Wall Street LAWYER
Securities in the Electronic Age

July 2017 ▪ Volume 21 ▪ Issue 7

THE FINANCIAL CHOICE ACT: LEGISLATION CURBING SEC ENFORCEMENT POWERS MOVES FORWARD

By Marc J. Fagel, Mary Kay Dunning, Amy Mayer & Alexandra Grossbaum

Marc J. Fagel is a partner in the San Francisco office of Gibson, Dunn & Crutcher and a former Regional Director of the Securities and Exchange Commission's San Francisco Regional Office. Mary Kay Dunning is of counsel in Gibson Dunn's New York office. Amy Mayer and Alexandra Grossbaum are associates in the firm's New York office. Contact: mfagel@gibsondunn.com or mkdunning@gibsondunn.com.

On June 8, in a vote cast almost entirely along party lines, the Republicans in the U.S. House of Representatives passed H.R. 10, the "Financial CHOICE Act." The legislation rolls back a number of reforms established by the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), which represented a thorough overhaul of U.S. financial laws in response to the financial crisis. While the CHOICE Act is not expected to pass the Senate, pieces of the Act could move through the Senate separately. Moreover, President Trump has made the repeal of Dodd-Frank a priority.

Most of the public discussion of the CHOICE Act has centered on its repeal of Dodd-Frank's banking regulations and other sweeping regulatory changes that would impact the financial markets. However, the Act also includes multiple provisions aimed at curbing the Securities and Exchange Commission's enforcement authority. Under the previous administration, the SEC implemented a number of initiatives viewed as particularly aggressive and arguably unfair to companies and individuals who found themselves on the receiving end of an SEC investigation. The Act targets not just recent changes in SEC procedures, but several longstanding practices of the SEC's Division of Enforcement. Some of the more significant limitations to the SEC's enforcement authority proposed by the CHOICE Act are discussed below.

Opt-Out Provisions for Administrative Proceedings

Among the most potentially far-reaching aspects of the CHOICE Act is its significant pushback on the SEC's use of administrative proceedings. The SEC Enforcement Division's increasing reliance on its own administrative forum, rather than on federal district court, for litigated enforcement actions has received substantial attention in recent years. Though

IN THIS ISSUE:

THOMSON REUTERS®

the SEC has long had the ability to institute administrative proceedings (APs), the forum has historically been used primarily for cases against individuals and entities registered with the SEC, such as investment advisers and broker-dealers. Dodd-Frank, however, expanded the remedies available to the SEC in APs, such as the imposition of monetary penalties, leading the SEC to increasingly bypass civil court trials in favor of APs against non-registered entities as well.

The rising number of SEC APs post-Dodd-Frank has led to significant criticism. Unlike in federal courts, respondents in APs are tried on an accelerated hearing schedule with minimal pre-trial discovery and limited procedural safeguards. For example, until recently, parties in APs were not entitled to take any witness depositions before trial. While the SEC last year responded to concerns about the fairness of the AP process by implementing new rules (among other things, permitting a small number of depositions and providing for additional motion practice), the forum is still viewed by many as tilted towards the SEC. Some studies have shown that the Enforcement Division has a record of greater success when litigating before the SEC's own administrative law judges (ALJs)—who are employees of the agency—than they do in federal court.[1] Unsuccessful parties must appeal the ALJ's ruling to the SEC itself—the same five-member Commission that authorized the Enforcement Division to file charges in the first place. Moreover, there is currently a Circuit split regarding whether the manner in which ALJs are appointed violates the Appointments Clause of the U.S. Constitution, leading to some uncertainty around SEC APs.[2]

Under current law, the decision of whether to pursue an enforcement action in federal court or in an AP is wholly within the SEC's discretion, based on the recommendation of the Enforcement Division staff. Section 823 of the CHOICE Act would essentially remove the forum-selection discretion from the Enforcement Division, allowing respondents in APs to petition the SEC to terminate the proceeding and file the case in federal court. Under the plain language of the bill, the SEC would be required to grant such a petition. (The proposal does appear to exempt proceedings in which monetary penalties are *not* sought, so presumably APs in which the SEC seeks to impose bars or suspensions on brokers or advisers, or limit the ability of accountants or lawyers to practice before the SEC, would not be affected.)

In addition, for those respondents who choose to litigate in the administrative forum, the legislation

Wall Street Lawyer
West LegalEdcenter
610 Opperman Drive
Eagan, MN 55123

This publication was created to provide you with accurate and authoritative information concerning the subject matter covered; however, this publication was not necessarily prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional.

One Year Subscription ● 12 Issues ● $ 1092.00
(ISSN#: 1095-2985)

would require the Enforcement Division to prove its case through clear and convincing evidence, a higher burden of proof than the preponderance of the evidence standard currently used in both federal court and APs.

Recent analyses of SEC litigation filings have shown that, in the past year, the trend towards pursuing more litigated administrative proceedings has largely reversed itself, most likely as a result of public critiques and concerns about the constitutionality of the ALJ appointment process.[3] Passage of the CHOICE Act would not only solidify the situation, but likely further reduce the number of cases pursued as APs.

Presentations to SEC Staff

Upon the completion of an investigation, longstanding internal SEC procedures require the Enforcement Division staff to notify potential parties of the staff's intention to pursue an enforcement action (sending what is known as a "Wells notice"). The parties are then given an opportunity to make a written submission to the Commission before it considers authorizing the enforcement action. Section 821 of the CHOICE Act would supplement this procedure, affording the recipient of a Wells notice the right to make an in-person presentation to the SEC staff, and permitting the Commissioners themselves to attend such a presentation.

While individuals and entities currently have the ability to request such a meeting, the decision to entertain the request is at the discretion of the Enforcement staff. As a practical matter, members of the investigative team will almost invariably meet with counsel for proposed defendants. These meetings serve the interests of both sides, giving members of the Enforcement staff (including supervisors less familiar with the facts and trial counsel who may be litigating the matter) an opportunity to talk through the evidence with opposing counsel before moving forward, and giving parties an opportunity to discuss possible settlement of the case. And though the proposed legislation provides a right for the target of the action (not just counsel) to make a presentation, many attorneys would advise against doing so.

What is more variable, and not specifically addressed by the legislation, is the availability of more senior Enforcement officials to meet with counsel to discuss the proposed enforcement action. While potential defendants often request meetings with senior personnel, including the Director of the Enforcement Division, such individuals tend to agree to meetings primarily for particularly high-profile cases or those presenting novel legal or policy issues. To the extent the CHOICE Act makes these meetings more prevalent, the legislation has the potential to level the playing field for potential defendants in more routine cases; but at least as drafted, such meetings are not guaranteed.

Recent analyses of SEC litigation filings have shown that, in the past year, the trend towards pursuing more litigated administrative proceedings has largely reversed itself.

The legislation further requires the Enforcement staff to provide written reports of these Wells presentations to the Commission. Under current practices, the Commissioners receive copies of the proposed parties' written Wells submissions before voting to authorize the enforcement action, but there is no express requirement that supplemental materials or presentations provided to the Enforcement staff must be passed on to the Commission. Though some Commissioners have historically requested such materials (at least for non-settled cases), the proposal would provide further comfort to potential defendants that all of their submissions are given consideration before the enforcement action is authorized.

Finally, this provision of the bill authorizes Commissioners themselves (or their designees) to attend Wells meetings. Historically, parties to proposed enforcement actions and their counsel have not had direct access to the Commissioners outside of their written Wells submissions. The Act does not require any SEC Commissioner to participate, and whether any Commissioners would have the time or inclination to sit through such presentations (except perhaps in matters of unusual importance) is an open question. However, for certain cases that test the limits of the law, raise policy issues, or involve close evidentiary questions, opening the meeting to interested Commissioners could provide an added opportunity for the SEC to consider pursuing the case before initiating litigation.

One open question, however, would be the extent to which the proposal could create bureaucratic slowdowns insofar as the Enforcement staff (particularly from far-flung SEC regional offices across the country) would need to schedule Wells meetings to accommodate Commissioner participation.

Corporate Penalties and Other Remedies

Additionally, Section 824 of the Act would make it more difficult for the Commission to seek civil monetary penalties against public companies. While other provisions of the CHOICE Act increase the size of penalties that can be awarded generally, this provision would require an analysis by the SEC's Division of Economic and Risk Analysis regarding whether the alleged securities law violation resulted in direct economic benefit to the company, and whether the penalty would harm the company's shareholders. Though these factors are typically given some consideration by Commissioners,[4] such consideration has generally been informal, with the weight of such matters varying based on the individual Commissioner's personal views as to whether imposing corporate penalties is or is not good policy.

Imposing such a restriction could dramatically curtail penalties assessed against public companies in typical accounting and disclosure cases. At minimum, the bureaucratic burdens of obtaining an economic analysis of corporate penalties in each case could slow down the institution of enforcement actions against public companies, or incentivize the Enforcement staff to forgo penalties entirely in some cases for the sake of expediency.

The CHOICE Act would limit SEC enforcement sanctions in other respects as well. Section 827 of the Act would eliminate certain automatic disqualifications (such as the ability to take advantage of certain securities registration exemptions) which currently flow from enforcement actions, whether litigated or settled. While the loss of these exemptions may currently be waived by the SEC, such waivers are far from assured, and such disqualifications are viewed by many as unduly punitive. Under the legislation, the SEC would be required to make a specific finding, following a hearing, that the disqualification is appropriate.

Finally, Section 825 of the Act would eliminate the SEC's ability to bar individuals from serving as officers or directors of public companies, a sanction imposed in many enforcement actions, particularly public company accounting fraud cases.

> *One open question, however, would be the extent to which the proposal could create bureaucratic slowdowns.*

Additional Oversight

In addition to the above provisions, the Act includes several proposals mandating greater oversight of and rigor around SEC investigations:

- ***Enforcement Ombudsman*** (Sec. 818): The bill requires the Commission to appoint an "Enforcement Ombudsman" to serve as a confidential liaison between persons under investigation and the Commission. The Ombudsman would be required to submit annual reports to the Commission and to Congress. The new position would provide a mechanism for those who wish to escalate issues they encounter during the course of investigation. Of course, it is highly uncertain how this would operate in actual practice. In its most favorable light, the proposal would allow individuals and companies to challenge perceived overreach by the SEC staff and give the Commission greater visibility into the manner in which investigations are being conducted. But the procedure could also be ripe for abuse, allowing alleged wrongdoers to slow down investigations and impose bureaucratic second-guessing on the work of the SEC Enforcement staff.

- ***Adequate Notice*** (Sec. 819): This provision would prohibit the Commission from bringing an enforcement action "for an alleged violation of securities laws. . . if such person did not have adequate notice of such law, rule or regulation." The provision further requires the Commission to have provided some guidance on the conduct at issue before the conduct could be the subject of an enforcement action. Again, it is difficult to predict how this would actually be implemented. To be sure, the SEC has been criticized in the past (including by its own members) for "rulemaking through enforcement," *i.e.*, pursuing novel legal theories in enforcement actions to clarify or expand on the scope of the securities laws and regulations.[5] In theory, the proposal could curb suits against people and companies for acts not reasonably anticipated to subject them to enforcement scrutiny. However, the provision would almost certainly invite extensive litigation over whether there is specific enough guidance regarding whether particular conduct is prohibited by the securities laws.

- ***Advisory Committee*** (Sec. 820): The bill requires the Commission to establish an advisory committee to review enforcement policies and make recommendations regarding the SEC's enforcement objectives and strategies, due process concerns, investor protection, and the criteria for bringing or declining to bring enforcement actions. The Advisory Committee would be tasked with submitting a report to the Commission for consideration.

- ***Publication of Enforcement Manual*** (Sec. 822): This provision requires the Division of Enforcement to publish an updated enforcement manual setting forth the policies and practices that the staff must follow in investigations and administrative proceedings. (The Enforcement Division has in fact maintained an online manual for the past decade, so it is unclear what additional guidance would be required.) This provision further requires the publication of an annual enforcement plan and report identifying enforcement priorities, emerging trends and legal theories in its enforcement proceedings, and summaries of past enforcement actions, with a specific focus on any litigation lost by the Enforcement Division.

Conclusion

While the CHOICE Act's pushback on SEC enforcement has garnered much less attention than its other provisions, the legislation has the potential to dramatically change the tools and remedies available to the SEC's Enforcement Division.

If ultimately passed, the legislation would go a long way towards curbing some of the more aggressive practices which individuals and companies on the receiving end of enforcement interest have experienced. At the same time, some of the Act's more novel propositions could unduly hamper the ability of the Enforcement Division to conduct efficient, effective investigations and protect investors. Indeed, as Columbia University Law School Professor John C. Coffee, Jr. contended in his recent House testimony, aspects of the CHOICE Act "will hobble the SEC enforcement program," and while some provisions have merit, "the cumulative effect will be devastating."[6]

Given the breadth of the Act—not just in terms of SEC Enforcement, but its overall rollback of Dodd-Frank—it is not surprising that the legislation will face a far greater uphill battle in the Senate than it did in the House. Democrats are expected to filibuster the bill as it currently stands, and it may be a more likely scenario that the legislation is broken up and only smaller components submitted to a vote.

Regardless of the eventual fate of the legislation, the Act does serve to capture the frustration and sense of unfairness that many individuals and entities who find themselves caught up in SEC investigations experience. While nobody questions the need to investigate and remediate securities fraud and other regulatory violations, investigations themselves are long and prohibitively expensive, and the repercussions of even minor infractions can be severe.

A perception that the playing field is tilted in favor of the government does not serve the interests of investors or industry participants. Even a more modest version of the legislation could provide significant benefits in curbing SEC overreach.

ENDNOTES:

[1] *See* Jean Eaglesham, "SEC Wins with In-House Judges," Wall St. J. (May 6, 2015), www.wsj.com/articles/sec-wins-with-in-house-judges-1430965803, finding the SEC won 90% of APs between Oct. 2010 and March 2015, and only 69% of federal court trials. *But compare* Joshua Newville & Samantha Springer, "Who Wins in SEC Administrative Proceedings?," Nat'l L. Rev. (June 15, 2016), www.natlawreview.com/article/who-wins-sec-administrative-proceedings, finding greater SEC success in federal court than in APs.

[2] *Bandimere v. SEC*, No. 15-9586 (10th Cir. Dec. 27, 2016) (finding SEC ALJ appointments to violate the Constitution; *Raymond J. Lucia Cos. v. SEC*, No. 15-1354 (D.C. Cir. Aug. 9, 2016) (upholding ALJ appointments). A petition for *en banc* review of the Lucia decision was denied by a 5-5 vote of the D.C. Circuit on June 26, setting up a Circuit split which may be ripe for Supreme Court consideration.

[3] *See* David Kornblau & Sarah Mac Dougall, "SEC In-House Practice Going Back to 'Old Normal,' " Law360 (Nov. 18, 2016), www.law360.com/articles/864301/sec-in-house-practice-going-back-to-old-normal.

[4] In 2006, the SEC announced a longer list of factors to be considered in seeking penalties from public companies, though the benefit of the fraud to the company, and the potential harm to shareholders of a penalty, were core considerations. *See* Statement of the Securities and Exchange Commission Concerning Financial Penalties (Jan. 4, 2006), www.sec.gov/news/press/2006-4.htm.

[5] *See* Comm. Michael S. Piwowar, Remarks to the Securities Enforcement Forum 2014 (Oct. 14, 2014), www.sec.gov/news/speech/2014-spch101414msp ("I oppose the use by the Commission of enforcement measures as an alternative to rulemaking. . . I have significant concerns when Commission orders—especially in settled administrative actions—create new interpretations of the laws or regulations or impose new regulatory requirements. When Commission actions create such results, we fail in our duty to uphold due process.")

[6] Testimony of John C. Coffee Before the House Financial Services Committee (Apr. 28, 2017), financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-jcoffee-20170428.pdf.

IMPLICATIONS OF THE SUPREME COURT'S *KOKESH* DECISION

By Matthew T. Martens, Daniel P. Kearney, Jr., Benjamin Neaderland, John T. Byrnes & Gary Dyal

Matthew T. Martens is a partner at WilmerHale and is an experienced litigator of complex, high-stakes criminal and civil matters, previously serving in the US Department of Justice and as Chief Litigation Counsel for the Division of Enforcement at the Securities and Exchange Commission. Daniel P. Kearney, Jr. is a partner and has a practice that focuses on enforcement and regulatory matters for financial institutions, as well as government regulatory litigation and policy counseling. Benjamin Neaderland, also a partner, has a practice that focuses on high-profile securities and financial regulatory investigations and enforcement matters. John T. Byrnes is a senior associate and focuses on complex litigation matters. Gary Dyal is an associate focusing on enforcement and regulatory matters for financial institutions. All work out of WilmerHale's Washington, D.C. office.
Contact: matthew.martens@wilmerhale.com, daniel.kearney@wilmerhale.com or benjamin.neaderland@wilmerhale.com.

Earlier this month, the Supreme Court ruled unanimously in *Kokesh v. SEC*[1] that a claim for disgorgement arising from the violation of federal securities laws constitutes a "penalty" for purposes of the general statute of limitations provision in 28 U.S.C. § 2462. That provision imposes a five-year limitation on any "action, suit or proceeding for the enforcement of any civil fine, penalty, or forfeiture, pecuniary or otherwise." Because § 2462 applies to actions brought by *any* government entity, the Court's recent decision could have significant implications not only for enforcement actions by the Securities and Exchange Commission (SEC), but for *all* financial regulatory agency actions seeking disgorgement as a remedy for past misconduct.

The Decision

The Court looked to two principles in determining whether SEC disgorgement is a "penalty" for purposes of § 2462. *First*, the Court held that SEC disgorgement is a penalty because it is meant to address a wrong to the public, not an individual investor. Indeed, various courts—as well as the U.S. Government—have characterized disgorgement in SEC cases as a remedy for "harm to the public at large"[2] and as "an effective deterrent to future violations."[3]

Second, the Court held SEC disgorgement is a penalty because a primary purpose of disgorgement is deterrence—an inherently punitive goal. The Court rejected the Government's contention that SEC disgorgement is "remedial" and simply seeks to "restore the status quo." Although disgorged funds are sometimes distributed to affected individuals, this distribution is discretionary, and "courts have required disgorgement 'regardless of whether the disgorged funds will be paid to. . . investors as restitution.' "[4]

In short, the Court concluded, because disgorgement in SEC cases operates as punishment for violations of public laws rather than compensation for private wrongs, the disgorgement sanction "bears all the hallmarks of a penalty."[5]

Implications

The *Kokesh* decision has significant implications both for SEC actions and for actions by other federal financial regulators.

For one, the Court's decision was categorical: SEC disgorgement is a "penalty" under § 2462 even if used to compensate individual victims and restore the status quo. The decision will accordingly put pressure on the SEC to conduct investigations and bring actions promptly, and seems likely to increase agency aggressiveness in seeking and renewing tolling agreements. Agencies may also seek to devise alternative approaches—such as use of the "continuing violation" doctrine—to avoid application of § 2462.

In addition, although *Kokesh* addressed disgorgement only "as it is applied in SEC enforcement proceedings," its rationale could apply equally to disgorgement sought by other financial regulatory agencies. Like the SEC, these agencies can seek disgorgement through courts' "inherent equity power to grant relief ancillary to an injunction,"[6] but they can also seek disgorgement using their statutory authorities.

The Kokesh *decision has significant implications both for SEC actions and for actions by other federal financial regulators.*

For example, the Consumer Financial Protection Bureau (CFPB) is expressly authorized by statute to seek disgorgement as a remedy.[7] And under 12 U.S.C. § 1818(b), the Federal Reserve, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation can order institutions subject to cease-and-desist proceedings to take "affirmative action"—including the provision of "restitution" or "reimbursement"—in order to "remedy any conditions resulting from any violation" of the laws these agencies enforce.[8] It is not uncommon for agencies to seek such remedies beyond the 5-year limitation in § 2462. *Kokesh* calls this approach into serious doubt.

At a minimum, other agencies will have to distinguish their disgorgement remedies from SEC disgorgement if they hope to get around the limitations period in § 2462. That could be difficult, as existing case law suggests that disgorgement claims by financial regulatory agencies share the characteristics that drove the *Kokesh* analysis. The U.S. Court of Appeals for the Ninth Circuit, for example, recently recognized that the purpose of CFPB disgorgement claims was "not to redress consumer injuries but to deprive wrongdoers of ill-gotten gains."[9] The court described disgorgement as requiring "only a reasonable approximation of profits causally connected to the violation" and found "no basis" for the position that a disgorgement calculation should exclude funds paid by consumers who did not suffer any injury.[10]

Finally, *Kokesh* indicates that aggressive agency statute of limitations arguments are likely to be met with skepticism at the Supreme Court. This is the Supreme Court's second unanimous decision in recent years that soundly rejected agency arguments for a broader statute of limitations. In 2013, the decision in *SEC v. Gabelli*[11] held that no discovery rule applies to the limitations period in § 2462. This trend signals trouble for aggressive statute of limitations arguments advanced by several agencies. For example, federal banking agencies have long claimed that no limitations period governed administrative proceedings under the Federal Deposit Insurance Act[12]—a position the D.C. Circuit Court has rejected to the extent the agency's claim implicates § 2462.[13] Similarly, the CFPB has taken the position that no statute of limitation applies where the agency proceeds administratively.[14] The only court to address this argument ruled against the agency.[15]

Kokesh *indicates that aggressive agency statute of limitations arguments are likely to be met with skepticism at the Supreme Court.*

At a minimum, applying § 2462 to claims for disgorgement would serve as a significant constraint on the financial regulatory agencies' ability to avoid statute of limitations constraints.

ENDNOTES:

[1] *Kokesh v. SEC*, No. 16-529, 581 U.S. ____ (slip op.) (Jun. 5, 2017).

[2] Op. at 8-9 (quoting Br. for the United States at

22).

[3] Op. at 11 (citing *SEC v. Texas Gulf Sulphur Co.*, 312 F. Supp. 77, 91 (SDNY 1970), *aff 'd in part and rev'd in part*, 446 F. 2d 1301 (2d Cir. 1971); *see also* Op. at 11 ("The primary purpose of disgorgement orders is to deter violations of the securities laws by depriving violators of their ill-gotten gains." (quoting *SEC v. Fischbach Corp.*, 133 F. 3d 170, 175 (2d Cir. 1997))).

[4] Op. at 12 (quoting Fischbach Corp., 133 F. 3d at 175).

[5] Op. at 12.

[6] *Texas Gulf Sulphur Co.*, 312 F. Supp. at 91. The Federal Trade Commission claims similar authority. *See, e.g., F.T.C. v. Cephalon, Inc.*, 100 F. Supp. 3d 433, 439 (E.D. Pa. 2015) (ruling that "the FTC is permitted to seek disgorgement in cases brought pursuant to Section 13(b) [of the FTC Act]").

[7] 12 U.S.C. § 5565.

[8] 12 U.S.C. § 1818(b)(6).

[9] *Consumer Fin. Prot. Bureau v. Gordon*, No. 12-6147, 2013 WL 12116365, at *5 (C.D. Cal. June 26, 2013), *aff'd in part, vacated in part*, 819 F.3d 1179 (9th Cir. 2016).

[10] *Consumer Fin. Prot. Bureau v. Gordon*, 819 F.3d 1179, 1195-96 (9th Cir. 2016). It appears the CFPB does not dispute this characterization of disgorgement or the implication that § 2462 therefore applies to the remedy. In the past, the agency has taken the position that "no statute of limitations applies" when it seeks disgorgement through an administrative proceeding. *See* Brief of Respondent Consumer Financial Protection Bureau, *PHH Corp. v. CFPB*, 839 F.3d 1, 50 (D.C. Cir. 2016), *reh'g en banc granted, order vacated* (Feb. 16, 2017). Following the *Kokesh* decision, however, the CFPB submitted a notice of supplemental authority in PHH acknowledging that "the five-year limit in 28 U.S.C. 2462 applies. . . to disgorgement, which is the monetary remedy that the Bureau imposed." *See id.*, Letter Pursuant to FRAP 28(j) (June 7, 2017).

[11] *SEC v. Gabelli*, 133 S. Ct. 1216 (2013).

[12] *See, e.g.*, OCC Interpretive Letter, 1977 WL 23261 (Oct. 6, 1977) ("the Comptroller is not restricted by any statute of limitations under either the Truth in Lending Act or [the FDI Act].").

[13] *Proffitt v. FDIC*, 200 F.3d 855, 860 (D.C. Cir. 2000).

[14] *PHH Corp. v. CFPB*, 839 F.3d 1, 50 (D.C. Cir. 2016), *reh'g en banc granted, order vacated* (Feb. 16, 2017).

[15] *Id.* at 50.

10 QUESTIONS EVERY BOARD SHOULD ASK IN OVERSEEING CYBER RISKS

By Yafit Cohn & Karen Hsu Kelley

Yafit Cohn is Counsel in Simpson Thacher & Bartlett's Public Company Advisory Practice in New York. Her practice focuses on advising public companies on issues pertaining to securities law and corporate governance. Karen Hsu Kelley is a Partner and Head of Simpson Thacher's Public Company Advisory Practice. She counsels U.S. and non-U.S. public companies on compliance with federal securities laws and the listing requirements of the major U.S. exchanges. The article was prepared in conjunction with Nasdaq Corporate Solutions' Meetx Board Portal, which was designed to provide public, private, and nonprofit boards and leadership teams with greater governance management, throughout the organization. Contact: yafit.cohn@stblaw.com or kkelley@stblaw.com.

Those who work in the cybersecurity industry believe that there are two types of companies in the United States: "those that have been hacked and those that don't know they've been hacked."[1] Indeed, more and more companies are experiencing data breaches, and it seems that hardly a week goes by without a data breach reported in the headlines.

The consequences of such a breach could be significant. Predictably, a data breach is typically followed by a slew of lawsuits, including putative consumer class action lawsuits and shareholder derivative actions filed against the directors and officers of the company for their alleged breach of fiduciary duties. In recent years, for example, dozens or even hundreds of lawsuits have been filed against certain companies in the retail and healthcare spaces in connection with data breaches. Additionally, various government agencies, on both the federal and state level, have investigated companies for data breaches, and such investigations have resulted in enforcement actions and, consequently, settlements (some of which have been significant). Moreover, data breaches could have a substantial impact on the company's business. The disclosure of a data breach could lead to a meaningful drop in the company's stock price and, as seen in recent months, can reduce the purchase price of a target company significantly. Finally, there is often an incalculable but very real reputational cost to companies that have suffered a data breach. This cost can far surpass the monetary amount paid to settle any lawsuits or regulatory actions.

The costs of a data breach can be exponentially greater where the board is perceived not to have taken the appropriate steps to properly oversee the company's cybersecurity. These added costs include diminished chances to be able to dismiss a shareholder derivative action filed on behalf of the company, as well as negative vote recommendations from proxy advisory firms against the company's directors.

Because of the costs associated with a data breach and the fact that no company today is immune from them, it is essential that each board ensure that it is adequately overseeing the company's cyber risks. Especially for directors who do not have a technology background, this mandate can be a daunting task. The good news, however, is that Delaware sets a very high threshold for finding that directors breached their duty of care; as articulated in the seminal case *In re Caremark*, while directors have a duty to oversee corporate risk, they are only liable if plaintiffs can demonstrate "sustained or systemic failure of the board to exercise oversight—such as an utter failure to assure a reasonable information and reporting system exists." Recognizing that directors can protect themselves from liability by taking an active oversight role in their company's cybersecurity preparedness, this article sets out to provide boards with some practical advice regarding how to approach cybersecurity oversight and outlines specific categories of questions directors may wish to consider asking to fulfill their oversight duty.

A Practical Approach: 10 Questions Every Board Should Ask in Overseeing Cyber Risks

The overriding principle for any board overseeing cyber risks is that cybersecurity should be approached as an enterprise risk management (ERM) issue, rather than a technological problem for the information technology team to handle. The management of cyber risks is just one element of the company's risk management and oversight, and overseeing such risks should be part of the board's oversight of the execution and performance of the company's ERM program (or, if the company doesn't have an official ERM program, the company's risk assessment and mitigation activities). Accordingly, while directors may not understand all the technological details surrounding data protection systems and processes, the board nevertheless needs to ensure that it is comfortable that management is effectively managing the company's cyber risks, as with any other risk the board oversees through the ERM process.

Fundamentally, to fulfill its duty of care in overseeing cyber risk under *Caremark*, the board must allot regular and adequate time on its agenda to discuss cybersecurity matters. At a minimum, the board should meet with the person in charge of organization-wide data privacy and security (such as the Chief Information Security Officer) on an annual basis. Similar to other risks the board oversees, the board should spend this time to ensure that it gains a solid understanding of, among other things:

- The cyber risks the company faces, including the potential impact of those risks on the company's business.

- The steps management is taking to mitigate those risks.

- How the company is prepared to handle a security breach.

In practice, ensuring that the company is adequately managing its cyber risks can be difficult. To be better prepared—and to ensure that it is properly fulfilling its oversight role—the board should ask thoughtful questions. While there is no "one size fits all" approach to questions a board should ask in its oversight of cybersecurity (particularly as different industries exhibit different risk profiles), we suggest ten categories of questions that boards of all companies should be asking members of management responsible for cybersecurity. In each case, directors should assess the responses to these questions and determine whether follow-up is required. Additionally, depending on the circumstances, additional questions may be necessary.

> *The overriding principle for any board overseeing cyber risks is that cybersecurity should be approached as an enterprise risk management (ERM) issue, rather than a technological problem for the information technology team to handle.*

1. Leadership

Has the company identified a senior person with clear responsibility for organization-wide cybersecurity preparedness, who has support from the top of the organization?

As with any important management function, someone needs to have ultimate responsibility for cybersecurity. This person is often (but need not be) the Chief Information Security Officer.

2. Budget and Staffing

Has management given serious consideration to how much of the budget and how much staff is adequate for proper cyber risk management?

The appropriate budget and staff will depend on a variety of factors, including the industry in which the company operates. Companies in the healthcare and financial services industries, for example, tend to experience more data breaches than companies in other industries, such as construction or real estate. The board's role is to ensure that management is thoughtful regarding its allocation of resources to cyber risk, given the company's industry and circumstances. Additionally, the board should ask questions to ascertain whether management is properly prioritizing the allocation of funds within the overall cyber budget in accordance with relative risk.

3. Comprehensive, Written Cybersecurity Program

Has management formulated a comprehensive, written data privacy and cybersecurity program consisting of reasonable and appropriate policies and procedures?

It is essential that companies formulate a comprehensive, written data privacy and cybersecurity plan that is reviewed by and distributed to all individuals who may be involved in its execution.

a. Prerequisites to Formulating a Comprehensive, Written Cybersecurity Program

In order to create a robust cybersecurity program, management must first:

- Know where its data resides and who is accessing it.

  Without this basic information, management will encounter significant hurdles in adequately safeguarding the company's sensitive data.

- Understand the company's top cyber risks.

  Without knowing what the company's specific cyber risks are at any point in time, management cannot take effective steps toward preventing a breach (or at least mitigating known risks) and cannot allocate its budget appropriately. While many think of data breaches as being synonymous with hacking or cyber-attacks, companies often encounter other types of cyber risk, which could be significant. A prime example is misuse of information by current or departing employees. According to *Verizon's 2017 Data Breach Investigations Report*, 25% of all data breaches occurred because internal actors abused the access with which they were entrusted—whether maliciously or not (*e.g.*, ignoring protocol or circumventing procedures to facilitate or expedite certain processes). Moreover, even cyber-attacks are multi-faceted and require an understanding of their different phases, each of which generally corresponds to different potential vulnerabilities of the company.

- Know whether there are industry standards applicable to the company's industry and what market practice is among the company's peers in the same industry.

  Benchmarking could be an important step in ensuring that the company's cybersecurity program is appropriately robust. In this regard, a company may choose to engage an outside advisor that can provide benchmarking services, comparing the company's data security processes and practices with those of its peers.

The board should ask questions to confirm that management has adequately gathered and addressed all of this information in formulating its cybersecurity plan. Given that this information can change over time, the board should make sure to revisit these questions at least annually. The board should also inquire whether and how management got comfortable with the fact that its plan is state-of-the-art.

b. Key Elements of a Comprehensive, Written Cybersecurity Program

Naturally, cybersecurity programs will differ, depending on the company and its industry. There are, however, several hallmarks of any comprehensive cybersecurity program. It must:

- Ensure that the company does not collect or store nonessential customer data.

  Sensitive information should be retained only as long as the company has a business reason for it. The rationale behind this is simple: If the data is not in the company's system, it cannot be stolen.

- Indicate how the company ensures that data is destroyed responsibly after it has outlived its business purpose.

- Ensure that more sensitive data is stored separately with higher safeguards.

- Ensure that employees are granted access to sensitive data only if necessary for them to perform their duties.

- Indicate the measures the company takes to protect against the downloading of malicious data.

- Indicate what measures the company takes to reduce the risk that data will be transferred from the company's internal network to the outside internet (*e.g.*, implementing a firewall between the company's internal systems and the internet, blocking particular internet connections known to be used by hackers or creating a list of approved servers to which the company's network is permitted to upload).

The board should ask thoughtful questions regarding each of these and any other significant aspects of the company's cybersecurity program.

c. Reassessing and Testing the Cybersecurity Program

The cybersecurity plan must be reviewed with critical eye at least annually, given that the nature and scope of cyber risks are in a constant state of evolution. The board should ask whether the plan has been reassessed and whether changes should be or have been made to the plan as a result.

Moreover, the cybersecurity plan must be tested to gauge its effectiveness. Some companies conduct such testing in-house, while others hire independent third parties to do so. In addition to inquiring as to whether the company's cybersecurity plan has been tested, the board should ask what the results of that test were and how the vulnerabilities identified during such assessment, if any, have been addressed.

4. Employee Training and Education

Has management instituted effective training programs that instruct employees on the appropriate handling and protection of sensitive data?

As with other forms of employee training, cybersecurity training programs should be meaningful, consisting of more than written policies that employees are required to review and sign. The board should ask probing questions to determine whether management has been adequately conveying to employees the company's protocol, the importance of following it and the consequences of not following it. The board should ensure that it is comfortable that management's training and education programs are properly designed to enable employees to internalize the company's cybersecurity policies. The board should also ask questions designed to ascertain whether management is fostering a culture of compliance with the company's data security policies and protocols and holds accountable those who are not compliant with them.

5. Third-Party Vendors

Has management taken steps to mitigate the cybersecurity risks associated with outsourcing business functions to third parties?

According to the *2016 Soha Systems Survey on Third Party Risk Management*, 63% of all data breaches were linked to a third party. This statistic underscores that even if a company has a state-of-the-art cybersecurity program, that program is worthless if the company's vendors, who have access to the company's network and/or sensitive data, do not have similarly robust data security policies and practices. In other words, a company's cybersecurity program is only as strong as the weakest link in its vendor chain.

There are several crucial steps companies should take with regard to their third-party vendors.

- Management should ensure that the company's third-party vendors are aware of the company's information securities policies and agree to adhere to them.

- Prior to entrusting a third party with sensitive data, management should review the third-party vendor's data security policies and ask the vendor specific questions about its data security practices to ensure that the vendor properly handles and secures shared sensitive information.

- Management should make sure that any agreement with a third party clearly identifies:

  — how the service provider will safeguard the organization's sensitive data;

  — whether the vendor will subcontract any services to other vendors and, if so, how minimum data security standards will be set; *and*

  — whether the service provider will notify the company in case of a breach.

- It is critical that companies properly segment the parts of their network accessible to vendors and those that house sensitive data to which the vendors do not need access.

With these points in mind, directors should ask the appropriate members of management thoughtful questions to ensure that the company is doing all it can to safeguard the sensitive information to which its third-party vendors have (or could get) access.

6. Legal Compliance and Regulatory

Does management have an effective system in place for staying abreast of and complying with evolving federal, state and international data security laws and regulations that are applicable to its operations?

Those charged with ensuring the company's data security must be aware of any federal, state and/or international laws that require them to take measures to secure sensitive data. Relevant regulations can change with some frequency, and management must have an effective system in place to track such changes and comply with all regulations. For many companies, this undertaking may entail using an outside vendor. The board should assure itself that management has an effective process for staying updated with regard to applicable legal and regulatory changes.

7. Insurance

Has management given serious consideration to purchasing cyber liability insurance?

In today's environment, management should at least give serious consideration to investing in cyber liability insurance. The board should ensure that management has explored whether it makes sense for the company to purchase cyber liability insurance and should ask questions to understand management's approach to purchasing such insurance. If the company has not purchased cyber liability insurance, the board should make sure that it is comfortable with management's rationale for its decision. If the company has cyber liability insurance, the board should ask about its terms and scope of coverage in an effort to ensure that it is sufficient given the company's specific facts and circumstances.

8. Detection

Has management installed adequate technology not only for preventing the downloading of malicious software but also for detecting and alerting the organization to attempted breaches?

It is essential that every company have robust security software tools and antivirus systems in place to detect attempted breaches. But this alone is not sufficient. Each company must also train security employees on the protocol for responding to automated alerts generated by this technology. If a company has systems that generate alerts but does not have personnel sufficiently trained in handling those alerts, the alerts are not worth much. Accordingly, directors should ask questions to help them understand and assess the measures management has implemented to detect breaches and train employees to respond to breach alerts. Among other things, directors should ask whether any data breaches or incidents have been detected in the past, how long it took for such breaches or incidents to be detected and how their detection was handled by the company's personnel.

9. Comprehensive, Written Breach Response Plan

Does management have a comprehensive, written breach response plan in place?

It is critical that companies be prepared to respond to a breach quickly, effectively and calmly. To that end, companies must have a comprehensive, written breach response plan in place and be clear on what events will trigger that response plan. As part of their response plan, companies should:

- Form a breach response team composed of individuals from key departments (including Information Technology, Legal and Corporate Communications) and identify individual functions and responsibilities in the event of a data breach.

- Select an individual with ultimate responsibility for overall implementation of the plan (*i.e.*, the person authorized to make the final decision on difficult questions).
- Identify outside advisors that may need to be contacted in the event of a breach, such as legal, forensic and public relations specialists, as well as regulators and law enforcement authorities.
- Outline each phase of the response plan, from initial response activities (such as reporting the breach) to strategies for notifying affected parties, to breach response review and the remediation process.
- Create hypothetical scenarios to test the plan (*i.e.*, do a practice run) and address any vulnerabilities identified during those simulations.
- Ensure that the plan is reviewed regularly and revised as necessary.

The board should make inquiries to determine whether management has taken each of these steps to the board's satisfaction and has otherwise formulated a comprehensive breach response plan.

10. Non-Digital Information and Physical Devices

What steps does management take to safeguard sensitive non-digital information?

With all the talk about "cyber," it is important to remember that safe and secure storage of non-digital data, as well as proper destruction of documents and devices, is equally essential. To the extent possible, companies should minimize the locations in which sensitive non-digital information is stored and should ensure the safe and secure storage of this data. Some measures they can take include locking office doors and filings cabinets and/or installing card keys on doors. In addition, companies should ensure that documents (as well as disks, DVDs, flash drives and computers) with sensitive information are properly destroyed before disposal (such as by shredding or burning), as dumpster diving is still a common means of stealing data.

Though it will be focused on overseeing cyber risks in the true sense of the term, the board should also make sure to ascertain whether the company's policies and practices adequately protect sensitive non-digital information in the company's possession.

Conclusion

To fulfill its duty of care with respect to overseeing the company's cyber risks—and to be able to demonstrate, in any future litigation, that it has fulfilled this duty—the board must ask thoughtful and strategic questions to understand how management is preventing, detecting and responding to data breaches and incidents and to ensure that it is comfortable that the measures being taken in this regard are sufficient and appropriate. By asking the questions outlined above—and any other questions relevant to the company's facts and circumstances—and by exercising good judgment, directors can successfully oversee the cyber risks facing the company and the company's plan to mitigate and respond to those risks.

ENDNOTES:

[1] Nicole Perlroth, "The Year in Hacking, by the Numbers," N.Y. Times, April 22, 2013.

THE FX GLOBAL CODE: GAME-CHANGING INTERNAL ENFORCEMENT

By William F. Johnson & Katherine Kirkpatrick

William F. Johnson is a partner at King & Spalding in the Special Matters and Government Investigations Practice Group. Mr. Johnson is a former federal prosecutor and Chief of the Securities and Commodities Fraud Task Force in the U.S. Attorney's Office for the Southern District of New York, and a former Enforcement Division attorney at the Securities and Exchange Commission. Katherine Kirkpatrick is a senior associate at King & Spalding in the Special Matters and Government Investigations Practice Group. Ms. Kirkpatrick focuses primarily on white collar criminal litigation, government investigations, corporate compliance and regulatory matters. Contact: wjohnson@kslaw.com.

In 2007, growth statistics excitedly touted the total turnover in global foreign exchange (FX) markets as six-times larger than U.S. Treasury bond trading and 30-times larger than trading on the New York Stock Exchange.[1] After decades of globalization, explosive growth in electronic trading and financial services, and open market access to a myriad of active participants, the FX market's status as world's largest seemed untouchable. But 10 years later, while still massive and hugely liquid, the market's growth has finally started to slow. Trading volumes in actively traded currencies like the yen, Swiss franc and Euro have slumped, and industry professionals have offered various reasons for the disconcerting numbers. One theme, however, has emerged—recent regulatory settlements, pleas and headlines have not helped.

Amidst this background, the Bank for International Settlements (BIS) established the Foreign Exchange Working Group (FXWG) in July 2015 to strengthen industry conduct standards and best practices in the form of a "Global Code." In turn, FXWG launched the initial phase of the Code in May 2016, and supplemented the early roll-out with a Phase 2 full publication on May 25, 2017.

The Code, which is meant to lay out best practices for the wholesale FX market, does not supplant or replace existing law. The design of the Code is twofold: *i*) to iterate obligations for FX market participants; and *ii*) to ensure compliance through an attestation regime centered around a "Statement of Commitment." The stated purpose—"desire to promote integrity and restore confidence in the wholesale foreign exchange market (FX market) in light of the recent cases of misconduct"[2]—is ambitious, laudable, and untested. Both reactive and proactive, it is a test case for industries striving to achieve compliance, to address aggressive regulation, or both.

Background

In October 2016, dramatic remarks by Minouche Shafik, Bank of England Deputy Governor, Markets and Banking, deemed the recent FX market troubles the result of "multiple forces" causing a "deterioration of conduct."[3] In his comments, Shafik theorized that reform could be best achieved by " 'hard law' (legislation and regulation by the official sector), 'soft law' (codes and standards defined collectively by market participants), and culture."

The Code, which is meant to lay out best practices for the wholesale FX market, does not supplant or replace existing law.

The Code is a perfect example of soft law, meant to compliment regulation and spur cultural and practical adherence to so-called "hard law." Meant to "become an integral part of the FX market globally,"[4] the Code needs the full support of a broad range of market participants to have its full effect, particularly if it aims to be globally applicable across jurisdictions. As the FX market inherently struggles with cross-border legal interpretation and jurisdictional issues, the high-level approach embodied in the Code could potentially, and intriguingly, apply to a Japanese client trading Australian dollars into Japanese yen (AUD/JPY) and an American client trading Euros into Swiss francs (EUR/CHF).

The Global Code—Leading Principles

In May 2016, Phase I of the Code was released, citing six leading principles. According to the FXWG, these principles were prioritized due to the market's need for clarity. The principles are as follows:

- **Ethics**—the expectation of ethical and professional behavior;
- **Governance**—requiring robust and clear policies, procedures and organizational structures;
- **Information Sharing**—anticipating clarity, accuracy and confidentiality in order to promote effective communication supporting a healthy, fair, open, liquid and appropriately transparent market;
- **Execution**—requiring the exercise of care when negotiating or executing transactions;
- **Risk Management & Compliance**—mandating the promotion and maintenance of a thriving control and compliance environment; *and*
- **Confirmation & Settlement Processes**—requiring efficient, transparent and risk-mitigating post-trade processes.

After the release of Phase I and leading up to the full release a year later, FX market participants rapidly indicated widespread support and signaled their intent to adopt the Code.[5] This vocal support continued after market participants were sent a working draft of the full Code in February 2017, and upon the full release on May 25.

Prior to the full release, Guy Debelle, Deputy Governor of the Reserve Bank of Australia and the head of the FXWG, promised that the full provisions would "provide a more comprehensive description of the suite of mechanisms to support adherence to the Code."[6] When the full Code was published, the text of the 78-page document was in line with Debelle's promise: it largely expanded on the original principles, offering details and "stylized examples" supporting expanded sub-principles under those six overarching themes.

Specifically, the full Code offers provisions tied to an expanded set of 55 principles categorized within the six leading principles. It also sets forth detailed illustrative examples; provides a framework for risk management, compliance and review; and includes the form "Statement of Commitment," meant to be signed and published by industry institutions.[7] In his speech upon the release of the full Code, Debelle ambitiously promised that the Code would help "restore confidence and promote the effective functioning of the wholesale FX market," and said the Code reflected the industry's collective judgment and comment. Debelle also set forth a timeframe of "no more than twelve months" for expected adherence by the "vast majority of market participants."[8]

To date, the feedback from market participants is largely positive, although minor areas of angst lie within the decision not to ban the controversial "last look" practice,[9] and surround potential logistical impediments to rolling out a fully compliant infrastructure prior to attestation. As to the former, the drafters have encouraged participants to "be transparent" regarding the use of last look, which begs the question of whether disclosure alone will end the practice. As to the latter, as the Code encourages the Statement of Commitment as a form of adherence, market participants have queried whether the attestation could create another avenue of civil attacks tied to misrepresentation were they to step out of line with some facet of the Code.

Once the Code is widely adopted, however, it will serve as an embodiment of industry standards, and thus could act as a defense indicating *de facto* good faith on the part of participants.[10]

Adherence & Implications

Adherence to the Code is a key aspect of the Code's rollout, as universal applicability and positive change is inherently tied to industry-wide modifications. To ensure adherence, after the full release of the Code on May 25, the FXWG agreed to form the Global Foreign Exchange Committee (GFXC), which will work to promote and maintain the Code, and "seek to promote collaboration and communication among local foreign exchange committees and other jurisdictions with significant FX markets."[11] The GFXC is also expected to publish guidance and create an index of a forthcoming register of Code signatories.[12]

The market community has shown early signs of enthusiasm for the Code. Some market participants have already signed the Statement of Commitment and many others—including numerous central banks[13]—have publicly touted their commitment to the Code. Most prominently, the UK's Financial Conduct Authority indicated that it intended to link the Code to its Senior Managers and Certification Regime.[14] Early feedback from domestic regulators, however, indicates that they intend to leave the Code alone and hope that "best practices" is effective.[15]

Although global regulators have not taken up the mantle of change themselves, the Code will still necessitate scrutiny, and thus require moves on the part of market participants. Firms will need to evaluate their current compliance with the six leading principles and 55 sub-principles, and publicly document their compliance under the auspices of transparency. Most firms will need to assign specific responsibility for coordination under the Code to compliance personnel and senior management, and integrate various provisions into existing policies and procedures. Certain market participants have already jump-started their integration—for example, according to Adrian Boehler, global co-head of FXLM and commodity derivatives at BNP Paribas: "We expect the mean time to sign statements [of commitment to the Code] between six and twelve months. There are a number of different mechanisms for firms to proportionately embed the code, such as training, and we have trained 700 staff."[16] Similarly, Citigroup, Inc., the world's largest currency trader, has embarked on a "sweeping educational initiative" designed to train thousands of staff members globally on market conduct.[17]

In addition to training, market participants should evaluate the use of technology to reduce operational risk; identify disclosures that other entities should receive regarding the protection of information and confidentiality; and scrutinize their existing risk management protocol. These high-level steps are some of the obvious first moves. But most importantly, firms should evaluate their own best practices to ensure they are prepared to be part of the solution, since the odds of a misstep in the FX market may be more likely in the future.

ENDNOTES:

[1] William Barker, *The Global Foreign Exchange Market: Growth and Transformation*, Bank of Canada (2007), http://www.bankofcanada.ca/wp-content/uploads/2010/06/barker.pdf.

[2] Foreign Exchange Working Group, *FX Global Code Public Update on Adherence*, Bank for International Settlements (May 2016), http://www.bis.org/mktc/fxwg/am_may16.pdf.

[3] Minouche Shafik, Deputy Governor for Markets and Banking, Bank of England, Panel Discussion at the Federal Reserve Bank of New York Conference on *'Reforming Culture and Behavior in the Financial Services Industry'* (Oct. 20, 2016) http://www.bis.org/review/r161024b.pdf.

[4] *See* Foreign Exchange Working Group, *supra* note 2.

[5] For example, on March 20, ACI The Financial Markets Association, a member of the Market Partici-

pants Group (MPG) and the largest trade association for the global FX market, mandated that its members commit to the code. *See* ACI Financial Markets Association, *ACI FMA Welcomes the BIS Global FX Code*, ACI Financial Markets Association (Mar. 20, 2017), ("[W]e will strongly urge all ACI FMA members and wholesale market participants to learn the code, attest to their compliance, and demonstrate their adherence to the new Code."); https://acifma.com/news/aci-fma-welcomes-bis-global-fx-code.

[6] Guy Debelle, Deputy Governor of the Reserve Bank of Australia; Opening remarks at the Trade Tech FX Asia Conference, *Regulatory overview: The FX Global Code—defining the next steps towards a standard industry Code of Conduct*, Bank for International Settlements (Mar. 22, 2017);, http://www.bis.org/review/r170322e.pdf.

[7] The Statement of Commitment, available in Annex 3 of the Code, is accompanied by an Explanatory Note outlining how the Statement should be used and its benefits. It also attemptings to anticipate and answer other questions by market participants, such as "How should market participants take account of their corporate structure?"

[8] Guy Debelle, Opening Remarks at the Launch of the FX Global Code, Reserve Bank of Australia (May 25, 2017); http://www.rba.gov.au/speeches/2017/sp-dg-2017-05-25.html.

[9] The "last look" practice, which enables market makers to pull out of a trade at the last minute if the market moves against them, has been restricted by certain major currency trading platforms like BATS and Thompson Reuters since May 2015, as it subjects forex dealers to buy-side complaints about unfair pricing.

[10] *See SEC v. Arthur Young & Co.*, 590 F.2d 785, 788 (9th Cir. 1979) (The court refused to censure certified public accountants in an action alleging violations of federal securities laws because the accounting firm "discharged its professional obligations" by complying with generally accepted auditing standards in good faith.)

[11] ACI America, *New Global Foreign Exchange Committee (GFXC) Formed*, ACI America (May 26, 2017); https://aciamerica.us/new-global-foreign-exchange-committee-gfxc-formed/.

[12] Joe Clark, *FX global code registers to be live within months*, Euromoney (May 25, 2017) (highlighting that industry utility CLS has already suggested that it will look to operate a public register); http://www.euromoney.com/Article/3720234/FX-global-code-registers-to-be-live-within-months.html.

[13] For example, days after the Code's full release, the Monetary Authority of Singapore, the Hong Kong Monetary Authority, the bank of Korea, the Reserve Bank of Australia and the Reserve Bank of India had indicated their support of the Code.

[14] Statement by the Financial Conduct Authority, *FCA statement on the publication of the FX Global Code*, Financial Conduct Authority (May 25, 2017) ("The FCA welcomes today's publication of the FX Global Code. As we set out in our mission, standards can be a useful way for the industry to police itself in support of our regulatory work, and can help firms to communicate expectations of individuals when linked to the senior managers and certification regime. We expect firms, senior managers, certified individuals and other relevant persons to take responsibility for and be able to demonstrate their own adherence with standards of market conduct."); https://www.fca.org.uk/news/statements/fca-statement-publication-fx-global-code.

[15] When questioned whether U.S. regulators might adopt a similar approach to the UK's link to the UK Senior Managers and Certification Regime, Federal Reserve Bank of New York Markets Head Simon Potter said: "I think that across the globe you will see different approaches depending on the regulatory environment and how used they are to using best practices. In the U.S., best practices have proved very helpful for us, and I have a strong expectation that in the New York market, these best practices will be very effective." Potter, who is a member of FXWG, led the work on the writing of the Code. *See* Clark, *supra* note 12.

[16] Shanny Basar, *Buyside Urged to Help Fix FX*, Markets Media (May 25, 2017); https://marketsmedia.com/buyside-urged-fix-fx/.

[17] Lananh Nguyen and Stefania Spezzati, *FX Ethics Revamp Spurs Citigroup Training, App for Traders*, Bloomsberg (June 1, 2017); https://www.bloomberg.com/news/articles/2017-06-01/fx-ethics-revamp-spurs-training-at-citigroup-app-for-traders.

THE ROLE OF BIG DATA, MACHINE LEARNING & AI IN ASSESSING RISKS: A REGULATORY PERSPECTIVE

A Speech by Scott W. Bauguess

Scott W. Bauguess is the Acting Director and Acting Chief Economist of the Securities and Exchange Commission's Division of Economic and Risk Analysis (DERA). He gave the keynote address at the 19th Annual Operational Risk North America Conference on June 21 in New York City. This is a partial transcript of his remarks.

[. . .] My remarks this afternoon will center on a technology topic that is encroaching on many aspects of our lives and increasingly so within financial markets: Artificial Intelligence. Perhaps better known by its two-letter acronym "AI," artificial intelligence has been the fodder of science fiction writing for decades. But the technology underlying AI research has recently found applications in the financial sector—in a movement that falls under the banner of "Fintech." And the same underlying technology [machine learning and AI] is fueling the spinoff field of "Regtech," to make compliance and regulatory-related activities easier, faster, and more efficient.

This is the first time that I have addressed the emergence of AI in one of my talks. But I have spoken previously on the two core elements that are allowing the world to wonder about its future: big data and machine learning.[1] Like many of your institutions, the Commission has made recent and rapid advancements with analytic programs that harness the power of big data. They are driving our surveillance programs and allowing innovations in our market risk assessment initiatives. And the thoughts I'm about to share reflect my view on the promises—and also the limitations—of machine learning, big data, and AI in market regulation.

Perhaps a good place to begin is with a brief summary of where we were, at the Commission, two years ago. I remember well, because it was then that I was invited to give a talk at Columbia University on the role of machine learning at the Securities and Exchange Commission (SEC). I accepted the invitation with perhaps less forethought than I should have had. I say this because I soon found myself googling the definition of machine learning. And the answers that Google returned—and I say answers in plural, because there seem to be many ways to define it—became the first slide of that presentation.[2]

The Science of Machine Learning and the Rise of Artificial Intelligence

Most definitions of machine learning begin with the premise that machines can somehow learn. And the central tenets of machine learning, and the artificial intelligence it implies, have been around for more than a half a century. Perhaps the best known, early application was in 1959, when Arthur Samuel, an IBM scientist, published a solution to the game of checkers. For the first time, a computer could play checkers against a human and win.[3] This is now also possible with the board game "Go," which has been around for 2,500 years and is purported to be more complicated and strategic than Chess. Twenty years ago, it was widely believed that a computer could never defeat a human in a game of "Go." This belief was shattered in 2016, when AlphaGo, a computer program, took down an 18-time world champion in a best-of-seven match.[4] The score: 4 to 1.

Other recent advancements in the area of language translation are equally, if not more, impressive. Today, if the best response to my question on the definition of machine learning is in Japanese, Google can translate the answer to English with an amazing degree of clarity and accuracy. Pull out your smart phone and try it. Translate machine learning into Japanese. Copy and paste the result into your browser search function. Copy and paste the lead paragraph of the first Japanese language result back into Google Translate. The English language translation will blow your mind.

What would otherwise take a lifetime of learning to accomplish comes back in just a few seconds.

The underlying science is both remarkable and beyond the scope of this talk.[5] (Not to mention my ability to fully explain it.) But it is not too difficult to understand that the recent advancements in machine learning are shaping how AI is evolving. Early AI attempts used computers to mimic human behavior through rules-based methods, which applied logic-based algorithms that tell a computer to "do this if you observe that." Today, logic-based machine learning is being replaced with a data-up approach. And by data-up, I mean programming a computer to learn directly from the data it ingests. Using this approach, answers to problems are achieved through recognition of patterns and common associations in the data. And they don't rely on a programmer to understand why they exist. Inference, a prerequisite to a rule, is not required. Instead, tiny little voting machines, powered by neural networks, survey past quantifiable behaviors and compete on the best possible responses to new situations.

If you want a tangible example of this, think no further than your most recent online shopping experience. Upon the purchase of party hats, your preferred retailer is likely to inform you that other shoppers also purchased birthday candles. Perhaps you need them too? Behind this recommendation is a computer algorithm that analyzes the historical purchasing patterns from you and other shoppers. From this, it then predicts future purchasing-pair decisions. The algorithm doesn't care why the associations exist. It doesn't matter if the predictions don't make intuitive sense. The algorithm just cares about the accuracy of the prediction. And the algorithm is continually updating the predictions as new data arrives and new associations emerge.

This data-driven approach is far easier to apply and is proving in many cases to be more accurate than the previous logic-based approaches to machine learning. But how does it help a market regulator to know that purchasers of protein powder may also need running shoes?

The simple, and perhaps obvious, answer is that regulators can benefit from understanding the likely outcomes of investor behaviors. The harder truth is that applying machine learning methods is not always simple. Outcomes are often unobservable. Fraud, for example, is what social scientists call a latent variable. You don't see it until it's found. So, it is more challenging for machine learning algorithms to make accurate predictions of possible fraud than shopping decisions, where retailers have access to full transaction histories—that is, complete outcomes for each action. The same is true for translating languages; there is an extremely large corpus of language-pair translations for an algorithm to study and mimic.

This data-driven approach is far easier to apply and is proving in many cases to be more accurate than the previous logic-based approaches to machine learning.

Two years ago, tackling these types of issues at the Commission was still on the horizon. But a lot of progress has been made since then, and machine learning is now integrated into several risk assessment programs—sometimes in ways we didn't then envision. I'm about to share with you some of these experiences. But let me preview now, that while the human brain will continue to lose ground to machines, I don't believe it will ever be decommissioned with respect to the regulation of our financial markets.

The Rise of Machine Learning at the Commission

Let me start by giving you some background on staff's initial foray into the fringes of machine learning, which began shortly after the onset of the financial crisis. That is when we first experimented with simple text analytic methods. This included the use of simple word counts and something called regular expressions, which is a way to machine-identify structured phrases in text-based documents. In one of our first tests, we examined corporate issuer filings to determine whether we could have foreseen some of the risks posed by the rise and use of credit default swaps [CDS] contracts leading up to the financial crisis. We did this by using text analytic methods to machine-measure the frequency with which these contracts were mentioned in filings by corporate issuers. We then examined the trends across time and across corporate issuers to learn whether any signal of impending risk emerged that could have been used as an early warning.

This was a rather crude proof-of-concept. And it didn't work exactly as intended. But it did demonstrate that text analytic methods could be readily applied to SEC filings. Our analysis showed that the first mention of CDS contracts in a Form 10-K was by three banks in 1998. By 2004, more than 100 corporate issuers had mentioned their use. But the big increase in CDS disclosures came in 2009. This was, of course, after the crisis was in full swing. And identification of those issues by the press wasn't much earlier. We analyzed headlines, lead paragraphs, and the full text of articles in major news outlets over the years leading up to the financial crisis and found that robust discussions of CDS topics did not occur until 2008. During that year, we found a ten-fold increase in CDS articles relative to the prior year.

Use of Natural Language Processing

Even if the rise in CDS disclosure trends had predated the crisis, we still would have needed to know to look for it. You can't run an analysis on an emerging risk unless you know that it is emerging. So this limitation provided motivation for the next phase of our natural language processing efforts. This is when we began applying topic modeling methods, such as latent dirichlet allocation[6] to registrant disclosures and other types of text documents. LDA, as the method is also known, measures the probability of words within documents and across documents, in order to define the unique topics that they represent.[7] This is what the data scientist community calls "unsupervised learning." You don't have to know anything about the content of the documents. No subject matter expertise is needed. LDA extracts insights from the documents, themselves using the data-up approach to define common themes—these are the topics—and report on where, and to what extent, they appear in each document.

One of our early topic modeling experiments analyzed the information in the tips, complaints, and referrals (also referred to as TCRs) received by the SEC. The goal was to learn whether we could classify themes directly from the data itself and in a way, that would enable more efficient triaging of TCRs. In another experiment, DERA research staff examined whether machine learning could digitally identify abnormal disclosures by corporate issuers charged with wrongdoing. DERA research staff found that when firms were the subject of financial reporting-related enforcement actions, they made less use of an LDA-identified topic related to performance discussion. This result is consistent with issuers charged with misconduct playing down real risks and concerns in their financial disclosure.[8]

These machine learning methods are now widely applied across the Commission. Topic modeling and other cluster analysis techniques are producing groups of "like" documents and disclosures that identify both common and outlier behaviors among market participants. These analyses can quickly and easily identify latent trends in large amounts of unstructured financial information, some of which may warrant further scrutiny by our enforcement or examination staff.

Moreover, working with our enforcement and examination colleagues, DERA staff is able to leverage knowledge from these collaborations to train the machine learning algorithms. This is referred to as "supervised" machine learning. These algorithms incorporate human direction and judgement to help interpret machine learning outputs. For example, human findings from registrant examinations can be used to "train" an algorithm to understand what pattern, trend, or language in the underlying examination data may indicate possible fraud or misconduct. More broadly, we use unsupervised algorithms to detect patterns and anomalies in the data, using nothing but the data, and then use supervised learning algorithms that allow us to inject our knowledge into the process; that is, supervised learning "maps" the found patterns to specific, user-defined labels. From a fraud detection perspective, these successive algorithms can be applied to new data as it is generated, for example from new SEC filings. When new data arrives, the trained "machine" predicts the current likelihood of possible fraud on the basis of what it learned constituted possible fraud from past data.

An Example of Machine Learning to Detect Potential Investment Adviser Misconduct

Let me give you a concrete example in the context of the investment adviser space. DERA staff currently ingests a large corpus of structured and unstructured data from regulatory filings of investment advisers into a Hadoop computational cluster.[9] This is one of the big data computing environments we use at the Commission, which allows for the distributed processing of very large data files. Then DERA's modeling staff takes over with a two-stage approach. In the first, they apply unsupervised learning algorithms to identify unique or outlier reporting behaviors. This includes both topic modeling and tonality analysis. Topic modeling lets the data define the themes of each filing. Tonality analysis gauges the negativity of a filing by counting the appearance of certain financial terms that have negative connotations.[10] The output from the first stage is then combined with past examination outcomes and fed into a second stage [machine learning] algorithm to predict the presence of idiosyncratic risks at each investment adviser.

The results are impressive. Back-testing analyses show that the algorithms are five times better than random at identifying language in investment adviser regulatory filings that could merit a referral to enforcement. But the results can also generate false positives or, more colloquially, false alarms. In particular, identification of a heightened risk of misconduct or SEC rule violation often can be explained by non-nefarious actions and intent. Because we are aware of this possibility, expert staff knows to critically examine and evaluate the output of these models. But given the demonstrated ability of these machine learning algorithms to guide staff to high risk areas, they are becoming an increasingly important factor in the prioritization of examinations. This enables the deployment of limited resources to areas of the market that are most susceptible to possible violative conduct.

The Role of Big Data

It is important to note that all of these remarkable advancements in machine learning are made possible by, and otherwise depend on, the emergence of big data. The ability of a computer algorithm to generate useful solutions from the data relies on the existence of a lot of data. More data means more opportunity for a computer algorithm to find associations. And as more associations are found, the greater the accuracy of predictions. Just like with humans, the more experience a computer has, the better the results will be.

This trial-and-error approach to computer learning requires an immense amount of computer processing power. It also requires specialized processing power, designed specifically to enhance the performance of machine learning algorithms. The SEC staff is currently using these computing environments and is also planning to scale them up to accommodate future applications that will be on a massive scale. For instance, market exchanges will begin reporting all of their transactions through the Consolidated Audit Trail system, also known as CAT, starting in November of this year.[11] Broker-dealers will follow with their orders and transactions over the subsequent 2 years. This will result in data about market transactions on an unprecedented scale. And, making use of this data will require the analytic methods we are currently developing to reduce the enormous datasets into usable patterns of results, all aimed to help regulators improve market monitoring and surveillance.

We already have some experience with processing big transaction data. Using, again, our big data technologies, such as Hadoop computational clusters that are both on premises and available through cloud services, we currently process massive datasets. One example is the Option Pricing Reporting Authority data, or OPRA data. To help you grasp the size of the OPRA dataset, one day's worth of OPRA data is roughly two terabytes. To illustrate the size of just one terabyte, think of 250 million, double-sided, single-spaced, printed pages. Hence, in this one dataset, we currently process the equivalent of 500 million documents each and every day. And we reduce this information into more usable pieces of information, including market quality and pricing statistics.

However, with respect to big data, it is important to note that *good* data is better than *more* data. There are limits to what a clever machine learning algorithm can do with unstructured or poor-quality data. And there is no substitute for collecting information correctly at the outset. This is on the minds of many of our quant staff. And it marks a fundamental shift in the way the Commission has historically thought about the information it collects. For example, when I started at the Commission almost a decade ago, physical paper documents and filings dominated our securities reporting systems. Much of it came in by mail, and some [documents] still come to us in paper or unstructured format. But this is changing quickly, as we are continuing to modernize the collection and dissemination of timely, machine-readable, structured data to investors.[12]

The staff is also cognizant of the need to continually improve how we collect information from registrants and other market participants, whether it is information on security-based swaps, equity market transactions, corporate issuer financial disclosures, or investment company holdings. We consider many factors, such as the optimal reporting format, frequency of reporting, the most important data elements to include, and whether metadata should be collected by applying a taxonomy of definitions to the data. We consider these factors each and every time the staff makes a recommendation to the Commission for new rules, or amendments to existing rules, that require market participant or SEC-registrant reporting and disclosures.

With respect to big data, it is important to note that good *data is better than* more *data.*

The Future of Artificial Intelligence at the Commission

So, where does this leave the Commission with respect to all of the buzz about artificial intelligence?

At this point in our risk assessment programs, the power of machine learning is clearly evident. We have utilized both machine learning and big data technologies to extract actionable insights from our massive datasets. But computers are not yet conducting compliance examinations on their own. Not even close. Machine learning algorithms may help our examiners by pointing them in the right direction in their identification of possible fraud or misconduct, but machine learning algorithms can't then prepare a referral to enforcement. And algorithms certainly cannot bring an enforcement action. The likelihood of possible fraud or misconduct identified based on a machine learning predication cannot—and should not—be the sole basis of an enforcement action. Corroborative evidence in the form of witness testimony or documentary evidence, for example, is still needed. Put more simply, human interaction is required at all stages of our risk assessment programs.

So, while the major advances in machine learning have and will continue to improve our ability to monitor markets for possible misconduct, it is premature to think of AI as our next market regulator. The science is not yet there. The most advanced machine learning technologies used today can mimic human behavior in unprecedented ways, but higher-level reasoning by machines remains an elusive hope.

I don't mean for these remarks to be in any way disparaging of the significant advancements computer science has brought to market assessment activities, which have historically been the domain of the social sciences. And this does not mean that the staff won't continue to follow the groundbreaking efforts that are moving us closer to AI. To the contrary, I can see the evolving science of AI enabling us to develop systems capable of aggregating data, assessing whether certain Federal securities laws or regulations may have been violated, creating detailed reports with justifications supporting the identified market risk, and forwarding the report outlining that possible risk or possible violation to Enforcement or OCIE staff for further evaluation and corroboration.

It is not clear how long such a program will take to develop. But it will be sooner than I would have imagined 2 years ago. And regardless of when, I expect that human expertise and evaluations always will be required to make use of the information in the regulation of our capital markets. For it does not matter whether the technology detects possible fraud, or misconduct, or whether we train the machine to assess the effectiveness of our regulations—it is SEC staff who uses the results of the technologies to inform our enforcement, compliance, and regulatory framework.

ENDNOTES:

[1] SEC Speech, *Has Big Data Made Us Lazy?* Midwest Region Meeting of the American Accounting Association, October 2016; *see* https://www.sec.gov/news/speech/bauguess-american-accounting-association-102116.html.

[2] Bauguess, Scott W., *The Hope and Limitations of Machine Learning in Market Risk Assessment*; U.S. Securities and Exchange Commission; March 6, 2015; *see* http://cfe.columbia.edu/files/seasieor/center-financial-engineering/presentations/MachineLearningSECRiskAssessment030615public.pdf.

[3] Arthur Samuel, 1959, *Some Studies in Machine Learning Using the Game of Checkers*; IBM Journal 3, (3): 210-229.

[4] *See* https://en.wikipedia.org/wiki/AlphaGo_versus_Lee Sedol.

[5] For an excellent layperson discussion on how machine learning is enabling all of this, *see*, *e.g.,* Gideon Lewis- Kraus, *The New York Times*, December 14, 2016, *The Great A.I. Awakening*.

[6] A term used in probability and statistics, *see here* https://en.wikipedia.org/wiki/Dirichlet_distribution.

[7] *See* http://www.jmlr.org/papers/volume3/blei03a/blei03a.pdf.

[8] *See*, G. Hoberg and C. Lewis, 2017, *Do Fraudulent Firms Produce Abnormal Disclosure?* Journal of Corporate Finance, Vol. 43, pp. 58-85.

[9] A Hadoop computational cluster is a special group of servers or other resources that are designed specifically for storing and analyzing huge amounts of unstructured data; *See* http://searchbusinessanalytics.techtarget.com/definition/Hadoop-cluster.

[10] Loughran, Tim, and McDonald, Bill, 2011; *When is a Liability Not a Liability*? *Textual Analysis, Dictionaries and 10-Ks*. Journal of Finance 66: 35-65.

[11] *See, e.g.,* https://www.sec.gov/divisions/marketreg/rule613-info.htm.

[12] Securities and Exchange Commission Strategic Plan Fiscal years 2014-2018, https://www.sec.gov/about/sec-strategic-plan-2014-2018.pdf.

SEC/SRO UPDATE: NASDAQ IS ADVOCATING FOR U.S. PUBLIC MARKET REFORM; NASDAQ CONTINUES TO SOLICIT COMMENTS ON SHAREHOLDER APPROVAL RULES

By Yelena M. Barychev & Melissa Palat Murawsky

Yelena M. Barychev and Melissa Palat Murawsky are Partners at Blank Rome LLP (www.blankrome.com). Ms. Barychev and Ms. Murawsky advise public companies on private and public offerings of securities, as well as on mergers and acquisitions and other corporate transactions. They also advise public companies on corporate and securities law issues, including executive compensation and corporate governance matters. The views expressed herein are those of the authors and not necessarily those of Blank Rome LLP or any of its clients. Contact: barychev@blankrome.com or murawsky@blankrome.com.

Nasdaq Is Advocating for U.S. Public Market Reform

In May, Nasdaq published a report titled, The Promise of Market Reform: Reigniting America's Economic Engine.[1] The report stems from Nasdaq's concern about the state of U.S. pubic markets, which have become "more complex and costly for issuers, particularly for publicly-listed small- and medium-growth companies and for private companies that might consider public offerings."

The report emphasizes that "companies increasingly question whether the benefits of public ownership are worth the burdens" and warns that if such burdens are not addressed, it "could ultimately represent an existential threat to our markets" as "a growing number of companies have been choosing to remain private—and some public companies are reversing course and going private."

The report also outlines consequences of a diminishing public capital market: job creation and economic growth could decline; main street investors could have a lesser chance to share in wealth creation; American companies could increasingly consider foreign public markets; and top international companies might choose not to list in the United States. But Nasdaq's report does not just create an alarm, it sets forth a blueprint for "critically-needed reforms.," in

The report identifies the following three specific problems and offers concrete solutions in these areas:

1. a complex patchwork of regulation disincentivizes market participation and creates the need to reconstruct the regulatory framework;
2. a one-size-fits-all market structure deprives companies of the benefits they need to participate in public markets (particularly for small- and medium-growth companies), which can be fixed by modernizing the market structure; *and*
3. a culture in the investment community and in the mainstream media that values short-term returns should be changed to promote long-termism.

Nasdaq suggests that the reconstruction of the regulatory framework would involve: *i*) reforming the proxy proposal process; *ii*) reducing the burden of corporate disclosure; *iii*) rolling back politically-motivated disclosure requirements; *iv*) reducing the burden of meritless class action lawsuits; and *v*) a tax reform to incentivize long-term investing.

For example, in order to reform the proxy proposal process, Nasdaq suggests the following approach:

- raise the minimum ownership amount and holding period from the current low threshold requirements of holding at least $2,000 of company stock for one year in order to submit a proposal that can be included for a shareholder vote in the company's proxy;

- streamline the Securities and Exchange Commission's process for removing nuisance proxy proposals from proxies; *and*

- create transparency and fairness in the proxy advisory industry.

In order to reduce the burden of corporate disclosure, Nasdaq proposes to:

- offer flexibility on quarterly reporting and allow companies to provide reports semiannually instead of filing Quarterly Reports on Form 10-Q (while keeping Annual Reports on Form 10-K);

- reconsider an XBRL tagging requirement; *and*

- expand and harmonize classifications for disclosure relief by raising the revenue cap to qualify as an emerging growth company from the current $1 billion to $1.5 billion and deleting the current phase-out of five years after the initial public offering, and harmonizing the definitions of a smaller reporting company, non-accelerated filer and emerging growth company.

The report suggests promoting long-termism by: *i*) supporting dual class structure; *ii*) creating disclosure requirements applicable to short positions; and *iii*) addressing concerns regarding activist investors using tactics that coerce companies into short-term actions to the detriment of long-term planning.

Nasdaq Continues to Solicit Comments on Shareholder Approval Rules

On June 14, Nasdaq released a *Solicitation of Comments by the Nasdaq Listing and Hearing Review Council About the Definition of Market Value for Purposes of Shareholder Approval Rules*.[2] The Listing Council is an independent advisory committee appointed by the Board of Directors of the Nasdaq Stock Market, and its mission is to review the application of Nasdaq's listing rules and suggest new rules for consideration by the Board.

Nasdaq has previously worked with the Listing Council to solicit comments on changes to the shareholder approval rules.[3] Although no determination has been made that changes to these rules are necessary, Nasdaq continues to evaluate them.

In the June 2017 solicitation of comments, the focus is on Listing Rule 5635(d) that requires a Nasdaq-listed company to obtain shareholder approval prior to issuing common stock or securities convertible into or exercisable for common stock equal to 20% or more of the shares or voting power outstanding at a price less than the greater of the book value or market value in connection with a private placement transaction. Listing Rule 5005 defines "market value" as the closing bid price.

Under the proposed Rule 5635(d), shareholder approval will be required for private placements, involving the issuance of common stock, or securities convertible into or exercisable for common stock that equals 20% or more of common stock or voting power outstanding before the issuance and is:

- at a price less than the average closing price of the common stock (as reflected on Nasdaq.com) for the five trading days immediately preceding the signing of the binding agreement for the issuance; or

- not approved either by: *i*) Independent Directors constituting a majority of the Board's Independent Directors in a vote in which only Independent Directors participate; or *ii*) a committee comprised solely of Independent Directors (for example, an independent pricing or financing committee).

Nasdaq and the Listing Council believe that a change from a closing bid price to a five-day average of closing prices will enhance transparency because "bid price may not always be transparent to companies and investors and does not always reflect an actual price at which a security has traded." The proposed rule also provides that

> any transaction of more than 20% of the company's shares outstanding will be approved by either a committee of independent directors (as defined in Listing Rule 5605(a)(2)) or a majority of the independent directors on the board, unless it is approved by the company's shareholders.

Nasdaq and the Listing Council are seeking comments on the foregoing changes to Rule 5635(d) until July 31, 2017. If Nasdaq determines to proceed with the proposed rule changes upon the review of comments, such proposal will be subject to the Securities and Exchange Commission's review and approval process.

ENDNOTES:

[1] The Promise of Market Reform: Reigniting America's Economic Engine; Nasdaq (May 2017); available at http://business.nasdaq.com/media/Nasdaq%20Blueprint%20to%20Revitalize%20Capital%20Markets_tcm5044-43175.pdf.

[2] *Solicitation of Comments by the Nasdaq Listing and Hearing Review Council About the Definition of Market Value for Purposes of Shareholder Approval Rules;* Nasdaq (June 14, 2017); *available at* https://listingcenter.nasdaq.com/assets/Shareholder%20Approval%20Comment%20Solicitation%20June%2014%202017.pdf.

[3] *See* https://listingcenter.nasdaq.com/assets/Shareholder%20Approval%20Comment%20Solicitation.pdf.

FROM THE EDITOR

Are Law Firms Doing Enough to Combat Cybersecurity Threats?

NEW YORK—The growing and constant threat of cybersecurity breaches is something law firms need to address urgently and forcefully; but increasingly, they are falling behind on investment and commitment to create and maintain adequate privacy and data protection, according to several legal and cybersecurity experts.

At least those were some of the conclusions of a recent panel on cybersecurity entitled, "Rumor of War: Regulation, Revelations & the State of Cybersecurity in 2017" that *Wall Street Lawyer* was able to observe.

"The threat of cybersecurity breaches is the most significant threat this country, its business and its law firms face," said panelist Timothy Murphy, President of Thomson Reuters Special Services, adding that in many cases, companies and law firms are outgunned by the sophistication of some hostile cyber-actors and are hamstrung by using outdated protections and inadequate resources. "Law firms, especially because of the data they hold, have to take this threat seriously," Murphy urged. "They have to get engaged and stay on top of it."

The stakes for law firms are quite high, as their valuable troves of client data make them prime targets. Regulators too have taken notice, urging law firms to do more—and disclose more—about how they are fighting cyberthreats. "Law firms are holding some of the most sensitive data you can have, and that should make them realize how important it is to invest in adequate security," said panelist James L. Quinn, Head of Security Architecture at Infotecs Americas.

Of course, there are certain hurdles unique to law firms, such as the partnership hierarchy, that makes addressing and funding non-income producing initiatives such as cybersecurity and data protection more difficult than in other enterprises, said another panelist, Nicholas Barone, Director and Co-Head of the Cybersecurity Practice at Eisner Amper. "One of the main challenges at law firms is getting cybersecurity paid for by the partners," noted Barone, adding that this challenge carries with it issues of determining allocations of costs, encouraging firm-wide training, and measuring levels of adoption by partners and staff.

So, what's a law firm to do?

One thing is for firms to re-examine their current cyber-plan—or even determine if they have one—because the chaotic time following a security breach is not the time to try to make far-reaching decisions. Clearly, such a situation shows the vital importance of pre-planning, the panel agreed. "You have to know what you're going to do *before* the breach," said Infotecs Americas' Quinn. "It's very difficult to make good decisions in a reactive mode."

Equally clearly, the hugely impactful issue of cybersecurity and the dangers of data breaches at law firms and their clients is not going away any time soon—*Wall Street Lawyer* will continue to keep an eye on it.

In this issue. . . Speaking of cybersecurity, the July issue of *Wall Street Lawyer* features authors Yafit Cohn and Karen Hsu Kelley of Simpson Thacher & Bartlett posing 10 questions every corporate board should be asking about cyber risks.

—Gregg Wirth, Managing Editor

EDITORIAL BOARD

Wall Street LAWYER

West LegalEdcenter
610 Opperman Drive
Eagan, MN 55123

Wall Street LAWYER

West LegalEdcenter
610 Opperman Drive, Eagan, MN 55123
Phone: 1-800-344-5009 or 1-800-328-4880
Fax: 1-800-340-9378
Web: http://westlegaledcenter.com

THOMSON REUTERS

YES! Rush me ***Wall Street Lawyer*** and enter my one-year trial subscription (12 issues) at the price of $1,092.00. After 30 days, I will honor your invoice or cancel without obligation.

Name ______________________

Company ______________________

Street Address ______________________

City/State/Zip ______________________

Phone ______________________

Fax ______________________

E-mail ______________________

METHOD OF PAYMENT

□ BILL ME

□ VISA □ MASTERCARD □ AMEX

Account # ______________________

Exp. Date ______________________

Signature ______________________

Postage charged separately. All prices are subject to sales tax where applicable.