the Corporate Governance advisor

November/December 2017 • Volume 25, Number 6

CYBERSECURITY

'Is That a Target on Your Back?': Board Cybersecurity Oversight Duty After the Target Settlement

By Stewart Landefeld, Lou Mejia, Allison Handy, and Todd Hinnen

In the wake of the onerous settlement imposed on Target Corporation arising from its data breach, the cyberattack against Equifax and its aftermath, the U.S. Securities and Exchange Commission's (SEC's) own questionable handling of its data breach,[1] and ongoing data breach lawsuits against directors, public company directors are rightfully concerned about their cybersecurity oversight duty.

To fulfill their duties of care and loyalty, state laws require boards to ensure the implementation of reporting and information systems, and to monitor and oversee these systems. As long as directors fulfill these duties, directors reduce the risk of personal liability in the wake of a data breach. Nevertheless, given the continuous rise of

Continued on page 2

Stewart M. Landefeld and Luis R. Mejia are Partners, Allison C. Handy is Counsel and Todd M. Hinnen is a Partner at Perkins Coie LLP. *They gratefully acknowledge the substantial contributions from colleague June Wang and the well-prepared interviews of Paula Rosput Reynolds, Barney Harford, Paulette R. Dodson, Esq., and Christopher L. Beers, Esq.*

Wolters Kluwer

CONTENTS

cyberattacks against companies, directors know that stakes are high and are looking for guidance on how to best protect their companies. The resulting fallout from recent data breaches provides real-life case studies that can help boards develop technical literacy around cybersecurity and best practices for their oversight responsibility so that they can work with management to identify new risks and avoid pitfalls.

The most recent and visible example of the crushing burden on public companies that results from a cybersecurity breach is the settlement that 47 states and the District of Columbia (D.C.) imposed on Target in May 2017, as well as Nationwide Mutual Insurance Company's settlement with 32 states and D.C. in August 2017. Directors should view Target (and Nationwide) in the appropriate context for their own circumstances.

Rather than viewing the settlement terms as new "best practices," we suggest the settlements be viewed as just two examples among many in assessing what applies to a specific corporate setting. There is no one-size-fits-all model for cybersecurity, as any company's program will be informed by its size and resources, the type of data it maintains, and applicable regulations. In addition, regulators often impose remediation steps or undertakings on a company in enforcement proceedings that are neither required by law nor appropriate for wide adoption.

Drawing on a review of recent regulatory actions, court decisions, and fallout from high-profile data breaches, as well as interviews with directors and senior executives who advise boards, we have developed steps that a board can use to find the right path to oversight of cybersecurity risks. As one director counseled, directors should lean in to "a topic that is being talked about in the board room," and for which "the stakes are being raised."

A Moving Target: Regulations, Guidance and Settlements

Companies are subject to new and evolving cybersecurity-related regulatory requirements and other standards that vary by industry and jurisdiction. Applicable requirements might include industry or regulatory cybersecurity program requirements and breach notification obligations.

Federal Guidance: Continuing Call for Security

Among others, the U.S. Federal Trade Commission (FTC) continues to issue guidance advising companies within its jurisdiction to develop a thorough, risk-based data security program with rigorous controls to ensure secure development, layered network defense, and diligent review of third-party vendors and service providers. The SEC's guidance for broker dealers and investment advisors is similar. Companies subject to the enforcement jurisdiction of these agencies should benchmark their programs against this guidance to make sure their programs fully comply.

To date, the SEC has not brought a cybersecurity-related enforcement action against a public company. Although the SEC's new enforcement directors have described cybersecurity as a major enforcement priority, the new investigations appear to be focused on parties engaged in the criminal cyberattacks, rather than the entities attacked.[2]

For SEC-registered public companies, the 2011 guidance from the SEC's Division of Corporation Finance remains the standard for disclosure obligations relating to cybersecurity risks and cyber incidents.[3] Recent comments from new SEC Chairman Jay Clayton, as well as the fallout from the SEC's own recent data breach, indicate the SEC may proceed with caution on cybersecurity as it relates to public companies. Before the SEC's data breach was disclosed, consistent with the 2011 guidance, Clayton said companies have an obligation to disclose "material information."[4]

When data breaches occur, "we need to be cautious about punishing responsible companies who nevertheless are victims of sophisticated cyber penetrations."[5] In Clayton's view,

"cyberspace has many bad actors, including nation states that have resources far beyond anything a single company can muster."[6] We can expect to see a "broad perspective" and "proportionality" from the SEC in the area of cybersecurity disclosure enforcement.[7] Although Clayton believes public companies should provide more and better disclosure, that wish is still within the framework of materiality, as made clear in the SEC's own 2011 guidance.

State Attorney Generals: New Cops on the Beat

State regulators have become actively involved in enforcement actions relating to cyber-attacks, most recently with respect to Target in May 2017 and Nationwide in August 2017.

Prior to the cyberattack in 2013, Target had spent $1.6 million on an anti-malware system, but apparently did not implement a feature that would automatically eliminate malware.[8] Using the compromised credentials of an HVAC vendor working for Target, hackers had uploaded several versions of malware. Several days after the malware had been installed—hackers, believed to be foreign, began to download data that had been taken from card swipes at close to 1,800 stores. Target was finally alerted to the theft by federal law enforcement officials, and by the time that Target eradicated the malware, almost two weeks later, the hackers had stolen more than 40 million credit card numbers. Target faced numerous lawsuits and stated in its 2016 annual report that its cumulative expenses to that point totaled $202 million, net of insurance recoveries. The attorneys general of almost every state pursued Target in the aftermath of the data breach. The May 2017 settlement contained numerous requirements to be met by Target. The following are the key elements of the settlement:[9]

- Target must make an $18.5 million monetary payment to be shared by the states.
- Target must develop, implement, and maintain a comprehensive information security program, and provide it in writing to the states.
- Target will employ an executive or officer who is responsible for executing the program, once developed and approved.
- Target must retain an independent, qualified third party to conduct a comprehensive security assessment, and provide a report on the progress and implementation to the states.
- Target is required to maintain and support software on its network and to maintain appropriate encryption policies, particularly as it pertains to cardholder and personal information data.
- Target will segment its cardholder data from the rest of its computer network and undertake steps to control access to its network, including implementing password rotation policies and two-factor authentication for certain accounts.
- Target must commit to devoting the appropriate resources and support to the information security program.

The terms did not mandate any board-specific duties or responsibilities. For example, the terms did not require Target to implement a specific type or level of board-level oversight, for example, by use of a specific cybersecurity oversight committee. However, consistent with existing law on a board's oversight duty, the Target board will have an obligation to monitor the implementation and progress and receive regular reports on the various steps.

Nationwide also recently reached a settlement with 33 states over its 2012 data breach. Due to the alleged failure by Nationwide to apply a critical security patch, hackers stole highly sensitive information (such as Social Security numbers, driver's license data, and credit-scoring information) of more than one million Nationwide customers and people seeking insurance quotes.[10]

The settlement required Nationwide to take specific steps to update its security practices and ensure timely application of patches to its software, including:

(1) Hiring a technology officer responsible for monitoring and managing software and application security updates;

(2) Conducting regular inventories of system patches used to maintain consumers' personal information; and

(3) Performing internal assessments of its patch management practices and hiring a third-party provider to perform an annual audit of its personal information collection and maintenance practices.

Like Target's settlement, the terms did not mandate any board-specific duties or responsibilities.[11]

The Target and Nationwide settlements were clearly tailored to those companies' specific challenges and incursions. Thus, we suggest that the elements of the settlements be viewed as general guidance to review with a board or committee as it considers its company cybersecurity program, not as something required to be adopted as a best practice. Regulators often impose undertakings and remedial steps not required or mandated by existing law.

Board Oversight Responsibility: Reasonableness, Not Perfection

State corporate law governing a board's responsibility to oversee cybersecurity risks remains favorable to directors. A board's oversight responsibility has been developed under Delaware law arising from and building on the foundational fiduciary duties of directors, the duty of care, and the duty of loyalty, beginning with *In re Caremark International Inc. Derivative Litigation*, and as clarified in *Stone ex rel. AmSouth Bancorporation v. Ritter*.[12] Director oversight liability occurs when the directors utterly fail to implement any reporting or information system or controls or, having implemented such a system of controls, consciously fail to monitor or oversee its operations, thus disabling themselves from being informed of risks or problems requiring their attention. In either case, imposition of liability requires a showing that the directors *knew* that they were not discharging their fiduciary obligations.[13]

Litigation since 2015 has further explored the board oversight responsibility described in *Caremark* and *Stone*. In *Reiter ex rel. Capital One Financial Corporation v. Fairbank et al.*, the Delaware Court of Chancery dismissed claims of personal liability against the Capital One board, finding they did not consciously disregard their responsibility to oversee Capital One's compliance with the Bank Secrecy Act and other anti-money laundering laws.[14]

Plaintiffs alleged the board failed to act after receiving reports that raised red flags about compliance. Although the reports described the company's heightened compliance risk, they also simultaneously explained to the directors in considerable detail on a regular basis the initiatives management was taking to address those problems and to ameliorate the compliance risk. Thus, the board did not *consciously* fail to monitor or oversee compliance. As the court stated, "good faith, not a good result, is what is required of the board."[15]

Despite "an incredibly high hurdle" to show personal liability of directors, plaintiffs have continued to bring claims against boards for failure of oversight in some of the major cyberattacks in recent years.[16] These actions have not gone well for plaintiffs, however. For example, cases against the boards of Home Depot and Target have been dismissed.

In a case arising out of the 2014 cyberattack on Home Depot, plaintiffs alleged the board failed to exercise their oversight duties by disbanding the infrastructure committee responsible for data security two years prior to the breach. Plaintiffs also alleged the board failed to implement adequate cybersecurity measures called for by the Payment Card Industry Data Security Standards (PCI DSS).[17]

The court found that plaintiffs failed to show the board consciously failed to act in the face of a known duty to act.[18] Although the board had

disbanded the infrastructure committee prior to the breach, it transferred its data security responsibilities to the audit committee. The failure to amend the audit committee's charter to reflect its new authority was irrelevant, as the audit committee received regular reports from management on the state of Home Depot's data security, and the board in turn received briefings from both management and the audit committee.[19] Thus, the board fulfilled its duty of loyalty to ensure that a reasonable system of reporting existed.

Plaintiffs' allegations that the board's plan was not good enough and moved too slowly were insufficient. As the court stated, directors violate their duty of loyalty only "if they knowingly and *completely* failed to undertake their responsibilities," and as long as the board "pursued *any* course of action that was reasonable, they would not have violated their duty of loyalty."[20] Although implementation of the plan was probably too slow and the plan probably would not have fixed all the problems, the board did not act in bad faith. Decisions by the board "must be reasonable, not perfect," and a "wrong decision in response to red flags…is not enough to plead bad faith."[21]

In a private action arising out of the Target data breach, plaintiffs fared no better. Shareholders in derivative actions alleged that the board breached their fiduciary duties by failing to take sufficient steps to protect the company from a breach and its consequences.[22] Following Minnesota law, the board formed a Special Litigation Committee (Target SLC) to investigate and evaluate the claims and concluded that it was not in Target's best interests to pursue the claims.[23] The court then dismissed all shareholder actions.[24]

The Target SLC followed the oversight liability standards of *Caremark* and *Stone* in its evaluation of the plaintiffs' claims.[25] The Target SLC listed nearly 40 factors that it weighed and balanced in reaching its conclusions, among them factors directly related to the conduct of the board: [26]

(1) The applicability of the business judgment rule protecting reasonably prudent, good faith business decisions;

(2) Management's reports to the board's audit and corporate responsibility committees covering Target's data security program, including compliance efforts and assessments of Target's data security and privacy programs;

(3) Reports made to Target's board that it had been assessed as PCI DSS compliant, including to the audit committee;

(4) Reports from Target's auditor to the audit committee that prior to the breach, there were no significant deficiencies or material weaknesses in the information technology general controls;

(5) The rights of directors to reasonably rely on the information and opinions of others; and

(6) The reasonableness of judgments that directors made concerning whether and when to address capital and employment needs related to data security risks.

The factors reflect a board that pursued a reasonable course of action, and certainly not a board that completely failed to undertake their responsibilities.

How Are Best Practices for Board Oversight of Cybersecurity Evolving?

Recent case law has demonstrated that there is an extremely high bar for imposition of liability on directors for failure to discharge the duty of oversight; however, many boards are concerned that they are not doing enough to address cybersecurity risks. Through interviews with directors and senior executives who advise boards, we have developed steps that a board can use to find the right path to oversight of cybersecurity risks. What a cybersecurity program looks like will vary from company to company, depending on factors such as risk profile, resources, and applicable regulations. Regardless of the type of cybersecurity program, certain oversight practices can help a board ensure that management has implemented an appropriate risk-adjusted

cybersecurity program and is prepared to deal with the aftermath in case of a data breach.

(1) Directors Should Educate Themselves on Current Technology Issues and Actively Inquire into Appropriate Cybersecurity Programs. A director oversees, rather than manages, a cybersecurity plan; the board relies on its senior executive team to develop and implement the program. For a director, oversight can often be best achieved through organized and active inquiry. Thoughtful questions can help a director to determine if a company's cybersecurity program is appropriately calibrated to the company's cyber risk profile and meets applicable industry standards and complies with any applicable regulatory requirements.

Most boards do not need to add a "cybersecurity expert" as a director, but every board needs every director or committee member to be personally conversant with, and comfortable asking questions about, the technology used by the company and its customers. General familiarity with information technology is an asset for any director.

Most boards, particularly those outside the higher risk retail and financial institution industries, should be able to rely on internal and external experts and not need to add a director with that special expertise. Just as an audit committee member must have financial sophistication, but not necessarily be a CPA, a director overseeing cybersecurity should have a high level understanding of what cybersecurity is, but not necessarily be able to fill in for the chief information security officer.

A key recommendation that we heard from other directors in our interviews was for board members to "lean in" to this issue. Although the board's role is oversight and not program design or implementation, it is clear in the current environment that no company is immune from cybersecurity concerns. In order to best help the companies that they serve, directors need to gain a broad understanding of cybersecurity practices so that they can probe internal and external experts with strategic questions and understand the company's strengths and weaknesses.

(2) Does a Committee or Board Take Responsibility for Oversight? No Single "Best Practice." There is no single best practice for what committee should oversee cybersecurity. A committee is generally the right home for close scrutiny. However, a small board may find it efficient to have the board itself retain the responsibility for oversight, if it can devote the appropriate time and attention. Not even the Target settlement sought to impose a "right" committee or board procedure.[27] A 2016 study indicated that 54 percent of all companies surveyed allocate cybersecurity issues to the audit committee, but 55 percent of financial services companies have a risk committee or information technology committee that oversees cybersecurity.[28]

The greater prevalence of these specialized committees for financial institutions has been an ongoing trend, as these companies have significant exposure to cybersecurity risks because of the type of data that they maintain. For companies with higher cybersecurity risk profiles, separating this risk oversight from already significant audit committee burdens commonly benefits board operations. Although the survey does not specify industry for other companies, 18 percent of all companies surveyed use a risk, information technology, or cybersecurity committee, up from 12 percent of companies surveyed in the equivalent study from 2014.[29] This may reflect an increase among retail companies and others with higher cybersecurity risk profiles shifting the burden of oversight away from their audit committees.

Target provides one such example of this shift. According to Target's 2015 proxy statement, the company embarked on a comprehensive review of risk oversight during 2014.[30] As a result of this review, Target clarified and

enhanced certain board practices, and reallocated and clarified risk oversight responsibilities, "elevating the risk oversight role of the Corporate Risk & Responsibility Committee (formerly known as the Corporate Responsibility Committee)."

The 2015 proxy statement indicates that the Corporate Risk and Responsibility Committee oversees "operating, business, compliance and reputational risks, including information security and technology." (Prior to this 2015 update, Target's proxy did not specifically address the board's oversight of information security risks, so it is unclear whether oversight of this matter rested primarily with the board, the audit committee, or the corporate responsibility committee.) In light of Target's frontline experience with a data breach, other companies with similar risk profiles might consider this committee structure in a review of their own practices.

(3) Regular "Keep Your Finger on the Pulse" Board Reports. The board or an appropriate committee should schedule periodic reports by the head of cybersecurity and possibly outside consultants on the board's, or applicable committee's, annual calendar. The frequency of a report will depend on the company's cybersecurity risk profile and should be reviewed and agreed to by the board. Periodic reports to a committee may be appropriate, with a board briefing on an annual basis.

Similar to a surgeon checking a list at each stage of a procedure, some directors may find it helpful in their oversight to have a standard agenda or checklist for cybersecurity that the board and internal experts use, and update, at each cybersecurity review. A cybersecurity report checklist could include the following:

- Discuss the company's cybersecurity risk profile, including any updates due to regulatory changes, shifts in the company's operations, or emerging threats. Directors should be sure that they understand what kind of data the company maintains and key practices to protect such data.

- Provide an evaluation of the current cybersecurity program in light of the company's current risk level. Directors should probe whether the budget and team remain appropriate, and they need to develop a level of trust with both the internal head of cybersecurity and any outside evaluator to ensure they are getting honest answers to such questions.

- Discuss any breaches, of any level, that happened during the most recent period. Like an audit committee reviewing a quarterly whistleblower hotline report, this step can help inform the board of how the cybersecurity program is working. Note that a report of no breaches or breach attempts might be more concerning (indicating that management is unable to detect such activity) than a report of three thwarted attempts.

- Provide results of internal or external testing of data security, including simulated phishing and spear phishing attempts, "white hat" hacker breaches, or other industry-specific audits.

- Discuss employee and director training efforts, including results of recent simulations or actual breaches. Ask about risks related to vendors.

- Probe how the cybersecurity program fits with the company's overall risk management system, including crisis response preparation.

(4) Third Party Consultants. Depending on available internal resources, a company or board may look to third-party consultants for one or more aspects of cybersecurity. First, many businesses have strong IT teams but rely on outside service providers to bring special cybersecurity expertise, or to do "white hat" probing of cyber defenses.

An audit committee or board could request annual updates from these outside service providers, or review the reports that they provide to management.

Second, sometimes a director will find it is easier to ask "dumb questions" of an outside advisor than an internal officer, whom the board is to some extent also evaluating.

Finally, an outside service provider can provide an objective, specialized audit of whether the company is truly following appropriate cybersecurity best practices and whether internal controls and processes are up-to-date with the latest developments in the industry.

(5) Oversee Appropriate Crisis Management Preparation. When a major cybersecurity breach occurs, a company must manage the substance of the breach itself and the sense of crisis that can immediately envelop the company. A board, in assessing the cybersecurity plan, should also be asking about crisis readiness. What sort of simulation exercises is management engaging in? Who is the core team? How have the exercises gone?

The senior team can prepare for crisis management in part through participation in crisis simulation or "tabletop" exercises, followed by self-evaluations of the results. Directors should be aware of these exercises and probe the lessons learned, including understanding who is on the core team and whether they have considered third-party participants, such as public relations firms and legal experts. But the board's role remains oversight and not management. Directors should satisfy themselves that the company is prepared for a crisis, but realize that they will not personally be the ones to manage the crisis.

(6) Board Vulnerability. For some companies, a point of great vulnerability can be communicating with the directors themselves. Internal technology staff may be deferential to the board and not want to inconvenience the directors; directors may be years behind in their own training and uses of technology. And the company may allow some communications outside the company's secure corporate email and board portals. Directors need to realize the importance of their own role in cybersecurity, including being subject to testing like all employees, and willingly adopting best practices for email and portal security.

Notes

1. *See, e.g.*, Tatyana Shumsky, "Hack Response Opens SEC to Criticism," *Wall Street J.*, Sept. 21, 2017, available at *https://www.wsj.com/articles/hack-response-opens-sec-to-criticism-1506024730,* last accessed Oct. 11, 2017.

2. Sarah N. Lynch, "New SEC enforcement chiefs see cyber crime as biggest market threat," *Reuters*, June 8, 2017, available at *https://www.reuters.com/article/us-usa-sec-enforcement-exclusive/exclusive-new-sec-enforcement-chiefs-see-cyber-crime-as-biggest-market-threat-idUSKBN18Z2TX,* last accessed Oct. 11, 2017.

3. Div. of Corp. Finance, U.S. Sec. & Exch. Comm'n, CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011), available at *https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm,* last accessed Oct. 11, 2017; Jay Clayton, Chairman, U.S. Sec. & Exch. Comm'n, Statement on Cybersecurity (Sept. 20, 2017), available at *https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20,* last accessed Oct. 11, 2017.

4. Jay Clayton, Chairman, U.S. Sec. & Exch. Comm'n, Remarks at the Economic Club of New York (July 12, 2017), available at *https://www.sec.gov/news/speech/remarks-economic-club-new-york,* last accessed Oct. 11, 2017.

5. *Id.*

6. *Id.*

7. *Id.*

8. Michael Riley *et al*., "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," *Bloomberg*, Mar. 17, 2014, available at *https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data,* last accessed Oct. 11, 2017 (Subscription required).

9. *In re Investigation of Target Corp*., Att'y Gen. of N.Y., Bureau of Internet & Tech., Assurance No. 17-094 (May 15, 2017), available at *https://ag.ny.gov/sites/default/files/nyag_target_settlement.pdf,* last accessed Oct. 11, 2017 [hereinafter *Target Settlement*].

10. Cara Salvatore, "Nationwide Pays $5.5M To AGs Over Data Breach," *Law360*, Aug. 9, 2017, available at

https://www.law360.com/articles/952737/nationwide-pays-5-5m-to-ags-over-data-breach, last accessed Oct. 11, 2017 (subscription required).

11. *In re Nationwide Mutual Insurance Co. and Allied Property & Casualty Insurance Co.*, Att'y Gen. of N.Y., Assurance of Voluntary Compliance (Aug. 9, 2017), available at *https://www.courthousenews.com/wp-content/uploads/2017/08/Nationwide-Settlement.pdf.*

12. *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996); *Stone ex rel. AmSouth Bancorporation v. Ritter*, 911 A.2d 362 (Del. 2006).

13. *Stone*, 911 A.2d at 370.

14. *Reiter ex rel. Capital One Fin. Corp. v. Fairbank et al.*, No. 11693-CB, 2016 WL 6081823 (Del. Ch. Oct. 18, 2016).

15. *Id.* at *14 (citation omitted).

16. *In re The Home Depot, Inc. S'holder Derivative Litig.*, 223 F. Supp. 3d. 1317, 1325 (N.D. Ga. 2016).

17. *Id.* at 1321–22.

18. *Id.* at 1327.

19. *Id.* at 1325–26.

20. *Id.* at 1326.

21. *Id.* at 1327 (citation omitted).

22. *In re Target Corp. S'holder Derivative Litig.*, No. 0:14-cv-00203 (PAM/JJK) (D. Minn. 2016).

23. *Id.*, Dkt. No. 62-2, Ex. B at 91 (Target Corporation Report of the Special Litigation Committee dated Mar. 30, 2016), available at *http://www.dandodiary.com/wp-content/uploads/sites/265/2016/07/Target-SLC-Report.pdf,* last accessed Oct. 11, 2017 [hereinafter *SLC Report*].

24. *Id.*, Dkt. No. 88 (Order Granting Motion to Dismiss dated July 7, 2016).

25. *SLC Report*, *supra* n.23 at 82–84.

26. *Id.* at 88–90.

27. *Target Settlement*, *supra* n.9.

28. Deloitte LLP, Center for Board Effectiveness and Society for Corporate Governance, *2016 Board Practices Report: A transparent look at the work of the board* (10th ed. 2017), available at *https://www2.deloitte.com/content/dam/Deloitte/us/Documents/center-for-board-effectiveness/us-cbe-2016-board-practices-report-a-transparent-look-at-the-work-of-the-board.pdf,* last accessed Oct. 11, 2017.

29. Deloitte LLP, Center for Corporate Governance and Society of Corporate Secretaries & Governance Professionals, *2014 Board Practices Report: Perspectives from the boardroom* (2014), available at *https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-2014-board-practices-report-final-9274051-12122014.pdf,* last accessed Oct. 11, 2017.

30. Target Corp., 2015 Proxy Statement (filed Apr. 27, 2015), available at *https://www.sec.gov/Archives/edgar/data/27419/000130817915000165/ltgt2015_def14a.htm,* last accessed Oct. 11, 2017.

Corporate Monitors: How to Avoid One If Possible and How to Deal With One If You Must

By John F. Wood

Over the past 15 years, independent compliance monitors have become increasingly common in Department of Justice (DOJ) resolutions of enforcement matters with corporations. Now, other federal agencies, state attorneys general, and even foreign government enforcement agencies are beginning to require monitors as well. This trend serves only to increase the need for corporate executives to understand the corporate monitor phenomenon and how imposition of a monitor could affect their companies.

This article addresses several issues that should be at the top of corporate executives' minds regarding monitorships—for example, what are the roles and responsibilities of a monitor, what steps a company can take to help avoid having a monitor imposed in the first place, how to work with a monitor if one is appointed, and whether there is a risk that the monitors' reports will become public.

What Is an Independent Compliance Monitor?

Independent compliance monitors were used rarely prior to the corporate scandals of 2001 and 2002. But following the scandals of Enron, WorldCom, Arthur Andersen, and other companies, corporate criminal prosecutions became a much higher priority for DOJ. The high-water mark for corporate prosecutions was DOJ's decision to seek and obtain an indictment of Arthur Andersen, which led to the demise of the venerable accounting firm. The fall of Arthur Andersen, in turn, led to a more concerted effort by DOJ to utilize (when possible) means of punishing corporations that were less drastic than indictment. Accordingly, DOJ increasingly relied on deferred prosecution agreements and non-prosecution agreements. Under these agreements, DOJ would agree not to move forward with a case against the company if the company agreed to certain actions, which usually involve paying a hefty fine, taking remedial actions, enhancing the company's compliance program, and preventing recurrence of the misconduct for some defined

 John F. Wood is a Partner of Hughes Hubbard & Reed LLP. John served in numerous high-level executive branch positions, including U.S. Attorney for the Western District of Missouri, Chief of Staff for the U.S. Department of Homeland Security, Deputy Associate Attorney General, Counselor to the U.S. Attorney General, and Deputy General Counsel for the White House Office of Management and Budget.

the Corporate Governance Advisor

The ***CORPORATE GOVERNANCE ADVISOR*** (ISSN 1067-6171) is published bimonthly by Wolters Kluwer at 76 Ninth Avenue, New York, NY 10011. Subscription rate, $895 for one year. POSTMASTER: Send address changes to *THE CORPORATE GOVERNANCE ADVISOR,* Wolters Kluwer, 7201 McKinney Circle, Frederick, MD 21704. Send editorial correspondence to Wolters Kluwer, 76 Ninth Avenue, New York, NY 10011. To subscribe, call 1-800-638-8437. For Customer service, call 1-800-234-1660.

period of time. Many of these agreements also included a provision requiring the appointment of a monitor. The monitor's role was to review the company's compliance with the terms of the agreement with DOJ for a defined period of time—usually two to four years (with three years being the most common).

The use of monitors quickly became controversial. Some of the early monitors were perceived as overly intrusive, with monitors reviewing day-to-day activities of the companies to seek out any evidence of further misconduct. Along with that broad monitor role came great expense, with some monitors costing companies tens of millions of dollars. The corporations subject to the monitors complained that they had too little say in the selection of the monitors, who were unilaterally chosen and imposed by DOJ. This concern took on greater prominence with the appointment of former Attorney General John Ashcroft to serve as monitor for Indiana-based medical supply company Zimmer Holdings. News reports indicated that Ashcroft's contract was worth between $28 million and $52 million, and his appointment as monitor by then U.S. Attorney Chris Christie led some to charge that DOJ was showing political favoritism in its appointment of monitors.

DOJ took much of the steam out of the criticisms by releasing in 2008 a set of principles to guide prosecutors in the selection and use of monitors. The principles explained that "[a] monitor's primary role is to evaluate whether a corporation has both adopted and effectively implemented ethics and compliance programs to address and reduce the risk of recurrence of the corporation's misconduct." The principles further called for companies to have a greater role in the selection of the monitors. Specifically, the principles stated that there should be a pool of three qualified candidates selected by the company, DOJ, or both, and that in many cases the company should submit its choice from among the three to DOJ for review and approval. Even in cases in which the selection process called for DOJ to play a greater role in selecting the monitor, the principles explain that DOJ should identify at least three acceptable monitor candidates and the company should choose from that list.

By making the monitor-selection process more competitive and giving the company greater say in the selection of monitors, DOJ has helped reduce the cost of monitorships, as monitor candidates now seek to be as cost-effective as possible in an attempt to be chosen for these prestigious assignments. Perhaps even more importantly, the role of the monitors has been clarified to some extent. Although every monitorship is different, today monitors tend to be less focused on monitoring the day-to-day activities of companies in search of evidence of misconduct, but instead tend to be more focused on reviewing the overall effectiveness of the companies' compliance programs as implemented. This is not to say that disputes among monitors and the companies they monitor have gone away, as there have been several recent disputes in which companies have complained that their monitors have run amok. But overall, monitors have become less costly and less intrusive since DOJ released its guidance principles.

Monitors are expected to review the companies' compliance programs (both on paper and in practice) and to assess the companies' adherence to their agreements with DOJ. In most cases, monitors are required to issue reports on a regular basis (often annually, but sometimes more frequently) to both the company and DOJ. Because the monitor is independent and not counsel to the company, these reports are not covered by the attorney-client privilege. They generally have been treated as confidential by both the companies and DOJ, but as explained later there have been recent efforts by the media and the public to obtain access to these reports.

Importantly, the DOJ principles apply only to DOJ-appointed monitors. As noted previously, many other enforcement agencies—including other federal and state agencies, as well as foreign government enforcement agencies—have begun requiring monitors as well. While in some cases those agencies look to DOJ's principles for guidance, often they do not. Perhaps the most

notable example is the New York Department of Financial Services, which has imposed monitors on several leading financial institutions that conduct business in New York.

Steps to Avoid the Appointment of a Monitor

Although monitorships have become less costly and less intrusive in recent years, the fact remains that no company has ever wanted to have a monitor imposed on it. There are several things that a company can do to reduce the chances of having a monitor imposed.

First, of course, a company should take steps to reduce the risk that it will violate the law at all. This requires having an effective compliance program, both on paper and in practice. The program should include strong policies and procedures, training, clear and compelling messages from company leadership about ethics and compliance, due diligence on business partners, and a strong internal compliance organization, among many other things.

Second, no compliance program is perfect, so even companies with the best of intentions might find themselves in the government's crosshairs. This is where the compliance program is critical once again. Even if the compliance program did not prevent all misconduct, DOJ might deem it sufficiently effective that an independent compliance monitor is not necessary. The most compelling issue for DOJ in determining whether to impose a monitor as a condition of settlement is whether DOJ has confidence in the company's compliance program to prevent a recurrence of the misconduct. If the compliance program is weak or still in development, DOJ is far more likely to require a monitor as a tool to help prevent and identify recidivism.

Third, some companies that are under investigation and fear that DOJ will appoint a monitor choose to proactively hire an outside law firm or investigative firm to serve as an independent compliance consultant. This is not a sure-fire way to head off the appointment of a monitor, but it may be seen by the government as a sign that the company has the matter under control. A self-imposed independent compliance consultant may be less intrusive and less expensive than an independent compliance monitor required by the government and reporting on a regular basis to the government.

How to Deal with a Monitor If You Must Have One

No company wants to have a monitor, but some are far worse than others. A good monitor can be relatively cost-effective, minimize disruption to business operations, and actually help make the company better in the long run. In contrast, a bad monitor can make corporate executives' lives miserable. So it is critical that the company get a monitor who understands the company's business realities and will seek to make the company better, rather than to make a name for the monitor or obtain a short-term windfall from the appointment. A company should consider not only a monitor candidate's credentials, but also the monitor's judgment, personality fit, and trustworthiness.

Once a monitor is in place, it is essential that the company be entirely honest and up front with the monitor. Even the most reasonable monitor will likely become intrusive if the monitor does not trust that the company is providing accurate and truthful information. Any effort to mislead the monitor or conceal information from the monitor will lead to distrust.

One of the best rules for dealing with a monitor is a "no surprises" rule. A good monitor will understand that no compliance program is perfect. When the inevitable shortcomings or mishaps occur, the company is far better off telling the monitor of the occurrence and how the company is addressing it than to have the monitor find out by other means. But this "no surprises" rule should run in both directions—the company should expect the monitor to inform the company of any shortcomings identified in the company's compliance program and give the company an opportunity to address

them, rather than play "gotcha" by raising the concerns for the first time in a report to the government.

With mutual trust and a constant flow of information between the monitor and the company, the monitorship can actually help make the company better suited for the future, while minimizing costs and intrusion on business operations.

Are Monitors' Reports Public?

As mentioned previously, the companies and DOJ generally treat monitors' reports as confidential, but there have been recent efforts by the media and the public to use the courts to gain access to these reports. The companies, DOJ, and the monitors themselves have all opposed such efforts to make the reports public. To date, two of these cases have reached the courts of appeals. In both cases the courts of appeals have concluded that the monitors' reports are not "judicial records," and therefore that the public does not have a First Amendment or common law right of access. But in some cases reporters have tried a separate route to get access to the reports—the Freedom of Information Act (FOIA). FOIA requires federal government agencies to produce certain records when requested by the public, but the law contains several exemptions. Thus far, DOJ has invoked FOIA's exemptions to avoid release of the monitor reports, but reporters have challenged DOJ's decision in court. Those cases are still being litigated, thus creating some remaining uncertainty about whether the reports could ultimately be released.

The possibility of public release of monitors' reports should cause great concern for the corporate community. Those reports often contain very sensitive business information, as a good monitor will explain in the reports how the program works in actual business contexts. If the reports were to become public, it could have a chilling effect on communications between companies and their monitors in the future. Companies might be reluctant to share sensitive business information with their monitors for fear that it could be included in the monitors' reports and ultimately released to the public. Likewise, a monitor who is sensitive to this concern might limit how much detail the monitor puts in the reports, which in turn can reduce the amount of information that the government obtains regarding the monitor's work.

The possibility that monitor reports could become public is all the more reason why companies should take steps proactively to make sure that they never have to have a monitor in the first place.

SEC Announces Whistleblower Award for Government Employee

By Douglas Paul, Richard Parrino, Emily Lyons, and Ann Koppuzha

On July 25, 2017, the Securities and Exchange Commission (SEC) announced that it would grant $2.5 million "to an employee of a domestic government agency whose tip helped launch an SEC investigation and whose continued assistance enabled the SEC to address a company's misconduct." The government employee assisted the SEC by providing tips that led to the opening of the case, and by furnishing key documents and testimony. Importantly, the SEC indicated that the agency where the whistleblower worked had law enforcement responsibilities. The SEC's order makes government employees eligible for whistleblower awards and creates both uncertainty and opportunity for a monetary award for government employees who may possess information relevant to SEC enforcement actions.

Background

Subject to certain exceptions, individuals are eligible for an award when they voluntarily provide the SEC with "original information that leads to a successful enforcement action." Whistleblowers are eligible for 10 percent to 30 percent of the money collected when the monetary sanctions exceed $1 million. According to the SEC, it has awarded $156 million to 45 whistleblowers since inauguration of the program in July 2010. All awards are paid out of an investor protection fund established by Congress, which is funded by monetary sanctions paid to the SEC. Whistleblowers are not guaranteed a reward and must apply for the reward after the monetary sanction has been decided.

 Douglas Paul and Richard Parrino are Partners, and Emily Lyons and Ann Koppuzha are Associates, at Hogan Lovells US LLP.

Broad Interpretation of Government Employees Eligible for Whistleblower Awards

The July 25 order represents the first time that the SEC has announced a whistleblower award for a government employee. In a footnote in its July 25, 2017, Order Determining Whistleblower Award Claim, the SEC explained that federal, state, and local government employees are eligible for this award except when they work for (1) an "appropriate regulatory agency" or (2) "a law enforcement organization." The Securities Exchange Act of 1934 (Exchange Act) defines an "appropriate regulatory agency" as the SEC and related banking agencies listed in the Exchange Act, including the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation.

The SEC relegated to a lengthy footnote the most complex part of its order, in which it indicated that although an employee of a law enforcement organization is not normally eligible as a whistleblower, there may be an exception when law enforcement is just one component of the agency's purposes and the employee does not work for that component of the agency. According to the SEC, employees of law enforcement organizations—defined as organizations "having to do with the detection, investigation, or prosecution of potential violations of law"—are eligible for the award so long as they do not work for the "sub agency components that perform the law enforcement responsibilities." The SEC cited Congress's choice of the word "organization" instead of "agency" or "authority" in the Exchange Act as affording the SEC the opportunity to "interpret the exclusion flexibly." Under the SEC's reading, the law enforcement exception applies to agency components that perform law enforcement actions, not to all employees of an agency that "happens to have been

granted law enforcement powers among its many other separate responsibilities and powers."

In this case, the employee did work for an agency that possessed law enforcement responsibilities, but the SEC still granted the award because the employee did not work in a law enforcement division of the organization. The SEC emphasized that this was not a situation in which the employee "sought to circumvent the potential responsibilities that his or her government agency might have to investigate."

In its order, the SEC thus narrowed the definition of "law enforcement organization," which in turn broadened the scope of government employees eligible for awards as whistleblowers. In its wake, the SEC left both opportunity for potential government-employee whistleblowers and ambiguity relating to the scope of the law enforcement exception.

Implications of SEC's Order for Sharing of Information with Government Agencies

Despite speculation under the Trump Administration that the SEC was likely to step away from enforcement and regulation, the agency's grant of a whistleblower reward to a government employee demonstrates that the SEC will continue aggressively to use the whistleblower program to bring enforcement actions. It is once again encouraging those with relevant and reliable information, whether they work in the private or public sector, to come forward and cooperate with the SEC. Accordingly, companies should expect cooperation by whistleblowers to contribute to future SEC investigations and enforcement actions.

The order also reinforces the potential for information-sharing between government-agency employees and the SEC. Personal gain could motivate a government employee to pass along information to the SEC in hopes of receiving an award, especially if the reward encourages competition among government employees to provide information to the SEC. Companies that regularly work and communicate with regulatory agencies should consider the risk of sharing information that could serve as evidence of securities violations, particularly if the likely sanctions could exceed $1 million, which is the threshold required to receive a whistleblower award.

Sentiment Analysis & Natural Language: Processing Techniques for Capital Markets & Disclosure

By Nicolas H.R. Dumont

Application of machine learning, artificial intelligence, and advanced analytics to big data influences nearly all industries today. The securities markets are no exception. Issuers use these tools for marketing, product development, and operations; investors harness data in search of trading insights; and regulators monitor compliance and detect risks. Markets themselves create a wealth of data that perpetuates a virtuous cycle of information generation, reliance and analysis.

To date, discussions surrounding technology and finance focus on how each player uses innovation to achieve its own goals, whether streamlining operations, increasing returns, or detecting fraud.[1] There is considerably less discussion about how these developments born of the Internet era influence (or should influence) issuers. Following an overview of sentiment analysis technology and how and to what extent it is currently being used in the capital markets, we then discuss the way these techniques could affect how issuers operate in the market.

The State of Play

"Big Data"

Business and finance have both long relied on data, as the term is used in the casual sense. A standard definition of data is any "factual information (such as measurements or statistics) used as a basis for reasoning, discussion, or calculation."[2] As implied by the terminology, big data is partially characterized by volume. But beyond sheer size, "big data" connotes a degree of complexity that results from the compilation of information taking different forms, stemming from multiple sources, produced at different times.[3] This complexity and volume calls for techniques that enable the capture, storage, processing, and analysis of such information. In this way, "big data" is more than just *a lot* of information; it represents a new frame in which information is collected, connected, and used.

While investors have long sought out new forms of information to enhance returns, the digital age generates exponentially more data from countless new sources. Investors can harness satellite images to measure customer cars in parking lots, and can "scrape" issuer Web sites for more information than what was perhaps intended for public consumption. In fact, data is now so big—in terms of relevance and scope—that many investors, and even some government agencies,[4] subscribe to data feeds to be processed in house, or prepackaged analytics from data analytics companies.[5]

Natural Language Processing & Sentiment Analysis

The proliferation of big data has required and encouraged new processing methods, and new methods have in turn required and encouraged new data sources. As the sheer amount of information grows and becomes more complex, storage and processing techniques become increasingly important, but as the universe of data constantly grows and evolves, it is increasingly inefficient and ineffective to rely on predetermined programming to govern processing techniques. A new area of artificial intelligence, known broadly as machine learning, responds to this issue. Such algorithms not only analyze data but also use such data to learn and enhance processing rules such that they adapt and change without additional guidance.[6]

 Nicolas H.R. Dumont is an Associate in the New York office of Gibson, Dunn & Crutcher LLP.

Natural language processing (NLP) developed in response to yet a third issue presented by big data. Much of the information that is traditionally important in capital markets is unstructured, meaning it is formatted and designed for humans, not computers, such as Management's Discussion and Analysis (MD&A) disclosures, financial footnotes, and oral disclosures. Applying machine-learning techniques to spoken and written language, NLP algorithms process these portions, and other sources, and learn to read and interpret language.[7]

For example, algorithms can now automatically supplement structured financial disclosures from Securities and Exchange Commission (SEC) filings with information from the textual disclosures without an analyst actually reading the text and manually adjusting a model.[8] And as NLP has developed, algorithms have advanced from mere text retrieval to automatic categorization and topic modelling, such that NLP algorithms can now retrieve filings, financial reports, press releases, news and the like, and then also compare the various sources to verify consistency, detect differences, synthesize information, and incorporate a wider range of sources into analysts' models.[9]

To illustrate the speed at which NLP can operate, consider Twitter's experience in April 2015 when that company accidentally posted an earnings report an hour early: A Web crawler using NLP algorithms seized the report, summarized, and then tweeted the contents within three seconds of the post.[10] In the regulatory space, NLP enables the SEC to rapidly scan regulatory filings and discover new terms as they appear, potentially unveiling new risks to the market as a whole or to specific industries.[11] Other NLP applications use sentence length or complexity as a proxy for obfuscation, which in turn measures risk,[12] and compares the detail or length of the topics discussed in MD&As as a proxy for accounting fraud.[13]

NLP also encourages the use of new data sources, now accessible through improved techniques. Algorithms mine less traditional sources of information, such as news and social media feeds, for insights on consumer trends and to discover market-moving events. For example, Dataminr, a company that sells real-time alerts based on social media feeds, alerted clients when the King of Saudi Arabia died more than four hours before crude oil prices spiked.[14] Similarly, using thousands of user posts on a Reddit feed, Eagle Alpha—a software company that provides data and analysis tools—predicted that Electronic Arts would sell more copies of its new video game than originally predicted before the company revised its projections.[15] Thus, social media and other alternative sources have earned the respect of at least some investors who seek to harness both the wisdom of the crowds and the speed at which news travels in these networks.

Finally, investors and the SEC also use NLP in sentiment analysis, a tool to assess issuer or consumer outlook. Premised on the idea that particular words connote uncertainty, intentional obfuscation, or a positive or negative outlook, investors and regulators alike use algorithms to measure prevalence of certain words,[16] and then draw inferences based on these subtle indicators. Positive or negative sentiment scores not only synthesize sizable amounts of language into a single composite score,[17] but can also be applied to portions of texts to show that optimism in a portion of a disclosure is camouflaging uncertainty in another.[18] The MD&A portion of a quarterly or annual report is particularly prone to sentiment analysis, as such disclosures are required for public issuers, the topics are dictated, and the disclosure is explicitly geared toward measuring management's perspective.[19] However, sentiment analysis is also applied to derive tonality from other corporate sources, such as oral statements on earnings calls[20] and press releases, as well as consumer sources, like user reviews, social media, and news.[21]

Applications & Challenges

Both investors and regulators are increasingly applying these new techniques to achieve their respective goals of higher returns and enforcement of market rules and regulations.[22]

Use by Traders

One estimate shows that more than a quarter of stock turnover is traded by funds run by algorithms using these techniques, up 100 percent in 2017 over just four years prior.[23] Half of the top 25 investment firms rely on a computer-based strategy of some kind.[24] BlackRock's AI machine, Aladdin, uses NLP to sift through sources from broker reports to social media feeds to generate sentiment scores and learn about news events, and Bridgewater Associates uses IBM Watson technology to glean insights on and predict market trends.[25]

Machine learning is still learning, however, and flaws remain. First, even as sentiment analysis improves, sarcasm or other non-"plain English" text can pose significant interpretation challenges for machines.[26] Further, while machines easily detect correlations, it is significantly harder to learn causality, which limits the application of the derived insights.[27] Especially given the large amount of data incorporated, models are bound to produce at least some strong correlations based on historical trends that are not representative of actual relationships that will hold in the future. Some correlations are just coincidental.

Lastly, increased reliance on algorithms also leaves investors vulnerable to false positives. For example, algorithms—and possibly people, as well—were fooled by two fake tweets sent under handles designed to pass for well-known market players, and a hacker manipulating the Associated Press's Web site sent the market down 145 points in only two minutes.[28]

For some analysts, the use of algorithms to interpret market data appears to have dampened the traditional market-moving effects of released material information. Some have attributed a recent decrease in market volatility to the rise of advanced analytical methods that integrate many small indicators rather than react to "material" information distributed by issuers. Over half of the lowest 25 volatility readings, as based on an options based index called VIX, were observed between May and July 2017.[29] Analytics experts attribute this lower volatility to algorithms that process news and events over a longer period, spreading the impact of what could be material information over a longer trading period.[30] An alternative theory is that the algorithms access and process so much data that models are converging, reducing spreads and the associated volatility.

There are reasons to be skeptical of this view, however. Data proliferation when combined with automated trading software creates risks, especially when that information is replaced by unverified outside sources. For example, human subscribers to the Muddy Waters and Citron Research feeds would not have been fooled by the fake tweets sent out in 2013 because they would compare the information to the real, vetted source.[31] Similarly, combining these less-vetted sources with processing systems that few understand can also downplay truly material information and focus too much attention on the noise. Synthesizing machine-simplified disclosures with indicators collected from disparate sources risks replacing deliberate nuances with random, potentially misleading ones. Further, in a world in which information is not only reported, tweeted, and posted, but also then re-tweeted and re-posted, algorithms risk mistaking echo chambers for trends. These issues, which have occasionally manifested themselves in actual volatility, call for increased monitoring by issuers of information relating to them.

Use by the SEC

The SEC, like many investors,[32] uses machine learning as a tool to assist, but not to replace, human judgment. In the enforcement context, the SEC uses transaction data and other information to detect insider trading, market manipulation, and compliance with suitability rules.[33] The SEC also employs NLP algorithms to sift through filings and discover new terms that could signal new risks and market exposures.[34] Both of these applications enable the SEC to take a more proactive approach to detecting fraud and risk. Rather than wait for suspicious behavior to be reported, the SEC can use modelling to uncover discrepancies. Even when the SEC does rely on tips, complaints, and referrals

submitted to the Office of the Whistleblower, NLP technology is used to group common complaints, enabling a more comprehensive and speedy review.[35]

Additionally, the SEC also uses sentiment analysis to assess the tonality of disclosures, looking for obfuscation or negativity as a measure of risk. Comparing the NLP results with more established risk indicators, like past enforcement actions or examination results, the SEC can more easily assess future filings by issuers known to pose risk, and train its models to aid examiners in deciding which other issuers deserve more scrutiny.[36] The SEC also compares the length and detail of disclosures for indicators of when obfuscation or brevity is a signal of fraud.

For example, the Division of Economic Risk and Analysis, using NLP techniques, has found that firms subject to enforcement actions related to financial reporting are less likely to discuss certain topics related to performance, essentially confirming that issuers charged with misconduct tend to downplay risks in financial disclosures.[37] In addition, regulators have started to address some of the implications for asset managers and funds, particularly as applied to computer-based strategy and robo-trading.[38]

Implications & Recommendations

These developments represent a change in the way that the market digests financial information. Not only are investors and investigators alike regularly harnessing record amounts of data, but they are also increasingly looking at innovative ways to integrate such data into predictive methodologies. Consideration must be given to what these technological developments imply for issuers as a practical matter. A few thoughts are presented.

- *Everything is (likely) being monitored.* Earnings calls have long been market-moving events, but the advent of sentiment analysis means that investors might be listening in a new way. Issuers should be aware that written and oral statements are exposed to such analysis and other NLP techniques, and that the unstructured or oral nature of a disclosure does not necessarily protect the content from machine analytics. As sentiment and topic variation are more easily detected in less structured settings, issuers should devote increased attention to the preparation and rehearsal of earnings calls, employee disclosures outside the firm, free writing prospectuses, 8-Ks and other less-scripted events. These disclosures should be reviewed carefully prior to dissemination with a view toward the way an algorithm designed to scrape information could interpret and re-transcribe them, as nuance may be lost.

- *Consistency across and within disclosures.* Issuers should ensure absolute consistency between different forms of disclosure.

  - Technology enables market watchers to spot even the most minor discrepancies among statements based on length, detail, and clarity of content. While explicitly scripting a message to counteract a sentiment-analysis algorithm could be considered manipulative or misleading (and potentially a violation of Regulation FD if designed to signal information to sophisticated market participants), developing an understanding how these algorithms function is recommended.

  - Issuers should recognize that the SEC (and perhaps investors) compare the length of topical discussions within issuer filings or statements over time and across the filings of multiple issuers in search of evidence that issuers are attempting to camouflage or downplay risks.[39] While there are clearly instances in which an issuer can and should omit discussion of specific risks, it should be remembered that subtle differences will likely be noticed and may increase scrutiny. For instance, if an issuer consistently discusses an aspect of the business or a risk in a certain level of detail, regulators and the market will notice when the length or detail of such discussion changes. Similarly, if one issuer

omits a risk or condition discussed by its peers, market participants and watch dogs will also take notice. This has generally always been true, but NLP has enabled investors and regulators to notice more detail and notice it more quickly. Thus, investors should be prepared to explain such changes, even if minimal.

- *Reinforce Regulation FD-type controls*. While most public issuers have controls and policies in place to monitor what is said by or on behalf of the company, the new paradigm of data analysis leaves little room for error. As online communications, just like oral disclosures, are governed by Regulation FD, issuers should have clear policies in place to govern who can transmit information online, when the information can be posted, and how the company and its employees conduct Regulation FD analysis on an *ad hoc* basis. Issuers should also consider developing compliance procedures for tracking employee and company sites, as well as a record-retention policy. Issuers should also enforce the appropriate level of security for all publicly facing sites to ensure that material information is not inadvertently exposed. Twitter's experience in 2015 proves that accidental exposures or similar lapses in security are not overlooked by software scanning the market automatically.

    - Issuers should also be mindful to monitor (or altogether avoid) unscripted oral communications made by company officials, especially those made in private or informal settings, as it is possible that those utterances will be captured, scrutinized and analyzed quickly in the future. While in the past it would have been unusual for such statements to reach investor or regulatory scrutiny simply because proof was difficult to come by, an era in which voice recordings are transcribed onto permanent records may soon emerge.

- *Survey & control your digital footprint*. Because investors are scrutinizing far more data than that reported to the SEC, issuers should be attentive to that data over which they may exercise control, and be otherwise aware of their pronouncements and their implications. Failure to monitor appropriately could result in exposure to increased liability.

    - First, companies may consider reformatting portions of their Web site not intended to convey investor information in a manner that is less conducive to analysis by even the smartest machines. For example, retail issuers may consider how much inventory information is available through consumer shopping portals, as investors have developed Web crawlers that access retailer sites for information on prices and sales.[40] Some online platforms require verification before users can access certain information. Whether requiring a user to check a box or decode a message, such preliminary screening tools might deter some Web crawlers from extracting data that is not intended to be used for trading.

    - Second, especially in the absence of any Regulation FD changes, issuers should consider their own data-sharing arrangements. Many companies share or sell data about the company or its customers, which in turn, implies information about the company. For instance, payment processors, like banks and credit cards, often negotiate the rights regarding information gleaned from consumer transaction data. The terms of these arrangements should be considered, not only with respect to consumer privacy and marketing potential, but also in light of the new uses to which data has been put. For example, for an issuer who sells consumer transaction data aggregated by issuer rather than customer demographic, the data could easily now convey sensitive financial information about the issuer, rather than its customers, as intended.

        - Issuers that do share data should also conduct an appropriate Regulation FD analysis tailored to their own facts and circumstances to determine whether the receiving parties are covered under Regulation FD, whether the

information is material, and whether the data is released on a schedule that could conflict with disclosure rules.

- In sum, given the prevalence of data in markets, companies should review data contracts to see how much information they are sharing, when it is transmitted, what that information can be used for, and with whom that data can be shared.

- Third, because information and new stories can be generated quickly and without filter or scrutiny, issuers should continue to monitor the proliferation of stories for which they are not responsible that are nevertheless erroneous, and act swiftly to correct the story (if possible) before it is reproduced too quickly or causes any movements in the markets.

- Fourth, while the SEC encourages issuers to use company Web sites as a method of communication, issuers should also recognize that these less formal environments are likely to attract equal if not more attention from investors. Just as the MD&A portion of a filing is a ripe target for sentiment analysis because it is less structured, Web sites and social media often offer additional opportunities to mine executive and company statements for subtle clues regarding outlook and future performance. Issuers should ensure that all statements are carefully drafted, even when conversing orally or posting in a seemingly more casual environment.

- *Consider what constitutes "material" information*. What constitutes "material" information in the age of machine learning? When the US Securities Act was enacted in 1933, information regarding issuers was difficult to access and far harder to distribute than today. The disclosure regime imposed by U.S. securities laws effectively contemplates an information pipeline: Issuers determine what information could be considered material to investors in response to forms developed, and events identified, by the US SEC. While it has always been true that investors have sought to gain an advantage in the markets (sometimes illegally) by looking outside the "pipeline," new data, whether oral, written, or on social media, exacerbates the chatter.

  - Advances in big data and analytics call into question an approach to material disclosure based solely on the opinions of human drafters. Because company disclosures and other information outside the "pipeline" are analyzed to decipher and discover hidden meanings not contemplated by, or hidden from, their writers, "material" information may be more difficult to identify from the perspective of an issuer. The securities laws were designed to create information digestible by the typical investor, who would presumably review and analyze such information in a similar manner one to the next.

    Today, in reality, information is now digested, interpreted, and acted upon by algorithms at speeds exceeding human capacity. Those algorithms are, in certain circumstances, making investment decisions that almost by definition make unseen data (and related patterns in that data) material. It is unlikely that these interpretations, at least in all instances, are what the typical issuer intends when accounting, investor relations, and legal teams produce disclosures for the investing public. With limited data and limited tools, crafting nuanced disclosures to be read by humans produces a certain type of disclosure that has long guided the public markets. With lots of data that is easily produced and distributed, relating what is "material" may be more challenging because counterparties are listening in a way that most humans never intended.

Notes

1. *See, e.g.* Penny Crosman, "All the Ways AI Will Slash Wall Street Jobs," *Am. Banker*, Mar. 16, 2017, available at *https://www.americanbanker.com/news/all-the-ways-ai-will-slash-wall-street-jobs* (noting Wall Street's use of AI not

only in trading but also in robotic process automation, front office work, compliance and HR), last accessed Oct. 10, 2017; Bryan Yurcan, "What Santander's Latest Bets Say About the Future of Fintech," *Am. Banker*, Jul. 12, 2017, available at *https://www.americanbanker.com/news/what-santanders-latest-bets-say-about-the-future-of-fintech* (highlighting use of real time sentiment analysis of phone calls to aid call center workers) last accessed Oct. 10, 2017.

2. *Data*, *Merriam-Webster Dictionary* (online ed.), *https://www.merriam-webster.com/dictionary/data*, last accessed Oct. 11, 2017.

3. *See* Svetlana Sicular, Contributor, "Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three 'V's," *Forbes Mag*., Mar. 27, 2013, available at *http://onforb.es/103sM27, last accessed Oct. 10, 2017*.

4. Jen Wieczner, "How Investors are Using Social Media to Make Money," *Fortune Mag*. (Dec. 7, 2015), available at *http://fortune.com/2015/12/07/dataminr-hedge-funds-twitter-data/, last accessed Oct. 10, 2017*.

5. *See* Sarah Butcher, "43 of the Top Big Data Companies to Work For, by J.P. Morgan," *efinancialcarreers* (Jun. 1, 2017), available at *http://news.efinancialcareers.com/us-en/285462/the-top-big-data-companies-to-work-for-by-j-p-morgan/* (listing top financial data services) last accessed Oct. 10, 2017; Ivy Schmerken, "Quant Funds Get Sentimental About Big Data," *Market Media*, Aug. 4, 2016, available at *https://marketsmedia.com/quant-funds-sentimental-big-data-by-ivy-schmerken-flextrade/* (discussing various analysis services), last accessed Oct. 10, 2017; Penny Crosman, "Beyond Robo-Advisers: How AI Could Rewire Wealth Management," *Am. Banker*, Jan. 5, 2017, available at *https://www.americanbanker.com/news/beyond-robo-advisers-how-ai-could-rewire-wealth-management* (discussing in house analytics), last accessed Oct. 10, 2017.

6. Tom Loftus, "What Your CEO Is Reading: Designing Around AI's 'Black Box'; Flash Organizations; Nature's End," *The Wall St. J*., Jul. 14, 2017, available at *http://on.wsj.com/2tTwvV3* (quoting Katharine Schwab from Fast Company), last accessed Oct. 10, 2017 (subscription required).

7. Alex LaPlante and Thomas F. Coleman, *Teaching Computers to Understand Human Language: How Natural Language Processing is Reshaping the World of Finance*, The Global Risk Institute, Jan. 15, 2017, available at *http://globalriskinstitute.org/publications/natural-language-processing-reshaping-world-finance/,* last accessed Oct. 10, 2017.

8. "Achieving Transparency in Financial Reporting With Artificial Intelligence," *Kognetics Blog* (Oct. 3, 2016), available at *http://www.kognetics.com/2016/1%3/achieving-transparency-in-financial-reporting-with-artificial-intelligence/* last accessed Oct. 10, 2017.

9. LaPlante and Coleman, *supra* n.7.

10. Wieczner, *supra* n.4.

11. Scott W. Bauguess, Champagne Keynote Address: The Role of Big Data, Machine Learning, and AI in Assessing Risks: a Regulatory Perspective (June 21, 2017), available at *https://www.sec.gov/news/speech/bauguess-big-data-ai*, last accessed Oct. 10, 2017.

12. *See* David F. Larcker and Anastasia A Zakolyukina, "Detecting Deceptive Discussions in Conference Calls," 50 *J. of Acct. Res*. 495, 499 (2012) (citing other sources).

13. Gerard Hoberg and Craig Lewis, "Do Fraudulent Firms Produce Abnormal Disclosure?," 43 *J. of Corp. Fin.* 58, 75–77 (2017) (showing which topics are correlated with a fraud finding when measured by deviation from a standard explanation).

14. Wieczner, *supra* n.4.

15. *Id.*

16. A great deal of academic research focuses on the proper mapping of words to sentiment. *See generally* Sanjib Ranjan Das, "Text and Context: Language Analytics in Finance," 8 *Found. and Trends in Fin*. 3 (2014); Ann Devitt and Khurshid Ahmad, "Is There a Language of Sentiment? An Analysis of Lexical Resources For Sentiment Analysis," 47 *Language Resources and Evaluation* 475 (2013); Jessen L Hobson, William J. Mayew and Mohan Venkatachalam, "Analyzing Speech to Detect Financial Misreporting," 50 *J. of Acct. Res*. 349 (2012); Tim Loughran and Bill McDonald, "When Is a Liability Not a Liability? Textual Analysis, Dictionaries, and 10-Ks," 66 *J. of Fin*. 35, (2011).

17. Andreas Chouliaras, "The Pessimism Factor: SEC EDGAR Form 10-K Textual Analysis and Stock Returns" (Jul. 6, 2017), available at *http://dx.doi.org/10.2139/ssrn.2627037*, last accessed Oct. 10, 2017; LaPlante and Coleman, *supra* n.7; Schmerken, *supra* n.5.

18. Hoberg and Lewis, *supra* n.13 at 76–79.

19. *Id.* at 59.

20. Larcker and Zakolyukina, *supra* n.12 at 499.

21. Schmerken, *supra* n.5; Nigel Farmer, "Sentiment Analysis: Where Next?," *Markets Media*, (Sept. 11, 2015), available at *https://marketsmedia.com/sentiment-analysis-where-next/*, last accessed Oct. 10, 2017.

22. The SEC has been increasing its use of machine learning in enforcement and compliance as well as risk detection, as discussed later. Additionally, it is reported that Dataminr, a data and analysis supplier to large investment firms, also has government clients. *See* Wieczner, *supra* n.4.

23. Spencer Jakab, "How Quants Are Calming the Stock Market," *The Wall St. J*., B12, July 21, 2017 (citing Tabb Group).

24. Jonathan Ratner, "Last days of the stock picker as money managers embrace artificial intelligence," *Fin. Post*, Apr. 7, 2017, available at *http://business.financialpost.com/*

investing/last-days-of-the-stock-picker-as-money-managers-embrace-artificial-intelligence/wcm/333a7ba8-e0c9-487f-8787-2cb67970300e#comments-area, last accessed Oct. 10, 2017.

25. Crosman, *supra* n.5.

26. Penny Crosman, "Why AI Still Has a Ways to Go in Wealth Management," *Am. Banker*, Jul. 13, 2017, available at *https://www.americanbanker.com/news/why-ai-still-has-a-ways-to-go-in-wealth-management*, last accessed Oct. 10, 2017; Wieczner, *supra* n.4 (noting that one hedge fund's AI was fooled by sarcastic tweets regarding Lululemon).

27. Ratner, *supra* n.24.

28. Wieczner, *supra* n.4.

29. Jakab, *supra* n.23.

30. *Id.*

31. Wieczner, *supra* n.4 (discussing how an individual set up imposter accounts to tweet fake news about companies Audience and Sarepta Therapeutics, causing the stocks to fall 28 percent and 16 percent respectively).

32. Crosman, *supra* n.26.

33. *See* Mary Jo White, Chair, A New Model for SEC Enforcement: Producing Bold and Unrelenting Results (Nov. 18, 2016), available at *https://www.sec.gov/news/speech/chair-white-speech-new-york-university-111816.html*, last accessed Oct. 10, 2017.

34. Bauguess, *supra* n.11.

35. *Id.*

36. Scott W. Bauguess, Has Big Data Made Us Lazy? (Oct. 21, 2016), available at *https://www.sec.gov/news/speech/bauguess-american-accounting-association-102116.html*, last accessed Oct. 10, 2017.

37. Bauguess, *supra* n.11.

38. Financial Stability Board, *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention* (Jun. 27, 2017) (focusing on robo-advisors and machine learning); International Organization of Securities Commissions, *IOSCO Research Report on Financial Technologies* (Feb. 2017) (discussing risks from robo-advisors and social media analysis, among other topics); Financial Industry Regulatory Authority, *Report on Digital Investment Advice* (March 2016) (analyzing digital investment advice through traditional broker-dealer rules).

39. Bauguess, *supra* n.11.

40. Wieczner, *supra* n.4.

Wolters Kluwer

Wolters Kluwer
The Corporate Governance Advisor
Distribution Center
7201 McKinney Circle
Frederick, MD 21704

TIMELY REPORT

Please Expedite

November/December 10041526-0060