions/ea2012-261.pdf>; and FRB Docket Nos. 12-062-CMP-FB, 12-062-CMP-HC, and 12-062-B-FB, 2-4 (December 11, 2012), available at <http://www.federalreserve.gov/newsevents/press/enforcement/enf20121211a2.pdf>.

<sup>24</sup> See Press Release, U.S. Treasury Department (December 11, 2012), available at <http://www.treasury.gov/press-center/press-releases/Pages/tg1799.aspx>.

<sup>25</sup> 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>.

<sup>26</sup> See *Bankers to Be Held Personally Responsible for Sanctions Violation: Treasury*, Reuters (March 22, 2013), citing to Treasury Department spokesman John Sullivan stating:

Although sanctions enforcement cases involving financial institutions have typically concluded with civil penalties at the corporate level, individuals can and do face liability ... when they are personally responsible for sanctions violations, and Treasury’s Office of Foreign Assets Control will take appropriate enforcement action in these circumstances.

<sup>27</sup> The FINRA action is available at: <http://www.finra.org/web/groups/industry/@ip/@enf/@ad/documents/industry/p443448.pdf>.

---

<sup>28</sup> Thomas J. Curry, *Remarks before the Association of Certified Anti-Money Laundering Specialists* (March 17, 2014), transcript available at: <http://www.occ.gov/news-issuances/speeches/2014/pub-speech-2014-39.pdf>.

<sup>29</sup> See note 25, *supra*.

<sup>30</sup> See Andrew R. Johnson and Ben Fox Rubin, *M&T Merger With Hudson City Faces Further Delay*, *Wall St. J.*, Dec. 17, 2013, available at <http://online.wsj.com/news/articles/SB10001424052702303949504579263991250784538>.

<sup>31</sup> John Adams, "Why HSBC's Money Laundering Settlement Could Benefit IT," *American Banker* (Dec. 14, 2012).

<sup>32</sup> FFIEC BSA/AML Examination Manual, pgs. 75-76 (2010).