Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

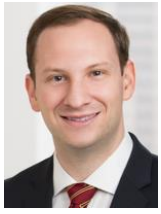
Directors Must Heed SEC On Cybersecurity And Social Media

By **Clifford Thau, Amy Riella, Laurel Fensterstock and W. Logan Lewis**
(May 20, 2019, 3:24 PM EDT)


Clifford Thau


Amy Riella


Laurel Fensterstock


W. Logan Lewis

In recent years, the U.S. Securities and Exchange Commission has demonstrated an increased willingness to investigate and enforce violations of the federal securities laws arising from cybersecurity breaches and information disseminated through a company's social media outlets, including by bringing actions directly against individual directors and officers.

SEC guidance and enforcement actions make clear that the SEC expects companies to take certain precautions with respect to avoiding and remediating cybersecurity breaches, and that the SEC now views information disclosed via social media as a formal disclosure made by a company, which in turn will be subject to the SEC's reporting requirements and regulations.

As a result of several high-profile cyber breaches and matters involving disclosures through social media, officers and directors are increasingly involved with their companies' cybersecurity and social media strategies. Despite this increased awareness, reports indicate that many officers and directors remain insufficiently protected from potential enforcement actions — and underprepared for SEC compliance inspections and examinations relating to cybersecurity and social media.

Corporate Directors, Cybersecurity and Social Media

PricewaterhouseCoopers' 2018 Annual Corporate Directors Survey revealed that, while directors are generally aware of risks associated with cybersecurity and social media, most boards do not have a written process or policy for addressing cybersecurity breaches, including disclosure of the same.[1]

Moreover, the PwC survey demonstrated that many directors are not aware that by disseminating information about their company through social media, they expose the company to potential violations of the federal securities laws.

Specifically, while 95% of directors PwC surveyed reported that their boards or companies had taken steps to prepare for potential cybersecurity incidents (including receiving increased reporting metrics on cybersecurity, increasing the budget associated with

cybersecurity and engaging third-party advisors), many directors do not prioritize the need of employing an individual with cyber risk expertise within the company.[2]

Additionally, only 47% of directors surveyed reported that their company had created a written policy for addressing cybersecurity breaches, and only 28% of directors surveyed have participated in simulated crisis management scenarios. With respect to social media, just 54% of directors surveyed reported that their board is involved in their company's monitoring of social media. Presumably, if directors understood how great their exposure in this area can be, they would be more heavily involved in such monitoring.

2018 SEC Annual Report of the Division of Enforcement

In 2018, the SEC's Division of Enforcement pledged to keep pace with technological change.[3] On Feb. 21, 2018, the SEC issued guidance concerning companies' disclosure obligations under existing law regarding (1) cybersecurity risk and incidents;[4] (2) cybersecurity policies and procedures; (3) disclosure controls and procedures; (4) insider trading prohibitions; and (5) Regulation FD and selective disclosure prohibitions in the cybersecurity context.

SEC chairman Jay Clayton referenced the SEC guidance in a speech on Dec. 6, 2018,[5] during which he emphasized the importance of sufficient disclosures around cyber risks to ensure that "investors are sufficiently informed about the material cybersecurity risks and incidents affecting the companies in which they invest."

Clayton further stated that it was imperative for public companies to have "disclosure controls and procedures that enable [them] to make accurate and timely disclosures about material cybersecurity events, as well as policies that protect against corporate insiders trading in advance of company disclosures of material cyber incidents." And he reiterated the fact that the SEC will "continue to prioritize cybersecurity in [its] examinations of market participants, including broker-dealers, investment advisers and critical market infrastructure utilities."

2018 Enforcement Actions Policing Cyber-Related Misconduct

The SEC's enhanced focus on these areas should come as no surprise. With the formation of the SEC's Cyber Unit[6] in September 2017, the enforcement division signaled its intent to formally police cyber-related misconduct.

In 2018, the SEC brought 20 standalone enforcement actions, and, as of the end of 2018, had more than 225 open cyber-related investigations. Among others, a few noteworthy enforcement actions include:

Altaba

The SEC's enforcement action against the entity formerly known as Yahoo! Inc., now known as Altaba Inc.,[7] one of the world's largest internet media companies, was the first cause of action brought by the SEC against a public company for failing to properly inform investors about a cyber breach.[8] Without admitting or denying the SEC's allegations, Yahoo agreed to resolve the enforcement action, paying $35 million.

The SEC alleged that Yahoo misled investors by failing to disclose what was considered at the time to be the largest known theft of user data within the first few days that followed the breach. Specifically, the

SEC alleged that in December 2014, Yahoo's information security team learned that Russian hackers had stolen usernames, email addresses, phone numbers, birthdates, encrypted passwords and security questions and answers for hundreds of millions of user accounts.

Although information relating to the breach was reported to members of Yahoo's senior management and legal department, Yahoo allegedly failed to (1) properly investigate the circumstances of the breach, and (2) adequately consider whether the breach should be disclosed to investors. The breach was not disclosed to the public until 2016, when Verizon was in the process of acquiring Yahoo's operating business.

The SEC further alleged that Yahoo never disclosed the breach, its potential business impact or its potential legal implications in any of the quarterly and annual reports filed with the SEC during the two-year period following the breach. Additionally, the SEC alleged that Yahoo did not share information relating to the breach with its auditors or outside counsel in order to assess the company's potential disclosure obligations, and that Yahoo failed to maintain disclosure controls and procedures designed to ensure that reports from its information security team concerning cyber breaches — or the risk of such breaches — were properly and timely assessed for potential disclosure.

Voya

The SEC brought cease-and-desist proceedings against Voya Financial Advisors Inc., an Iowa-based broker-dealer and investment adviser, stemming from VFA's alleged failure to maintain adequate cybersecurity policies and procedures.[9] In April 2016, VFA experienced a cyber intrusion that compromised the personal information of thousands of its customers in violation of Regulations S-P and S-ID.

This was the SEC's first ever action charging violations of Regulation S-ID, known as the Identity Theft Red Flags Rule.[10] Without admitting or denying the SEC's allegations, VFA agreed to resolve the matter with the SEC for $1 million.

According to the SEC, cyber intruders impersonated VFA contractors over a six-day period by calling VFA's support line and requesting that the contractors' passwords be reset. The intruders used the new passwords to gain access to the personal information of 5,600 VFA customers. The intruders then used the customer information to create new online customer profiles and to obtain unauthorized access to account documents for three customers.

The SEC alleged that VFA's failure to terminate the intruders' access stemmed from weaknesses in its cybersecurity procedures, and that VFA failed to apply its procedures to the systems used by its independent contractors, who comprise the largest part of VFA's workforce.

2018 Enforcement Actions Related to Social Media Communications

In perhaps the most widely publicized SEC enforcement action of 2018, the SEC charged Elon Musk, chairman and CEO of Tesla Inc., an American automotive and energy company based in Palo Alto, California, with securities fraud for tweeting a series of allegedly false and misleading statements about his plan to take Tesla private.[11]

The SEC alleged that Musk violated Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5, 17 C.F.R. § 240.10b-5, because his tweets were false and misleading disclosures subject to the federal

securities laws. The SEC also charged Tesla with failing to maintain disclosure controls and procedures over Musk's communications via his Twitter account.[12]

According to the complaint against Tesla, on Nov. 5, 2013, Tesla publicly filed a Form 8-K with the SEC stating that it intended to use Musk's Twitter account as a means of announcing material information to the public about Tesla and its products and services, and has encouraged investors to review the information about Tesla published by Musk via his Twitter account. The complaint further alleged that Musk has used his Twitter account since then to distribute material information about Tesla, including company financial projections and key non-financial metrics.

According to the complaint, Tesla violated Rule 13a-15, 17 C.F.R. § 240.13a-15 of the Exchange Act, 15 U.S.C. § 78a, et seq., because Tesla had not implemented disclosure controls or procedures to assess whether the information Musk disseminated via his Twitter account should be disclosed in reports Tesla files pursuant to the Exchange Act, or to ensure that the information Musk published via his Twitter account was accurate or complete.

As part of the final judgment entered on Oct. 16, 2018, Musk and Tesla each agreed to resolve the matter with the SEC for $20 million in penalties.[13] While the terms of the settlements did not require Musk or Tesla to admit or deny guilt, the settlements did require that Musk step down as Tesla's chairman, to be replaced by an independent chairman.

As a result, Musk will be ineligible to be reelected chairman for three years. The settlements also required Tesla to appoint two new independent directors to its board, establish a new committee of independent directors and put in place additional controls and procedures to oversee Musk's communications.

On Feb. 25, 2019, the controversy between Musk and the SEC entered a new phase, when the SEC filed a motion in the United States District Court for the Southern District of New York[14] seeking an order to show cause as to why Musk should not be held in contempt for violating the final judgment[15] when he allegedly tweeted, on Feb. 19, 2019, that "Tesla made 0 cars in 2011, but will make around 500k in 2019."

According to the SEC, a few hours later, after consulting with Tesla's "designated securities counsel," Musk tweeted a correction: "Meant to say annualized production rate at end of 2019 probably around 500k, ie 10k cars/week. Deliveries for year still estimated to be about 400k."

The SEC alleged that Musk's first tweet violated the final judgment, which required that Musk seek preapproval of any written communications, including social media posts, that "contain, or reasonably could contain, information material to [Tesla] or its shareholders."

In response, Musk argued that he not only complied with the final judgment, but he also complied with Tesla's internal "Senior Executives Communication Policy".[16] Musk argued that, pursuant to the policy, he is entitled to use his discretion when making the determination as to whether information is material, and in this case he used his discretion and made the determination that the information was immaterial.

On April 26, 2019, the SEC and Musk reached an agreement to resolve the SEC's contempt motion, and successfully sought to amend the final judgment to require Musk to "obtain pre-approval of an experienced securities lawyer employed by [Tesla] … of any written communication that contains

information" regarding various topics related to Tesla's business.[17]

The SEC and Musk agree that "[t]his enhanced clarity will reduce the likelihood of future disputes regarding compliance with this provision of the Final Judgment." The amendment underscores the SEC's enhanced focus on disclosures made through social media by officers and other key personnel of public companies.

Regulatory Agencies' 2019 Focus on Cybersecurity

Like the SEC's Division of Enforcement, the SEC's Office of Compliance Inspections and Examinations, or OCIE, and the Financial Industry Regulatory Authority, or FINRA, have recently indicated that a focus for 2019 will be misconduct relating to cybersecurity and social media.

Having insufficient cybersecurity strategies and plans to monitor a company's social media presence could leave officers and directors unprepared for examinations and inspections performed by the OCIE, and for any regulatory action brought by FINRA.

OCIE 2019 Priorities

In accordance with the Government Performance and Results Modernization Act of 2010, which requires federal agencies to outline their missions, planned initiatives and strategic goals for a four-year period, on Oct. 11, 2018, the SEC published its new strategic plan.[18]

The strategic plan reiterated the importance of examinations. Indeed, it described using examination resources, such as the OCIE, as a "core principle" in its mission to protect investors, maintain fair, orderly and efficient markets, and facilitate capital formation.

Relatedly, the OCIE recently announced that cybersecurity was among its 2019 examination priorities.[19] Because the OCIE has determined that cybersecurity protection is critical to the operation of the financial markets, and that a successful cyberattack may have consequences that extend far beyond the specific company to other market participants and retail investors, the OCIE plans to prioritize cybersecurity in each of its five program areas — Investment Adviser/Investment Company, Broker-Dealer and Exchanges, Clearance and Settlement, FINRA and Securities Industry Oversight, and the Technology Controls Program.

The OCIE is working with companies to identify and manage cybersecurity risks, and to encourage market participants to actively and effectively engage in this effort. The OCIE has indicated that examinations will focus on "proper configuration of network storage devices, information security governance generally, and policies and procedures related to retail trading information security."

The SEC reiterated its focus on cybersecurity during the highly publicized and well-attended Practising Law Institute's SEC Speaks conference held on April 8, 2019.[20] During this conference, Pete Driscoll, director of the OCIE, reaffirmed that the OCIE is "still pushing forward on [its] priorities," including cybersecurity. Likewise, SEC chairman Clayton stated during the conference that cybersecurity is an area presenting heightened risks, and thus will continue to be an area of focus in 2019.[21]

FINRA's 2018 Report on Cybersecurity Practices

In December 2018, FINRA issued its Report on Selected Cybersecurity Practices — 2018, which

"present[ed] FINRA's observations regarding effective practices that firms have implemented to address selected cybersecurity risks."[22]

The report covered five topics that FINRA identified through its examination program as primary challenges: (1) branch office cybersecurity controls; (2) phishing attacks; (3) insider threats; (4) the elements of a strong penetration testing program; and (5) controls over mobile devices.

A common theme throughout the report is that the success of a company's cybersecurity program depends largely on developing a corporate culture that focuses on cybersecurity awareness and providing regular cybersecurity training. Moreover, the report concluded that penetration testing (often referred to as a "pen test") is critical to the success of many companies' cybersecurity programs.

A pen test simulates an attack on a company's computer network to determine the vulnerabilities in the network and to evaluate the effectiveness of the company's protective measures. The process requires an active analysis of a company's network, applications or other targets for any weaknesses.

Conclusion

The SEC's 2018 enforcement actions and the 2019 priorities of the enforcement division, the OCIE and FINRA collectively demonstrate that regulators are heavily focused on cybersecurity and the use of social media. In contrast, PwC's 2018 Directors Survey indicates that while many directors and officers are generally aware of the risks related to cybersecurity and social media disclosures, their companies have not adopted written plans for addressing, remediating or disclosing cybersecurity breaches, nor have they adopted policies for reviewing and vetting social media content.

By designating a cybersecurity expert on their boards, creating written escalation policies in the event of a cyber breach and participating in simulated crisis management scenarios, directors will be better prepared to prevent and address issues relating to cybersecurity.

Additionally, as regulators are treating information disseminated through social media as formal disclosures issued by a company, it would benefit companies, as well as their officers and directors, to ensure that their employees and representatives are educated in this area, understand the risks associated with the information they share and monitor closely the substance of the material publicized.

Clifford Thau and Amy Lamoureux Riella are partners, Laurel S. Fensterstock is a senior associate and W. Logan Lewis is an associate at Vinson & Elkins LLP.

[1] PwC, 2018 Annual Corporate Directors Survey, October 2018, at 12, 34.

[2] The percentage of directors rating the need to have cyber risk expertise within the respective organization as a high priority fell 14% from 2016 to 2018. Id.

[3] See Div. of Enf't, U.S. Sec. & Exch. Comm'n, ANN. REP. 2018, https://www.sec.gov/files/enforcement-annual-report-2018.pdf.

[4] Statement and Guidance on Public Cybersecurity Disclosures, Exchange Act Release Nos. 33-10459, 34-82746, 83 Fed. Reg. 8166, 8168-70 (SEC, Feb. 26, 2018).

[5] See Jay Clayton, Chairman, U.S. Sec. & Exch. Comm'n, SEC Rulemaking Over the Past Year, the Road Ahead and Challenges Posed by Brexit, LIBOR Transition and Cybersecurity Risks (Dec. 6, 2018).

[6] The Division of Enforcement's Cyber Unit focuses on violations involving digital assets, initial coin offerings and cryptocurrencies; cybersecurity controls at regulated entities; issuer disclosures of cybersecurity incidents and risks; trading on the basis of hacked nonpublic information; and cyber-related manipulations, such as brokerage account takeovers and market manipulations using electronic and social media platforms. See U.S. Sec. & Exch. Comm'n, Spotlight on Cybersecurity, the SEC and You, https://www.sec.gov/spotlight/cybersecurity (last visited Apr. 29, 2019); see also Press Release, U.S. Sec. & Exch. Comm'n, SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors (Sept. 25, 2017), https://www.sec.gov/news/press-release/2017-176.

[7] Altaba Inc., Securities Act Release No. 10485, Exchange Act Release No. 83096, Accounting and Auditing Enforcement Release No. 3937 (Apr. 24, 2018). On June 16, 2017, Yahoo changed its name to Altaba in connection with its sale to Verizon Communications, Inc. The company operated as Yahoo during all relevant times related to the SEC's cease-and-desist order.

[8] Notably, Yahoo neither admitted nor denied the findings in the SEC's order, which required the company to cease and desist from further violations of Sections 17(a)(2) and 17(a)(3) of the Securities Act of 1933, Section 13(a) of the Securities Exchange Act of 1934 and Rules 12b-20, 13a-1, 13a-11, 13a-13 and 13a-15.

[9] Voya Fin. Advisors Inc., Exchange Act Release No. 84288, Investment Advisers Act Release No. 5048 (Sept. 26, 2018).

[10] "On January 1, 2011, the Federal Trade Commission (FTC) began enforcing its Fair and Accurate Credit Transactions Act of 2003 (FACT Act) Red Flags Rule. The Red Flags Rule requires that each 'financial institution' or 'creditor' — which includes most securities firms — implement a written program to detect, prevent, and mitigate identity theft in connection with the opening or maintenance of 'covered accounts.' These include consumer accounts that permit multiple payments or transactions, such as a retail brokerage account, credit card account, margin account, checking or savings account, or any other accounts with a reasonably foreseeable risk to customers or your firm from identity theft. On July 21, 2011, the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) transferred responsibility for rulemaking and enforcement of identity theft Red Flag Rules and guidelines to the SEC and the [Commodity Futures Trading Commission] for the firms they regulate. On April 19, 2013, the SEC and CFTC published their joint final Identity Theft Red Flags Rules and guidelines with a compliance date of November 20, 2013. The SEC rule is called Regulation S-ID." The joint rules and guidelines align with the FTC Red Flags Rule and guidelines. Fin. Indus. Regulatory Author., SEC Identity Theft Red Flags Rule, http://www.finra.org/industry/sec-identity-theft-red-flags-rule (last visited Apr. 29, 2019).

[11] Complaint, SEC v. Musk, No. 18-cv-8865 (S.D.N.Y. Sept. 27, 2018).

[12] Complaint ¶ 1, SEC v. Tesla Inc., No. 18-cv-8947 (S.D.N.Y. Sept. 29, 2018).

[13] Press Release, U.S. Sec. & Exch. Comm'n, Elon Musk Settles SEC Fraud Charges; Tesla Charged with and Resolves Securities Law Charge (Sept. 29, 2018), https://www.sec.gov/news/press-release/2018-226.

[14] SEC's Motion in Support of Order to Show Cause, SEC v. Musk, No. 18-cv-8865 (Feb. 25, 2019).

[15] Id. See also Final Judgment, SEC v. Musk, No. 18-cv-8865 (Oct. 16, 2018).

[16] Response to Order Show Cause at 1, SEC v. Musk, No. 18-cv-8865 (Mar. 11, 2019).

[17] Consent Motion to Amend Final Judgment, SEC v. Musk, No. 18-cv-08865 (Apr. 26, 2019).

[18] U.S. Sec. Exch. Comm'n, Strategic Plan Fiscal Years 2018-2022, 6, 10 (2018), https://www.sec.gov/files/SEC_Strategic_Plan_FY18-FY22_FINAL_0.pdf.

[19] Office of Compliance Inspections and Examinations, U.S. Sec. & Exch. Comm'n 2019 Examination Priorities, 5,11 (2018), https://www.sec.gov/files/OCIE%202019%20Priorities.pdf.

[20] See Melanie Waddell, SEC "Still Struggling" With Advisor Exam Rate, ThinkAdvisor (Apr. 8, 2019), https://www.thinkadvisor.com/2019/04/08/sec-still-struggling-with-advisor-exam-rate/.

[21] See Jay Clayton, Chairman, U.S. Sec. Exch. Comm'n, Management's Discussion and Analysis of the SEC: Remarks at the "SEC Speaks" Conference (Apr. 8, 2019), http://www.sec.gov/news/speech/speech-clayton-040819.

[22] Fin. Indus. Regulatory Auth., Report on Selected Cybersecurity Practices — 2018, FINRA, 1 (2018), https://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf.