BSA/AML COMPLIANCE AN

BY DANIEL P. STIPANO, ELLEN M. WARWICK, BRENDAN M. CLEGG, AND BENJAMIN W. HUTTEN

AFTER NINE MONTHS IN OFFICE, it seems unlikely that the administration's efforts to change the existing financial industry regulatory regime will affect enforcement of the Bank Secrecy Act (BSA) and its implementing regulations. To the contrary—it appears that law enforcement and national security will be top priorities for this administration. Because the BSA regulatory regime is designed to combat financial crime, money laundering and, most notably in the post-9/11 world, terrorism, banking institutions and their regulators will continue to focus on compliance. The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency, known as the federal banking agencies (FBAs), will continue to scrutinize institutional compliance with both the existing regulatory requirements, as well as newer initiatives such as the Financial Crimes Enforcement Network's (FinCEN) customer due diligence (CDD) rule (www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf). Although leadership vacancies continue at several agencies key to setting policy and enforcing the BSA (including FinCEN and the FBAs), it seems likely that BSA enforcement will remain a top priority even after permanent officials are in place and their policy preferences are established.

SHUTTERSTOCK

D ENFORCEMENT

Trends and Issues in an Uncertain Time

Overview

Various regulatory and law enforcement agencies are responsible for enforcing compliance with the BSA. The FBAs pursue enforcement through an array of formal and informal actions. When a bank fails to establish and maintain an adequate Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance program, or fails to correct a previously reported problem with its program, the FBAs are statutorily mandated to issue a cease-and-desist order (C&D) against the bank pursuant to 12 U.S.C. § 1818(s) (www.gpo.gov/fdsys/pkg/USCODE-2010-title12/pdf/USCODE-2010-title12-chap16-sec1818.pdf). Civil money penalties (CMPs) for significant BSA violations can also be assessed by the FBAs. (See 12 U.S.C. § 1818(i)(2): www.gpo.gov/fdsys/pkg/USCODE-2010-title12/pdf/USCODE-2010-title12-chap16-sec1818.pdf.) Institutions willfully violating the requirement to establish and maintain an adequate BSA/AML compliance program, or to file Suspicious Activity Reports (SARs), also face prosecution by the Department of Justice (DOJ) and the imposition of criminal sanctions. (See 31 U.S.C. § 5322: https://www.gpo.gov/fdsys/pkg/USCODE-2011-title31/pdf/USCODE-2011-title31-subtitleIV-chap53-subchapII-sec5322.pdf.) Similarly, individuals are subject to enforcement actions for noncompliance with BSA/AML requirements, ranging from removal from their position and imposition of CMPs by regulators, to potential criminal liability for willful violations, including fines and imprisonment. (See, e.g., 12 U.S.C. §§ 1818(e), (i)(2); 31 U.S.C. § 5322: https://www.gpo.gov/fdsys/pkg/USCODE-2010-title12/pdf/USCODE-2010-title12-chap16-sec1818.pdfhttps:/www.gpo.gov/fdsys/pkg/USCODE-2010-title12/pdf/USCODE-2010-title12-chap16-sec1818.pdf).

Financial regulators and law enforcement will rigorously continue to ensure compliance with the BSA/AML regime to combat criminal activity, money laundering and terrorist financing, all of which are top priorities for this administration.

Enforcement

Enforcement Actions Against Institutions

While the number of BSA-related enforcement actions taken by the FBAs against banks has declined over the last few years, this does not reflect that the FBAs are any less vigilant. Currently, virtually all large banks are under enforcement actions for BSA violations. Some are also under deferred prosecution agreements and have paid substantial penalties. Additionally, numerous midsize and community banks, as well as foreign branches operating in the U.S., are subject to enforcement actions based on BSA violations. When bank examiners identify new concerns and an institution is already subject to an enforcement action, the FBAs typically address these problems by amending the action plan already in place rather than taking a new action. This practice may reduce the number of new actions taken, at least with respect to large institutions; however, the reality is that regulators are continuing to require corrective action when new problems are identified.

Corrective action is also encouraged and achieved through the ongoing supervisory process. Bank examiners regularly examine banks for compliance with the BSA, and will continue to do so, including compliance with the new CDD rule—the so-called "fifth pillar" of a BSA/AML compliance program. (See Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29398 (May 11, 2016): www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf.) Examiner concerns regarding an aspect of an institution's BSA/AML compliance program or an isolated technical violation of law, are usually addressed through the supervisory process when management demonstrates the capability and willingness to take appropriate corrective action. Supervisory Matters Requiring Attention (MRAs)—which are nonpublic—will continue to be used in the supervisory process to hold banks accountable for correcting deficiencies that are not severe enough to require enforcement action. However, when an institution is experiencing serious or systemic breakdowns in its compliance program, or is engaging in an egregious pattern of failing to file SARs, the FBAs will continue to pursue enforcement action, including the assessment of significant CMPs. (See generally, Interagency Statement on Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements (July 19, 2007): www.federalreserve.gov/newsevents/pressreleases/bcreg20070719a.htm.) Institutions willfully violating the BSA may also face significant criminal penalties from the DOJ, which has remained active in the BSA/AML space after the change in administration. (See Press Release, Department of Justice, Office of Public Affairs, Banamex USA Agrees to Forfeit $97 Million in Connection with Bank Secrecy Act Violations (May 22, 2017): www.justice.gov/opa/pr/banamex-usa-agrees-forfeit-97-million-connection-bank-secrecy-act-violations.)

Enforcement Action Against Individuals

In cases of severe misconduct, the FBAs will continue to hold managers and directors accountable for serious compliance breakdowns, and take enforcement actions against these senior officials, rather than lower level employees. The DOJ has made safeguarding national security and restoration of law and order top priorities. It is, therefore, expected that DOJ will continue to hold individuals accountable, including compliance professionals who engage in willful violations of the law. In April 2017, DOJ confirmed that its September 2015 memorandum entitled Individual Accountability for Corporate Wrongdoing remained in effect as Department policy. (See Kate Berry, Trump's DOJ Takes Same Hard Line as Obama's in Wells Probe, Am. Banker (Apr. 10, 2017): www.americanbanker.com/news/wells-probe-trumps-doj-takes-same-hard-line-as-obamas.) Commonly referred to as the Yates Memo, this memorandum put the banking industry on

notice that individuals would not escape civil or criminal liability for their role in corporate misconduct.

In May of this year, FinCEN's Acting Director, in announcing a settlement of charges against the former Chief Compliance Officer of MoneyGram International, Inc., highlighted the need for individual enforcement actions to strengthen the compliance profession and protect compliance professionals' unique positions of trust. (*See* Press Release, *FinCEN, FinCEN and Manhattan U.S. Attorney Announce Settlement with Former MoneyGram Executive Thomas E. Haider* (May 4, 2017): https://www.fincen.gov/news/news-releases/fincen-and-manhattan-us-attorney-announce-settlement-former-moneygram-executive). More recently, however, the DOJ's Deputy Attorney General suggested that some aspects of the Yates Memo could soon be changed. (*See* Josh Gerstein, *Rosenstein Signals Changes Coming on Corporate-Crime Prosecution Policy*, Politico (Sept. 14, 2017): http://www.politico.com/blogs/under-the-radar/2017/09/14/corporate-crimes-prosecutions-rod-rosenstein-242721). Even though he indicated some changes may be coming, the Deputy Attorney General stated that he still favored prosecutions of individuals in "appropriate cases." Therefore, individuals will still likely remain under scrutiny depending on the nature of the case.

ISTOCK/ BAONA

Enforcement at the State Level

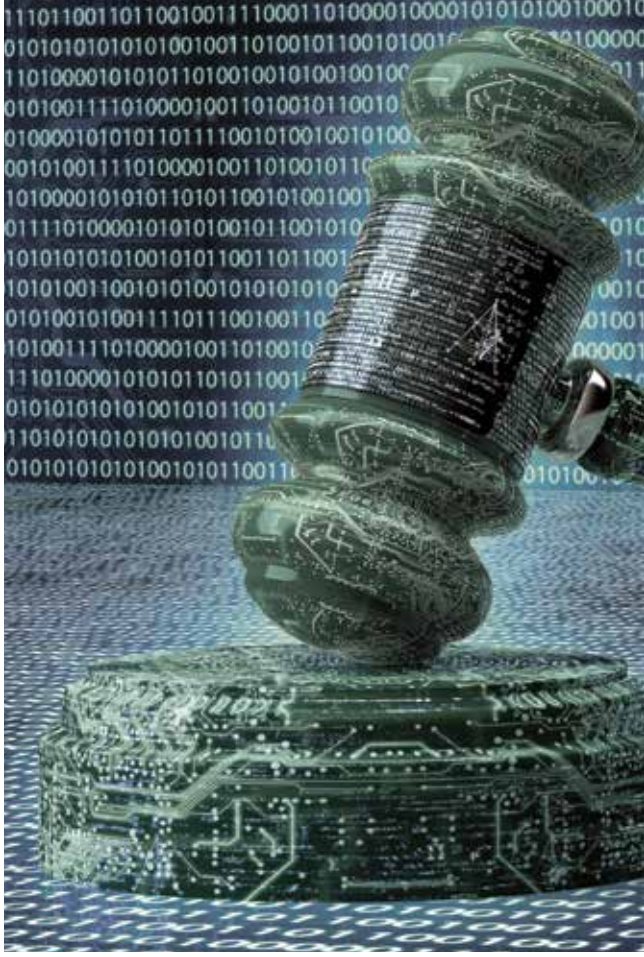
State banking supervisors, in addition to their federal counterparts, vigorously continue to enforce the BSA by requiring remedial action and assessing large fines when banks fail to comply with BSA/AML obligations. For example, in January 2017, the New York Department of Financial Services (NYDFS) and Deutsche Bank agreed to a consent order to address serious compliance deficiencies with the bank's BSA/AML program and a fine of $425 million. (*In re* Deutsche Bank AG, New York State Department of Financial Services, Consent Order Under New York Banking Law §§ 39, 44 and 44-a (Jan. 30, 2017): www.dfs.ny.gov/about/ea/ea170130.pdf.) More recently, NYDFS fined Habib Bank and its New York branch $225 million for failure to comply with state laws and regulations designed to combat money laundering and terrorist financing, and Habib Bank surrendered its license to operate its New York branch. (*In re* Habib Bank Limited, New York State Department of Financial Services, Consent Order Under New York Banking Law §§ 39, 44 and 605 (Sept. 7, 2017): http://www.dfs.ny.gov/about/ea/ea170907.pdf.)

In addition, in 2016, NYDFS issued Rule 504 entitled Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications. It required regulated institutions to implement and maintain a transaction monitoring program and a filtering program designed to prevent, detect, and report BSA/AML and OFAC violations. Beginning in April 2018, New York state-regulated institutions must adopt either an annual board resolution or senior compliance officer finding to certify compliance with this rule, which could expose the Board and compliance professionals to personal liability. Therefore, NYDFS may use the Rule 504 certification requirement as a basis for taking enforcement actions in the near future for individual misconduct. Banks must remain cognizant that state banking supervisors, independent of the FBAs, will continue to ensure institutions and their officers and directors comply with the BSA/AML regulatory regime, as well as additional related requirements adopted under state law.

The Broader BSA/AML Landscape

Regulatory Expansion

Given the current administration's focus on protecting national security and fighting terrorism, institutional compliance with the BSA/AML framework is likely to continue to be a priority. U.S. Department of the Treasury Secretary Mnuchin, in an April statement to the International Monetary and Financial Committee Meeting, affirmed that "[t]argeting and dismantling the financial networks of terrorist organizations is a top U.S. priority, and improving anti-money laundering and counter terrorist financing systems is critical to this goal. (See Steven Mnuchin, Statement of Secretary Mnuchin for the International Monetary and Financial Committee Meeting (Apr. 21, 2017): www.treasury.gov/press-center/press-releases/Pages/sm0054.aspx.) In the U.S. House of Representatives, the increased focus on money laundering and terrorist financing is evidenced by the formation of a new antiterrorism subcommittee—the House Subcommittee on Terrorism and Illicit Finance—within the House Financial Services Committee.



In June, Congress began to engage the legislative machinery to rollback certain Dodd-Frank regulations with the passage of the House relief bill, the Financial Choice Act. (See Financial Choice Act, H.R. 10, 115th Cong. (2017): https://financialservices.house.gov/uploadedfiles/hr_10_the_financial_choice_act.pdf.)

The Department of the Treasury (Treasury) also issued its comprehensive recommendations for financial regulatory reform on June 12, 2017.[1] However, neither Congress nor the Treasury have targeted the May 2018 implementation of the CDD rule, or more generally the BSA/AML regime, as opportunities to provide banks with relief from regulatory burden.

FinCEN's new CDD rule will add a "fifth pillar" to banks' BSA/AML compliance programs that will be the subject of scrutiny by FinCEN and the FBAs. (See 31 C.F.R. § 1020.210(b)(5): www.gpo.gov/fdsys/pkg/CFR-2016-title31-vol3/xml/CFR-2016-title31-vol3-sec1020-210.xml.) The looming compliance date for FinCEN's CDD rule, in May 2018, will bring significant change to the industry by requiring risk-based procedures for conducting due diligence on all customers, including the new categorical requirement to verify the identity of beneficial owners of legal entities.[2]

While the number of BSA-related enforcement actions taken by the FBAs against banks has declined over the last few years, this does not reflect that the FBAs are any less vigilant.

On June 28, 2017, twin bills were introduced in the U.S. House of Representatives and U.S. Senate that would complement the beneficial ownership provisions of FinCEN's CDD rule. The proposed legislation would require non-exempted corporations and limited liability companies formed in the United States to disclose their beneficial owners. (*See* H.R. 3089, 115th Cong. (2017): www.congress.gov/bill/115th-congress/house-bill/3089/text, and S. 1454, 115th Cong. (2017): www.congress.gov/bill/115th-congress/senate-bill/1454/text.) Generally, the proposed legislation directs the Treasury Department to issue regulations by 2019, requiring companies formed in states that do not already require basic disclosures, to submit information about their beneficial owners. The bills would also include a requirement to update changed beneficial ownership information and to submit an annual report of beneficial owners. If passed, this legislation would reduce the ability to incorporate non-transparent shell companies in the United States and provide a source of beneficial ownership information to law enforcement in addition to that collected pursuant to the CDD rule. Although similar measures have failed repeatedly in the past due to strident opposition from certain states, Treasury Secretary Mnuchin, as well as bipartisan groups within Congress, have signaled support of government collection of beneficial ownership information.[3]

Combatting cybercrime will also continue to emerge as an important priority for this administration. As cybercriminals proceed to target financial institutions, the BSA/AML regime and cybersecurity will also continue to intersect given the ever-increasing number of cyberattacks and intrusions. Both the Federal Financial Institutions Examination Council (FFIEC) and FinCEN have recently issued guidance on SAR reporting of cyber-events and cyber-crime.[4] FinCEN's cyber-crime advisory reminds banks of their obligation to report cyber-events when "a financial institution knows, suspects, or has reason to suspect that a cyber-event was intended, in whole or in part, to conduct, facilitate, or affect a transaction or a series of transactions." The FBAs also impose cyber-related SAR-filing obligations on the banks they supervise that require those institutions to report unauthorized electronic intrusions or certain computer-related crimes.

In making the decision to file a SAR to report a cyber-event, banks will need to evaluate the nature of the cyber-event as well as the information and systems targeted and determine the monetary amounts involved in the transactions or attempted transactions. The determination of whether the attack was intended to affect, or could have affected any transaction, will be a judgment call based on the circumstances of the cyber-event. It is also a determination that could be second-guessed by regulators. Satisfying the cyber-event reporting requirements will require much greater coordination between BSA/AML compliance and cybersecurity personnel to ensure accurate and complete SAR reporting. Going forward, it will be important for banks to monitor the FBAs' expectations for integrating cyber-event reporting into existing BSA/AML programs.

Finally, FinCEN has proposed the imposition of "special measures" under Section 311 of the BSA resulting from North Korea's

ISTOCK/ BAONA

Regulatory technology, known as regtech, represents another new change for the industry: this rapidly-evolving technology is designed to assist institutions with their compliance obligations by streamlining, updating, and enhancing their monitoring and reporting capabilities.

escalation of nuclear activities. On June 29, 2017, FinCEN issued a notice of proposed rulemaking intended to sever a small Chinese bank's access to the U.S. financial system, based on a finding that the bank was used as a conduit for North Korea to access the U.S. financial system. The bank facilitated millions of dollars of transactions for companies involved in North Korea's weapons of mass destruction and ballistic missile programs (www.fincen.gov/sites/default/files/federal_register_notices/2017-06-29/NPRM_311Dandong_0.pdf). If finalized, the proposed rule would prohibit covered financial institutions from opening or maintaining a correspondent account in the United States for, or on behalf of, Bank of Dandong. It would also require covered financial institutions to take measures to guard against other foreign correspondent accounts being used to process transactions for Bank of Dandong. As a practical matter, with the issuance of the proposed rule, many U.S. institutions may choose not to conduct business with the Chinese bank based on their assessment of risk even before the proposed rule is finalized, effectively cutting Bank of Dandong off from most transactions in the United States and in U.S. dollars around the world.

Industry Reactions and Changes: De-Risking

The industry trend of de-risking customer accounts is not likely to abate anytime soon. In recent years, the increased scrutiny applied by financial regulators—and resultant public enforcement actions and fines—has caused banks to terminate certain accounts, clients, relationships, or in some cases, industries. In doing so, banks avoid both the risk posed by continuing to bank such entities, and the costs of managing that risk. While it is difficult to predict the approach that the FBAs will take toward loss of access to the banking system by various higher risk customers, financial institutions, particularly large banks, will continue to make strategic decisions regarding whether they should terminate or keep potentially risky accounts. Without a significant reduction in the cost of BSA compliance—and the consequences of getting it wrong—banks are likely to continue to de-risk customers. When large banks de-risk accounts, those customers often end up at smaller institutions which lack the compliance capabilities to monitor those customers adequately. This transition of customers could expose smaller institutions to significant BSA/AML compliance problems because they lack the resources and expertise to manage the risks presented by higher-risk customers. This domino effect could result in increased regulatory scrutiny for these smaller institutions, and exposure to BSA/AML risk.

Industry Reactions and Changes: FinTech

Financial technology companies—so-called FinTechs—provide financial services to customers through the use of technology, such as through innovative payment systems. During the past year, the Office of the Comptroller of the Currency (OCC) announced plans to issue special purpose banking charters to FinTech companies. As set out in the OCC's December 2016 white paper, and reiterated in public comments by the former Comptroller of the Currency and the Acting Comptroller, FinTech companies will, in general, be subject to the same laws, regulations, examination, reporting requirements, and ongoing supervision as other national banks (www.occ.gov/news-issuances/speeches/2017/pub-speech-2017-82.pdf and www.occ.gov/topics/responsible-innovation/comments/special-purpose-national-bank-charters-for-fintech.pdf). This includes the BSA/AML and the OFAC sanctions regimes. It will be challenging and costly for FinTechs to meet BSA/AML reporting and compliance requirements in a regulated environment, but they will need to invest the resources necessary to implement a reasonably designed BSA/AML program that withstands regulatory scrutiny. The consequences of a significant compliance breakdown could affect both a FinTech's reputation and financial soundness. The next Comptroller could have a major impact on the future of FinTech, as it is not clear that he or she will place the same level of priority on chartering FinTechs as the former Comptroller. In addition, the filing of lawsuits by state banking regulators against the OCC to prevent the expansion of FinTech charters could legally or politically derail the efforts to expand the special purpose charter.

Industry Reactions and Changes: Regtech

Regulatory technology, known as regtech, represents another new change for the industry: this rapidly-evolving technology is designed to assist institutions with their compliance obligations by streamlining, updating, and enhancing their monitoring and reporting capabilities. Regtech is coming, but it will not disrupt or replace conventional software technologies utilized by banks to assist them in fulfilling BSA/AML compliance obligations in the near term. Regtech can leverage technology to better understand and manage risks and ultimately reduce the costs of compliance. Machine learning and other artificial intelligence-based monitoring tools may provide financial institutions with better and more efficient solutions for achieving compliance with the BSA. But regtech will not replace conventional monitoring and control systems employed by financial institutions in BSA/AML compliance programs in the immediate future. Instead, regtech will gain importance over time because it presents an opportunity for institutions to replace aging technology with newer, more cost-effective technologies.

Although the larger financial regulatory landscape may significantly change under this administration, all signs indicate that enforcement of the BSA/AML regulatory regime will continue in much the same way it has over the last several decades.

Financial regulators, including the FBAs, may be slow to accept regtech until they become comfortable with how the technology works and its ability to sufficiently meet the objectives of the BSA/AML regime. At an institutional level, when an institution begins to move in the direction of incorporating regtech into its BSA/AML compliance program (to better identify, measure, monitor, and manage associated risks), examiners will expect an institution to maintain its current monitoring systems and controls until it can validate that the newer technology is effective and sustainable. Therefore, although regtech will have a significant impact on improving BSA/AML compliance as the technology evolves, the major effects will likely not be felt in the immediate future, as supervisory acceptance will be measured.

Conclusion

Financial regulators and law enforcement will rigorously continue to ensure compliance with the BSA/AML regime to combat criminal activity, money laundering, and terrorist financing—all of which are top priorities for this administration. Consequently, the burden and cost associated with ensuring compliance will continue to rise. And when banks fail to meet their compliance obligations, there will be supervisory and enforcement consequences for these institutions. Although the larger financial regulatory landscape may significantly change under this administration, all signs indicate that enforcement of the BSA/AML regulatory regime will continue in much the same way it has over the last several decades. ■

ABOUT THE AUTHORS

DANIEL P. STIPANO is a partner at Buckley Sandler, LLP., in Washington, D.C. He advises on bank regulatory and compliance issues, represents clients in banking enforcement actions, and provides assistance in regard to BSA/AML compliance programs. Prior to joining the firm, he was the Deputy Chief Counsel for the Office of the Comptroller of the Currency. He can be reached at **dstipano@buckleysandler.com**.

ELLEN M. WARWICK is senior counsel at the firm in Washington, D.C. She advises on all aspects of bank regulatory and compliance issues, represents clients in banking enforcement actions including investigations, and provides assistance in establishing and maintaining BSA/AML compliance programs. Prior to joining the firm, she was the Director of Enforcement and Compliance for the OCC. She can be reached at **ewarwick@buckleysandler.com**.

BRENDAN M. CLEGG is an associate at the firm in Washington, D.C. He provides counsel on regulatory and enforcement matters, with a focus on BSA/AML. He can be reached at **bclegg@buckleysandler.com**.

BENJAMIN W. HUTTEN is an associate at the firm in New York City. He provides regulatory and compliance counsel, with a focus on AML and financial sanctions. He can be reached at **bhutten@buckleysandler.com**.

ENDNOTES:

[1] U.S. Department of the Treasury, A Financial System That Creates Economic Opportunities: Banks and Credit Unions (June 2017), *available at* https://www.treasury.gov/press-center/press-releases/Documents/A%20Financial%20System.pdf.

[2] For an overview of the CDD rule, see Daniel P. Stipano, Ellen M. Warwick & Benjamin W. Hutten, *FinCEN's Customer Due Diligence and Beneficial Ownership Rule*, The Review of Banking & Financial Services (Aug. 17, 2017), *available at* https://buckleysandler.com/sites/default/files/Buckley-Sandler-Article-FINCEN-Customer-Due-Diligence-and-Beneficial-Ownership%20Rule.pdf.

[3] *See* Senate Finance Committee, Hearing on the Nomination of Steve Mnuchin to be Secretary of the Treasury (Jan. 30, 2017).

[4] *See* Federal Financial Institutions Examination Council, Joint Statement: Cyber Attacks Involving Extortion (Nov. 3, 2015), *available at* https://www.ffiec.gov/press/PDF/FFIEC%20Joint%20Statement%20Cyber%20Attacks%20Involving%20Extortion.pdf; Financial Crimes Enforcement Network, *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime*, FIN-2016-A005 (Oct. 25, 2016), *available at* https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf.