GOVERNMENT INVESTIGATIONS: CYBERSECURITY AND CORPORATE MONITORSHIPS

ANALYSIS: CYBER-MONITORING: THE NEXT FRONTIER

by Jacob S. Frenkel and Justin L. Root

Cybersecurity is "hot" and will stay "hot" for corporations, executives, regulators, law enforcement and legislators. Rarely is there a corporate compliance discussion in 2017 where cyber isn't "the" topic or a material part of the discussion. Corporate boards recognize that cybersecurity is and will remain a high priority because of the attendant risks on so many levels. And two recent matters – one a case and the other a high profile internal investigation – portend that an imminent frontier in corporate monitoring will be cybersecurity.

Recent governmental attention to corporate cybersecurity programs suggests strongly that cyber oversight will be the next priority area for corporate compliance monitoring. The Securities and Exchange Commission (SEC), for example, announced in January 2017 that cybersecurity compliance procedures would be a key focus for its Office of Compliance Inspections and Examinations (OCIE) this year.[i] OCIE previously announced cybersecurity as a priority for its 2016 examination program,[ii] tracking its September 2015 cybersecurity examinations initiative.[iii] Considering prior enforcement actions by the SEC against investment advisors and broker-dealers to address allegedly inadequate cybersecurity policies that enabled data breaches, the SEC's announcement is no surprise. Similarly, the Federal Trade Commission (FTC) has been flexing its enforcement muscle through actions alleging that policy failures led to the exposure of confidential consumer information.[iv] These actions consistently result in settlements that impose cybersecurity enhancements designed to prevent similar future incidents. In the absence of an informed and sufficient monitoring program, however, it is difficult to assess effectively whether the corporations are implementing the negotiated settlements properly and, perhaps more importantly, as expected by the agency.

The SEC has a well-established track record for using independent corporate monitors across a broad range of cases. The FTC, on the other hand is in its infancy doing so, somewhat surprisingly. In a September 2016 settlement, the FTC jumped into the monitorship space by imposing a monitor to ensure compliance with a settlement that required a company to change fundamentally its compensation structure by rewarding actual sales rather than recruitment of new distributors. Although that FTC settlement did not present a cybersecurity issue, the FTC nevertheless set the stage to connect monitorships with the agency's already active regulatory attention to cybersecurity matters. An example of such an opportunity presented on March 1, 2017 when Yahoo announced, in its Form 10-K filed with the SEC,[v] that as a result of an internal investigation associated with three cybersecurity incidents – including the theft of data from more than one billion accounts – the Company "took certain remedial action, notifying 26 specifically targeted users and consulting with law enforcement." The 10-K describes the cyber-centric "other remedial actions" as follows:

> [T]he Board has directed the Company to implement or enhance a number of corrective actions, including revision of its technical and legal information security incident response protocols to help ensure: escalation of cybersecurity incidents to senior executives and the Board of Directors; rigorous investigation of cybersecurity incidents and engagement of forensic experts as appropriate; rigorous assessment of and documenting any legal reporting obligations and engagement of outside counsel as appropriate; comprehensive risk assessments with respect to cybersecurity events; effective cross-functional communication regarding cybersecurity events; appropriate and timely disclosure of material cybersecurity incidents; and enhanced training and oversight to help ensure processes are followed.

The 10-K also references 43 related class action lawsuits and the company's cooperation with the SEC, the FTC, the United States Attorney's Office for the Southern District of New York, and two State Attorneys General. Additionally, the General Counsel and Secretary resigned, receiving no severance payments. Moreover, the CEO gave up $12 million in stock and did not receive her 2016 cash bonus. It is easy to see where breaches and remediation as Yahoo disclosed could become the door-opener for a cybersecurity monitor.

Traditional corporate monitoring models allow for the implementation of an independent monitor to oversee an organization's compliance with imposed obligations over a period of time. Independent monitors, by operation of the monitorship agreement, typically receive access to the subject company's personnel, files, books, and records that fall within the scope of the settlement agreement and have authority to take necessary steps to become fully informed regarding the monitored company's operations, within the parameters of the agreement. The independent monitors also are free to communicate with the regulatory body (or agency) regarding the monitored company's corrective measures (or lack thereof). If the subject organization is found not to have complied with the terms of the settlement (*i.e.,* not adhering to the compliance and other policies, procedures and steps designed to remediate and correct the conduct that gave rise to the settlement), then penalties can be assessed, including reinstitution of the criminal or regulatory action(s), and extension of the monitorship. And, particularly in the cybersecurity area, systems vulnerabilities easily can challenge the test of compliance with the settlement terms.

Cybersecurity-related regulatory actions, however, usually do not follow this model. Instead, many cybersecurity settlements and consent orders mandate only that independent third-party professionals periodically assess and report on the implementation of information privacy and cybersecurity safeguards. Because cybersecurity settlement agreements do not typically include an active independent monitor with the requisite background and experience to assess an organization's remedial cybersecurity measures on a granular level, the benefits of an imbedded qualified

professional to ensure true remediation are absent from the impacted company. Ideally, a cybersecurity monitor would and should have through knowledge, skill, training, experience, or education sufficient up-to-date technical expertise and a measurable level of experience – preferably a minimum of five years of demonstrable experience dealing with cybersecurity or incident responses – to act in a cyber-monitoring capacity. Also, the cybersecurity monitor should hold a minimum of one relevant technical certification. Instead, the present norm is the less beneficial periodic spot-checking undertaken by professionals who likely do not have the level of knowledge of the organization or an in-depth appreciation of the issues surrounding what gave rise to the settlement and need for remediation in the first place.

This seemingly minimalist approach to corporate cybersecurity monitoring is surprising because proper implementation of cybersecurity safeguards is, by design, meant to be tailored to a specific organization. It is not always clear, however, that proper implementation necessarily will satisfy regulators' expectations. For example, many experts view the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the "Cybersecurity Framework") to be a benchmark for modern digital security implementation standards. In a seeming inherent contradiction, the FTC has opined that (1) the Cybersecurity Framework is not something with which an organization can "comply," and (2) even if an organization follows the NIST Cybersecurity Framework (which the FTC describes as "a set of industry standards and best practices to help organizations identify, assess, and manage cybersecurity risks"), then that does not necessarily mean an organization's cybersecurity policies will withstand regulatory scrutiny.[vi] Additionally, cybersecurity enforcement actions often are precipitated by incidents exposing sensitive third-party information, which in turn result in the near inevitable perceptions of an absence of cybersecurity buy-in from management teams and a failure to fully appreciate various cybersecurity risk vectors. Periodic spot-checks of corporate policies, and even implemented practices, can miss these issues; meanwhile, an independent and informed monitor with appropriate in-depth knowledge of a company's remedial efforts undertaken pursuant to a settlement agreement would be well-positioned to identify and remediate corporate deficiencies while simultaneously satisfying regulators' expectations.

Properly addressing modern and emerging corporate and regulatory cybersecurity concerns demands a new compliance prism and model as part of settlement agreements with government agencies. Rather than simply accepting periodic external assessments, matters involving cybersecurity should be addressed more effectively through the use of a cyber-knowledgeable independent corporate monitor. That monitor will be able to appreciate the technical cyber and substantive needs of the subject company, have intimate knowledge of that company, and understand the goals and objectives of the regulatory body with the cyber-compliance expectations. Equally important is that the monitor will be in a position to ensure – from an informed position – that the company implements proper cybersecurity practices, and the Board, management and staff receive appropriate cyber-training. Thus, the not-too-distant future is now for cybersecurity monitoring and monitors.

[i] U.S. Securities & Exchange Commission, *SEC Announces 2017 Examination Priorities* (Jan. 12, 2017), https://www.sec.gov/news/pressrelease/2017-7.html.
[ii] U.S. Securities & Exchange Commission, *SEC Announces 2016 Examination Priorities* (Jan. 11, 2016), https://www.sec.gov/news/pressrelease/2016-4.html.
[iii] U.S. Securities & Exchange Commission, *OCIE's 2015 Cybersecurity Examination Initiative* (Sept. 15, 2015), https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.
[iv] *E.g., Federal Trade Commission v. Wyndham Worldwide Corporation*, 799 F.3d 236 (3d Cir. 2015); *Federal Trade Commission v. D-Link Corp.*, No. 3:17-cv-00039 ((N.D. Cal. Compl. filed Jan. 5, 2017)).
[v] https://www.sec.gov/Archives/edgar/data/1011006/000119312517065791/d293630d10k.htm.
[vi] See Andrea Arias, Fed. Trade Comm., *The NIST Cybersecurity Framework and the FTC* (Aug. 31, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the areas of government investigations (including SEC and FTC), cybersecurity and corporate monitorships. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Jacob S. Frenkel is a Member in Dickinson Wright's Washington, DC office and Chairs the Firm's Government Investigations and Securities Enforcement Practice. He is a former U.S. federal criminal prosecutor of public corruption and securities laws, a former SEC Enforcement lawyer, and is one of the founding directors of the International Association of Independent Corporate Monitors. Mr. Frenkel can be reached at 202.466.5953 or jfrenkel@dickinsonwright.com.

Justin L. Root is Of Counsel in Dickinson Wright's Columbus, Ohio office and leads the firm's Cybersecurity Practice. He is a former Special Agent for the Ohio Bureau of Criminal Investigation's Cyber Crimes Unit, a former Special Deputy United States Marshal on the FBI's Cybercrime Taskforce, and a current member of the Ohio Attorney General's Legal Cybersecurity Subcommittee. Mr. Root can be reached at 614.591.5465 or jroot@dickinsonwright.com.