Clients&FriendsMemo

Equifax Data Breach Highlights SEC Disclosure Obligations for Public Companies in the Wake of Cybersecurity Attacks

September 18, 2017

On September 7, 2017, Equifax, one of the country's three primary credit reporting bureaus, announced it had suffered a major cybersecurity breach that could potentially affect half of the U.S. population.[1] According to the company, it learned on July 29, 2017, that in mid-May 2017, hackers had gained access to its information systems and stole Social Security numbers, birth dates, addresses, and driver's license numbers for approximately 143 million of its customers, along with credit card numbers for over 200,000 customers. Since then, it has been separately reported that during the approximately five weeks between discovery of the breach and public disclosure, three senior executives sold approximately $1.8 million in Equifax shares.[2] Meanwhile, since Equifax's announcement, the company has lost $4 billion in market value, spurring at least one securities class action lawsuit along with a wave of consumer class action lawsuits and scrutiny by Congress.[3] In addition to the financial, litigation, and public relations costs that Equifax will now face – and the scrutiny to be applied as to whether the executives traded on non-public information – the event is an opportunity to review the expectations of the Securities and Exchange Commission ("SEC") regarding public companies' internal policies, procedures, and controls for managing cybersecurity threats, as well as how they handle disclosure of cybersecurity risks and events to customers and the investing public.

I. SEC Disclosure Guidance

In October 2011, the SEC's Division of Corporation Finance issued non-binding guidance on reporting obligations for public companies regarding cybersecurity risks and cyber incidents (the

[1] Equifax Press Release, *Equifax Announces Cybersecurity Incident Involving Consumer Information* (Sept. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.

[2] Anders Melin, *Three Equifax Managers Sold Stock Before Cyber Hack Revealed*, Bloomberg (Sept. 7, 2017, 5:59 PM), https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack.

[3] Barb Darrow, *Senators Want Answers From Equifax Over Its Massive Data Breach*, Fortune.com (Sept. 12, 2017), http://fortune.com/2017/09/12/equifax-data-breach-senate-finance-committee/.

"Disclosure Guidance").[4] The Disclosure Guidance recognized that while no existing disclosure requirement explicitly referred to cybersecurity, the growing reliance of companies on digital technologies meant that such risks and events could be sufficiently material to investors such that they may be required to be disclosed in registration statements, financial statements, and periodic reports such as Forms 8-K. As a result, public companies should review, on an ongoing basis, the adequacy of their disclosure policies relating to cybersecurity risks and cyber incidents along with other operational and financial risks.

- *Cybersecurity Risks*. The Disclosure Guidance suggested that companies should disclose the risk of cyber incidents if these issues are "among the most significant factors that make an investment in the company risky." In determining whether to report any cybersecurity risks, companies should consider, among other things, (i) the probability of a cybersecurity incident occurring; (ii) the potential magnitude and costs associated with the risk; (iii) prior cybersecurity incidents; and (iv) the adequacy of possible preventative measures. The Disclosure Guidance cautioned against "boilerplate" disclosures and, instead, advised that companies tailor the discussion of their specific cybersecurity risks. It emphasized, however, that companies need not disclose information that would, in itself, compromise its ability to defend against cyberattacks.

- *Cyber Incidents.* The Disclosure Guidance also set forth a number of considerations regarding the disclosure of cyber incidents, including whether (i) the incident will have a material effect on the company's financial condition; (ii) material intellectual property was stolen; (iii) the cyber incident materially affected products, services, or customer relationships; and (iv) the company has been subject to prior data breaches. A company should also consider the impact of remediation costs for stolen assets and information, repairs to internal systems that hackers may have compromised, and the necessity of engaging outside firms to assist with breach response and remediation.

The SEC has yet to bring an enforcement action over cybersecurity disclosures. In late 2013, when personal information belonging to 110 million customers were hacked from Target, the company reportedly faced an SEC investigation into its breach disclosures, which came several weeks following the discovery of the attack.[5] The Target investigation closed without an enforcement action. More recently, it has been reported that the SEC is investigating Yahoo for the nearly two-year delay between when Yahoo executives learned of a significant data breach and

[4] *CF Disclosure Guidance: Topic No. 2*, Division of Corporation Finance Securities and Exchange Commission (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[5] Ellen Rosen, *SEC Won't Recommend Enforcement Action Over Target's Data Breach*, Bloomberg Law (Aug. 27, 2015), https://bol.bna.com/sec-wont-recommend-enforcement-action-over-targets-data-breach/.

when the breach was reported to the public.[6] The incident led to Yahoo's general counsel resigning after an independent committee found that the legal team failed to sufficiently investigate the company's 2014 data breach of 500 million users' names, email addresses, birth dates, and telephone numbers, causing the company to fail to act adequately in response.

II. Adequacy of Equifax Disclosures

Given the magnitude and severity of the breach, Equifax is likely to face questions from the SEC, Congress, and investors regarding the adequacy of its pre- and post-breach disclosures of cybersecurity risks. These inquiries will likely focus on:

- Whether Equifax had identified material cybersecurity risks and vulnerabilities before the breach that were not disclosed;
- What steps Equifax took to investigate the breach following its discovery;
- Whether the volume and nature of the data exposed was immediately apparent to Equifax;
- When Equifax executives were informed of the breach; and
- Whether Equifax's post-breach disclosure was complete and accurate.

In addition, Equifax will likely be probed as to the timeliness of its disclosure, which came 41 days after its discovery of the breach. While this is far less than the nearly two-year disclosure delay by Yahoo, it is still likely to come under scrutiny. The Disclosure Guidance is silent as to the timing of the disclosure of a cyber event, leaving ambiguous how much time is reasonable for a company to wait before disclosing the existence and details of an attack to the public. This could depend on a multitude of factors, including the complexity of the breach, how quickly its scope and volume could be determined, and whether there is an active law enforcement investigation pending. And even if the SEC does not bring an enforcement action against Equifax based on the adequacy of its disclosures, the SEC will also likely be looking at the company's cybersecurity controls and related policies and procedures.

III. Scrutiny of Trading Activity

The other issue that may result in an SEC inquiry is the sale by three Equifax executives of almost $1.8 million of shares shortly after discovery of the breach. The events reportedly took place as

[6] Aruna Viswanatha & Robert McMillan, *Yahoo Faces SEC Probe Over Data Breaches*, The Wall Street Journal (Jan. 23, 2016, 9:56 AM), https://www.wsj.com/articles/yahoo-faces-sec-probe-over-data-breaches-1485133124.

follows: on July 29, 2017, Equifax discovered the breach; on August 1, 2017, two Equifax executives sold shares worth over $1.5 million; and on August 2, 2017, a third company executive sold over $250,000 worth of stock. Notably, the transactions were not part of each executive's scheduled trading plans, and they preceded a nearly $4 billion drop in market value following the company's disclosure of the attacks.

To prove insider trading, prosecutors would have to show that each Equifax executive traded on material non-public information about the company.[7] In response to questions about the transactions, an Equifax spokesperson said the executives "had no knowledge that an intrusion had occurred at the time" they sold their stock. Nevertheless, the possibility of SEC scrutiny of these trades offers a cautionary tale for businesses and executives. It is important that senior leadership be closely involved in responding to serious cybersecurity incidents, primarily to ensure that the response is coordinated and given appropriate priority, but also to prevent a situation where senior executives are not aware of a serious breach and can unwittingly appear to have traded on material non-public information.

IV. Conclusion

Since taking office earlier this year, newly appointed SEC Chair Jay Clayton has emphasized that disclosure requirements extend to cybersecurity issues, stating that "[p]ublic companies have a clear obligation to disclose material information about cyber risks and cyber events. I expect them to take this requirement seriously."[8] Along the same lines, Stephanie Avakian, the Co-Director of Enforcement, has stated that the SEC "absolutely" would bring an enforcement action for failure to make an appropriate cybersecurity disclosure.[9] How the SEC responds to the Equifax breach in the coming months may shed light on its approach to cybersecurity disclosure going forward. Meanwhile, companies at risk of significant cyberattacks should implement a fulsome cybersecurity defense against potential hackers, develop an action and response plan in the event a cyberattack does take place, and ensure that adequate pre- and post-breach disclosures are made to regulators, customers, and the investing public.

---

[7] Section 10(b) of the Securities Exchange Act of 1934, and Rule 10b-5 thereunder, state that a person cannot purchase or sell a security "on the basis of material nonpublic information…in breach of a duty of trust or confidence that is owed directly, indirectly, or derivatively, to the issuer of that security or the shareholders of that issuer, or to any other person who is the source of the material nonpublic information." 17 C.F.R. § 240.10b5-1 (2017).

[8] *Remarks at the Economic Club of New York*, United States Securities and Exchange Commission (July 12, 2017), https://www.sec.gov/news/speech/remarks-economic-club-new-york.

[9] *See* Jimmy Hoover, *SEC Suits Over Cyber Reporting Could Be on Horizon*, Law360 (Apr. 20, 2017, 1:25 PM), https://www.law360.com/articles/915377/sec-suits-over-cyber-reporting-could-be-on-horizon.

* * *

Should you have any questions about this summary, please contact:

Joseph Moreno	+1 (202) 862-2262	joseph.moreno@cwt.com
Kyle DeYoung	+1 (202) 862-2288	kyle.deyoung@cwt.com
Joseph Facciponti	+1 (212) 504-6313	joseph.facciponti@cwt.com
Peter Carey	+1 (202) 862-2339	peter.carey@cwt.com
Stephen Weiss	+1 (202) 862-2347	stephen.weiss@cwt.com