Houston, we have a breach. Now what? Lessons learned from the SEC's Facebook settlement

Corporate Governance Alert

31 July 2019
By: Sanjay M. Shirodkar

In late July 2019, Facebook Inc. entered into a settlement with the Securities and Exchange Commission (the SEC) for making misleading disclosures regarding the risk of misuse of its user data. The SEC asserted that the company had discovered the misuse in 2015, but failed to correct its existing risk factor disclosure for more than two years. Instead, the company's risk factors informed investors that "our users' data *may* be improperly accessed, used or disclosed" (*emphasis added*). The company disclosed the incident, but not until March 2018, leading to a large drop in its stock price. The company agreed to pay $100 million to settle the SEC's charges.[1]

Public companies and the general public are becoming increasingly aware of the fact that some sort of cybersecurity breach is being disclosed on a weekly and even daily basis. Much has been written about preventing breaches. But what should companies think about doing when they become aware of a breach? What are some of the lessons learned from the SEC's guidance on this topic, and from the Facebook proceedings? This article explores these topics.

Prior SEC guidance

Here is a brief summary of the relevant SEC and staff guidance:

- **CF Disclosure Guidance: Topic No. 2, Cybersecurity, Division of Corporation Finance (October 13, 2011**) – the staff of the Division of Corporation Finance provided guidance on how a company could address cybersecurity from a disclosure point of view.[2] The staff guidance reminded issuers to view cybersecurity as a business risk that, like other risks, might require disclosure if it could materially impact a company's operations.
- **Commission Statement and Guidance on Public Company Cybersecurity Disclosures (February 26, 2018**) – the SEC issued interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents. This guidance reminds companies that they should consider cybersecurity risks and incidents when preparing documents that they file with the SEC as the federal securities laws require them to disclose information about material cybersecurity risks and incidents. For example, disclosure may be required in the context of a public company's existing reporting obligations, such as the company's risk factors, management's discussion and analysis, or financial statements. This guidance emphasized the importance of maintaining comprehensive policies and procedures – including effective disclosure controls and procedures – that address cybersecurity risks and incidents. The guidance also noted that company insiders that trade securities while in possession of non-public information about cybersecurity incidents may violate the federal securities laws.[3]
- **Securities and Exchange Commission Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 (October 16, 2018)** – the staff of the Division of Enforcement and Division of Corporation Finance issued a report pursuant to Section 21(a) of the Exchange Act to make issuers and other market participants aware of certain cyber-related threats and emphasized the need for issuers to consider these threats in devising and maintaining a system of internal accounting controls as required by the federal securities laws.[4]

Lessons learned on disclosure controls and procedures

As we head into the last stages of summer, here are some of the lessons we have learned from the SEC guidance on cybersecurity and the Facebook proceedings that board members and senior management of a public company should consider:

> ***Action item***: Review risk factors and other public disclosures. Confirm the accuracy of any disclosures, including risks factors posed as hypotheticals. In the Facebook proceeding, the SEC noted that hypothetical phrasing can create the impression that the episode in question has not occurred. The SEC has previously indicated its view that "it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion."[5]
>
> ***Action item***: If you have a policy on a particular topic, ensure that you have a mechanism to summarize or report material violations of the policy to the proper party responsible for ensuring the accuracy of the company' filings with the SEC. According the SEC, Facebook had a set of rules governing what developers are allowed to do with the apps they create and the user data they gathered. However, the company did not have a "specific mechanism to summarize or report" violations of these rules to employees responsible for ensuring the accuracy of its SEC filings.
>
> ***Action item***: Review existing disclosure controls and procedures. Confirm that they are designed to "enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents."[6] Ask whether these procedures will "appropriately record, process, summarize, and report the information related to cybersecurity risks and incidents that is required to be disclosed in filings."[7] The SEC observed that Facebook did not "maintain disclosure controls and procedures designed to analyze or assess incidents involving misuse of user data for potential disclosure in the company's periodic reports."
>
> ***Action item***: If an incident has occurred, should a summary of the incident be shared and discussed with outside disclosure counsel and the company's independent auditors in order to assess the company's disclosure obligations? The SEC indicated that Facebook failed to share information about the incident with its independent auditors and outside disclosure counsel in order to assess the company's disclosure obligations.

Action item: Review existing internal accounting controls to confirm that they provide reasonable "assurances that transactions are executed with, or that access to company assets is permitted only with, management's general or specific authorization."[8] As part of its investigation into several investigations where certain public issuers were the victims of cyber-related fraud, the SEC Report notes that "internal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds. Public issuers …. must calibrate their internal accounting controls to the current risk environment and assess and adjust policies and procedures accordingly."[9]

As part of the FTC proceedings, Facebook agreed to pay a record $5 billion penalty; as part of the SEC proceedings, it agreed to pay a $100 million penalty. These are extraordinarily large fines and may signal the willingness of these agencies to aggressively pursue companies deemed to violate either privacy and data security requirements within the enforcement authority of the FTC or the US federal securities laws overseen by the SEC. With summer winding down, perhaps it is time to look closely at your securities law disclosure. Think about some of the lessons learned. And ask questions.

For more information about the matters discussed in this article, please contact the author or our privacy group at with questions about privacy and data security matters.

---

[1] See, SEC press release dated July 24, 2019 - Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data (available here) and the related complaint (available here). For additional details about this proceeding, see our alert about the parallel FTC complaint and stipulated consent order here. The scope and magnitude of FTC settlement is likely to mean a more aggressive stance by the agency when it comes to enforcing its privacy and data security regime.

[2] This article only discusses the disclosure obligations of a company with respect to the U.S. federal securities laws.

[3] CF Disclosure Guidance: Topic No. 2, Cybersecurity, Division of Corporation Finance (Oct. 13, 2011), *available here.*

[4] *Commission Statement and Guidance on Public Company Cybersecurity Disclosures (February 26, 2018)*, *available here* (the SEC Guidance).

[5] *Securities and Exchange Commission Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934* (October 16, 2018), *available here* (the SEC Report).

[6] SEC Guidance on page 4.

[7] SEC Guidance at page 20.

[8] *Id.*

[9] SEC Report at page 2.

[10] SEC Report at page 6.

AUTHORS

Sanjay M. Shirodkar
Of Counsel
Washington, DC | T: +1 202 799 4000
Baltimore (Mount Washington) | T: +1 410 580 3000
