By Jonathan B. New and Patrick T. Campbell

As we saw in Part One in last month’s newsletter (see, http://bit.ly/2DykAQ0), regulators have recently shown a tendency to focus on compliance officers who they deem to have failed to ensure that the compliance and anti-money laundering (AML) programs that they oversee adequately prevented corporate wrongdoing, and there are several indications that regulators will continue to target compliance officers in 2018 in actions focused on Bank Secrecy Act (BSA)/AML compliance.

Regulators’ Scrutiny of Compliance Officers in 2018

Regulators will likely continue to focus on individuals and corporate compliance programs this year. How do we know? For one, the Department of Justice (DOJ) “Yates Memo,” issued in September 2015 by then-Deputy Attorney General Sally Yates, which requires companies to provide all facts relevant to employee misconduct in order to receive cooperation credit, is still in effect. Despite the recent change in DOJ leadership, Attorney General Jeff Sessions and Deputy Attorney General Rod Rosenstein have each indicated that they will continue to prioritize individual accountability for corporate malfeasance. See, Jeff Sessions, Attorney General, DOJ, Remarks at Ethics and Compliance Initiative Annual Conference (Apr. 24, 2017) (http://bit.ly/2pef3Iz) (“The Department of Justice will continue to emphasize the importance of holding individuals accountable for corporate misconduct. It is not merely companies, but specific individuals, who break the law.”); Rod Rosenstein, Deputy Attorney General, DOJ, Remarks at the 34th International Conference on the Foreign Corrupt Practices Act (Nov. 29, 2017) (http://bit.ly/2Aedkuu) (“Effective deterrence of corporate corruption requires prosecution of culpable individuals. We should not just announce large corporate fines and celebrate penalizing shareholders.”). In addition, Securities and Exchange Commission (SEC) Chairman Jay Clayton stated during his confirmation hearing in 2017 that “individual accountability has a greater deterrent effect across the system than corporate accountability.” Nomination of Jay Clayton: Hearing Before the S. Comm. on Banking, Housing and Urban Affairs, 115th Cong. 99 (2017) (Responses to Written Questions of Sen. Reed from Jay Clayton) (http://bit.ly/2DxnvwV). The SEC’s 2017 Annual Report buttressed Chairman Clayton’s statement by including a “focus on individual accountability” as one of the five core principles that will guide SEC enforcement decision-making in 2018. SEC, Fiscal Year 2017 Agency Financial Report (2017) (http://bit.ly/2DFvOGa).

Also, various new policies and rules issued by federal and state regulators place increased BSA/AML responsibilities on compliance officers in 2018 and may add to their personal criminal and regulatory liability risk. On Nov. 29, 2017, Rosenstein expanded upon the DOJ's long-running efforts to encourage companies to self-disclose Foreign Corrupt Practices Act (FCPA) violations by announcing a revised FCPA Corporate Enforcement Policy. United States Attorneys’ Manual, FCPA Corporate Enforcement Policy, Section 9-47.120 (2017) (http://bit.ly/2nDIjuT). The revised FCPA Corporate Enforcement Policy seeks to further encourage self-disclosure of FCPA violations by providing,

Jonathan B. New and Patrick T. Campbell are both partners in the New York office of BakerHostetler’s White Collar, Investigations and Securities Enforcement and Litigation Team. Mr. New is also a member of the Board of Editors of this newsletter. The views expressed in this article are those of the authors and not necessarily those of BakerHostetler or its clients.
among other things, a presumption that the company will receive a declination if it voluntarily self-discloses misconduct, fully cooperates, and timely and appropriately remediates, as long as other requirements of the policy are met. Id. If the company does not make a timely self-disclosure, the maximum benefit the company may receive from the DOJ will be capped to a 25% reduction off the low end of the United States' Sentencing Guidelines range. Id. The DOJ’s revised FCPA Corporate Enforcement Policy will likely encourage companies to make earlier and more robust self-disclosures, which could place more information in the hands of regulators that they in turn can use to scrutinize compliance officers.

Compliance officers will face increased BSA/AML obligations under the Financial Crimes Enforcement Network’s (FinCEN’s) May 11, 2016, Customer Due Diligence (CDD) rules, with which covered financial institutions must be in compliance by May 11, 2018. Customer Due Diligence Requirements for Financial Institutions; Final Rule, 81 Fed. Reg. 29,398 (May 11, 2016) (codified at 31 C.F.R. pts. 1010, 1020, 1023, et al.). The CDD rules introduce a new requirement to FinCEN’s existing AML program requirements — the obligation to identify and verify the beneficial owners of certain legal entity customers at the time a new account is opened. See, 31 C.F.R. §1010.230(a)-(b). The CDD rules also codify two other elements of AML program requirements that are already implicitly mandated by FinCEN’s existing rules: “Understanding the nature and purpose of customer relationships to develop a customer risk profile” and “ongoing monitoring to identify and report suspicious transactions and, on a risk-basis, to maintain and update customer information.” See, e.g., 31 C.F.R. §1020.210(b)(5) (AML program requirements for banks, savings associations, and credit unions). As shown in its action against Thomas E. Haider, discussed in Part One, FinCEN will seek monetary penalties and industry bars against compliance officers for failing to ensure the effectiveness of the AML compliance programs that they oversee, and these new rules add to the types of AML compliance program deficiencies for which compliance officers may be held personally liable.

Finally, the first annual certifications under the New York State Department of Financial Services’ (DFS) new Transaction Monitoring and Filtering Program Requirements and Certifications (Part 504) are due on April 15, 2018. N.Y. Comp. Codes R. & Regs tit. 3, §§504.1 et seq. (2018). The DFS promulgated Part 504 after identifying “shortcomings in the transaction monitoring and filtering programs of [regulated financial] institutions attributable to a lack of robust governance, oversight, and accountability at senior levels.” Id. at §504.1. The key substantive elements of Part 504 require financial institutions regulated by the DFS to maintain a transaction-monitoring program that is reasonably designed to monitor transactions after their execution for potential BSA/AML violations and suspicious activity reporting. This will include reviewing and periodically updating the program to take into account and reflect changes to applicable BSA/AML laws, regulations, and regulatory warnings. Id. at §504.3(a). Each covered financial institution must also maintain watch-list filtering programs that are reasonably designed to identify and stop transactions that are prohibited by federal economic and trade sanctions. Id. at §504.3(b).

However, perhaps the most notable piece of Part 504 — and where the DFS’s rules go even further than FinCEN’s CDD rules — is the requirement that the subject bank annually certify compliance with Part 504, either by “Board Resolution” or “Senior Officer(s) Compliance Finding.” Id. at §§504.4, 504.6. These board resolutions or senior officer compliance findings must include statements that the board or senior officer “reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary to” adopt the board resolution or make the senior officer compliance finding, and that the board or senior officer “has taken all steps necessary to confirm that [the financial institution] has a Transaction Monitoring and Filtering Program that complies with the provisions of Section 504.3.” Id. at §504.7, Attachment A.

Compliance officers will have increased responsibilities, and possibly new criminal and civil liability exposure, under the DFS’s new AML rules. Tellingly, the prior, proposed language of the rules required the financial institution’s “chief compliance officer or their functional equivalent” to make the annual certification, and expressly stated that the certifying officer may be subject to criminal penalties for an incorrect or false annual certification. Dept’t of Fin. Servs., Proposed Superintendent’s Regulations, Part 504, Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications. While the DFS omitted these provisions from the final rules after receiving extensive criticism from the financial industry, their initial inclusion illustrates the DFS’s expectations that institutional responsibility for AML compliance falls on the firm’s CCO. In addition, in practice, CCOs will likely be executing, or be among those executing, these certifications, as the final rules define “Senior Officer(s)” as “the senior individual or individuals responsible for the management, operations, compliance and/or risk of a Regulated Institution ….” N.Y. Comp. Codes R. & Regs tit. 3, §§504.2(g). Regardless of whether Part 504 specifically provides
for criminal liability for incorrect or false compliance certifications, compliance officers can be prosecuted for knowingly filing false certifications under New York State penal law. See, e.g., N.Y. Penal Law §§175.30, 175.35 (McKinney 2017).

Clearly, the Sarbanes-Oxley-like certification required by Part 504 is one way the DFS will seek to hold compliance officers accountable for implementing its new AML rules. However, it remains to be seen whether the DFS will seek to hold compliance officers civilly liable for failures of their firms’ compliance with Part 504. It is unclear whether the DFS has the authority to institute civil enforcement actions against individuals, but it would not be surprising to see the DFS try to flex its regulatory muscle and seek to discipline compliance officers personally for failure to comply with Part 504.

**Best Practices for Compliance Officers To Mitigate Personal Liability Exposure**

Given the continued emphasis of regulators on corporate compliance and AML programs and those who administer them, compliance officers should review and assess their firms’ compliance and AML programs and their own practices to put them in the best position to mitigate personal liability. Compliance officers should, among other things:

- **Know and understand all applicable laws and regulations pertaining to their roles and responsibilities.** Different regulatory regimes each have their own requirements and expectations on corporate compliance and AML programs, and firms could be subject to multiple regulatory regimes at the same time. Compliance officers should assess all rules, regulations, and regulator expectations applicable to the business of their firms and ensure that their companies’ compliance and AML programs, and their own conduct, conform to all applicable regulatory requirements and expectations.

- **Understand their obligations and institutional reporting lines.** Compliance officers should know their obligations and carry them out accordingly. Compliance officers also need to understand the responsibilities of the individuals who report to them and ensure that they have the appropriate amount of resources to carry out their jobs. Regulators, in particular the SEC, can seek to take action against compliance officers based on the failures of their subordinates, in particular if those failures are the result of a lack of resources sufficient to perform the compliance function.

- **Timely act on red flags brought to their attention.** Regulators may use a compliance officer’s failure to act on suspicious activity brought to his or her attention as the basis for personal liability.

- **Monitor their firms’ compliance and AML programs for continued effectiveness.** Compliance officers should implement robust compliance monitoring and testing procedures to ensure that their firms’ compliance and AML programs remain tailored to the particular risks and potential conflicts of interest facing their companies and industries. Compliance officers should also stay informed of applicable regulatory developments, such as the FinCEN CDD rules and DFS Part 504, and update their firms’ compliance and AML programs accordingly.

- **Regularly communicate to and train all employees on the firm’s compliance and AML program.** Regulators may use inadequate communication of and training on a company’s compliance and AML program as a basis for holding compliance officers personally responsible for the company’s compliance and AML failures. Compliance officers should also make resources available to employees who seek guidance on the program.

Carefully document compliance with BSA/AML laws and regulations. DFS Part 504 in particular requires financial institutions to document the identification of areas, systems, or processes that may require material improvement or redesign, and the firm’s remedial efforts to address such areas, systems, or processes. N.Y. Comp. Codes R. & Regs tit. 3, §§504.3(d). Establishing a paper trail of compliance that includes communications with other senior executives and compliance personnel, information sharing, and decisions and actions is critical to protecting compliance officers from personal liability.

**Conclusion**

Compliance officers serve as the first line of defense for law enforcement personnel and regulators in their efforts to detect and prevent money laundering, sanctions violations, and fraud. Unfortunately, they often become the first to be scrutinized when it comes to assessing and retrospectively assigning fault for alleged corporate wrongdoing. Regulators’ recent focus on individual accountability has further exacerbated this dichotomy and increasingly placed compliance officers in their crosshairs. Despite the business-friendly and anti-regulatory perspective of the new administration, this trend is likely to continue in the coming year. Companies and compliance officers should redouble their vigilance, keep abreast of new regulatory requirements, and regularly review the effectiveness of their AML compliance programs.