You've Been Hacked! A Cybersecurity Disclosure Guide for In-House Legal Counsel

Prepared by:
David J. Lavan and David W. Jahnke
Dinsmore & Shohl LLP

LORMAN®

Published on www.lorman.com - August 2018

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

You've Been Hacked! A Cybersecurity Disclosure Guide for In-House Legal Counsel

Written by David J. Lavan and David W. Jahnke – 4/18/18

If your company has a cybersecurity incident, this guide is intended help you think through critical disclosure requirements and will direct you to sample disclosures from other companies that have endured cybersecurity issues.

I. Introduction

With the recent string of high profile cybersecurity attacks, the U.S. Securities and Exchange Commission (the SEC) issued further guidance regarding public companies' disclosure of cybersecurity incidents. Stressing the importance of public companies developing and maintaining "disclosure controls and procedures" that allow companies to disclose such material cybersecurity incidents accurately and promptly, the new guidance is meant to "reinforce and expand" the 2011 SEC guidance on this topic. In addition, the 2018 guidance highlights public companies' need to foster procedures that prevent corporate insiders from violating insider trading laws in connection with cybersecurity incidents. The SEC is becoming increasingly vigilant in monitoring these types of incidents and related disclosures. Consequently, companies should be cognizant of the increased emphasis the SEC is placing on cybersecurity disclosures, and the priority the Division of Enforcement of the SEC is placing on enforcing insider trading laws.

II. Disclosure of Cybersecurity Threats or Incidents

A. General Overview

While there is no affirmative disclosure obligation regarding cybersecurity threats or incidents in Regulation S-K or Regulation S-X, public companies have an obligation to disclose such risks and incidents in certain circumstances. For example, Form 10-K requires companies to provide disclosure regarding material developments in their risk factors, legal proceedings, Management's Discussion and Analysis of Financial Condition and Results of Operations (the MD&A), financial statements, disclosure controls and procedures and corporate governance. A cybersecurity threat or incident could have a material effect on any of these disclosures.

B. How to Determine Whether a Cybersecurity Threat or Incident is Material?

Although securities practitioners know how to define material for purposes of disclosure, the 2018 guidance provides clarification on the definition of "material" as it pertains to disclosing cybersecurity threats or incidents. The 2018 guidance states that omitted information is considered material if a reasonable investor would find the information pertinent when making a decision to invest in the company, or if the omitted information would have changed the mix of publicly available information. Furthermore, the materiality of the cybersecurity risk or incident depends on the nature and impact the potential harm will have on a company's operations. In the SEC's view, if there is a possibility of litigation or a government investigation, or if the potential scope of harm includes the company's reputation, financial performance or its customer relationships, such a threat or incident should be considered material.

For example, Equifax Inc., in Item 1 of its 2017 Annual Report (page 2), disclosed the material impacts of a 2017 cybersecurity incident. Equifax's annual report detailed how many people were affected by the incident in each country, the reputational harm the company suffered from the incident, the effect the incident had on its financial performance, and the governmental investigation taking place because of the incident. The severity of the Equifax cybersecurity incident left no doubt as to its materiality; consequently Equifax disclosed in great detail the impact the incident had on the company.

C. Is There a Duty to Update?

Generally, public companies have a duty to correct and update any previously disclosed facts that have become materially inaccurate. The SEC understands that, after a cybersecurity threat or incident, material facts may not be readily accessible and that an ongoing external or internal investigation may affect the timing of the disclosure. However, such an investigation is not a sufficient reason for omitting material cybersecurity threats or incidents. Additionally, companies should avoid using generic language to disclose such threats or incidents, and each disclosure should be tailored to the particular facts of a given situation.

In the aforementioned Equifax cybersecurity incident, Equifax was required to disclose additional information about the incident as more information became available. Approximately seven months after its initial disclosure, in a Form 8-K filed, March 1, 2018, Equifax disclosed an additional 2.4 million U.S. consumers had their identities stolen as a result of the cybersecurity incident. These additional U.S. consumers had not been identified in prior disclosures because Equifax was not in possession of that information at the time of the prior disclosures. Thus, companies should be aware they have a duty to update previous

disclosures when necessary and that disclosure language should be tailored to their specific cybersecurity incident.

D. What Criteria Should You Consider when Determining Whether to Disclose a Cybersecurity Threat or Incident as a Risk Factor?

In accordance with Item 503(c) of Regulation S-K, a company is required to disclose significant factors that make investing in a company's securities riskier. The 2018 guidance lists criteria for companies to use when determining whether a cybersecurity threat or incident should be disclosed as a risk factor:

- if appropriate to describe an ongoing cybersecurity threat or incident, the occurrence of prior incidents;
- the probability of the cybersecurity threat occurring, and the potential impact of the incident;
- the adequacy of the company's protection against such threats;
- the business segments and operations that will be most impacted;
- the cost of maintaining such protections;
- the potential reputational harm;
- existing or pending laws and regulations that will affect the company's cybersecurity protections, and any associated costs necessary to comply with such laws and regulations; and
- any litigation, investigation and remediation costs related to the cybersecurity threat or incident.

While the SEC does not intend this to be an exhaustive list, companies should use the criteria listed above as a guide when determining whether a cybersecurity threat or incident should be disclosed as a risk factor. For example, see how Equifax addressed its cybersecurity incident in its "Risk Factors" section starting on page 14 of its 2017 Annual Report.

E*. What Criteria Should You Consider when Determining Whether to Disclose a Cybersecurity Threat or Incident in the MD&A?*

Item 303 of Regulation S-K governs disclosures regarding public companies' financial condition and business operations. The MD&A mandates addressing cybersecurity threats or incidents in the event that:

- such threat or incident would have a material effect on the results of a company's operations, liquidity or financial condition,
- such incident would cause reported financial information to not be representative of the financial condition of the company, or
- a cybersecurity threat or incident could have a material effect on a reportable segment of the company.

In its 2016 Annual Report, Yahoo! discussed a cybersecurity incident in its MD&A disclosure. While the cybersecurity incident did not have a material impact on Yahoo!'s operations, cash flow or financial condition, the company spent over $16 million investigating the cybersecurity incident, remediating the incident, and various other non-legal expenses. However, in its MD&A, Yahoo! stated it expected to have further expenses in the future regarding cybersecurity incidents, and Yahoo! disclosed they did not have cybersecurity liability insurance. Interestingly, while Yahoo! maintained the breach would not have a material effect on its business and operations, it did have an impact on shareholders. Yahoo!'s

cybersecurity incident occurred during the pendency of its sale to Verizon. Verizon's reaction to the Yahoo! cybersecurity incident included decreasing the purchase price of the stock deal by hundreds of millions of dollars. Thus, even though Yahoo! did not feel its cybersecurity incident met any of the criteria listed above, its disclosure put shareholders on notice that the event had occurred, providing some cover for the shareholder angst over the purchase price reduction.

F. How to Determine Whether a Legal Proceeding Should be Disclosed?

Pursuant to Item 103 of Regulation S-K, disclosure is required if a company is a party to material litigation as a result of a cybersecurity incident. For example, if the cybersecurity incident results in a theft of customer information, which results in the customer suing the company, that litigation should be disclosed.

Equifax, on page 25 of its 2017 Annual Report, disclosed a general overview of the "hundreds of class action" lawsuits it had become a party to as a result of its cybersecurity incident. Equifax discussed, generally, the claims against them and the damages sought from the plaintiffs. For some, the fact an extremely detailed litigation report is unnecessary will make the threshold decision of whether to disclose less painful.

G. How to Determine Whether the Impact on Financial Statements Should be Disclosed?

Companies should disclose the impact a cybersecurity incident has on its financial statements. In preparing to do so, a company should consider: (1) the expenses and costs related to the threat or incident; (2) the loss of revenue or loss of customers; (3) claims related to breach of warranties or contract, any indemnification claims, or increased insurance

premiums; and (4) diminished cash flow or any impairment to assets. As an example, Equifax, on page 30 of its 2017 Annual Report, detailed the amount of pre-tax expenses the company incurred related to the cybersecurity incident and the increase in the cost of services due to the cybersecurity incident.

H. Board Risk Oversight Disclosures

Pursuant to Item 407(h) of Regulation S-K, companies must disclose the involvement of their board of directors with risk oversight, including the board's administration of its risk oversight function and the effect that has on the board's leadership structure. The 2018 guidance stressed this obligation extends to a company's risk management as it pertains to material cybersecurity threats and incidents.

III. Disclosure Controls and Procedures

Exchange Act Rules 13a-15 and 15d-15 require public companies to have controls and procedures in place to ensure information requiring disclosure can be properly summarized and reported, within the timeframe specified in the SEC's rules and forms, and that this information can be properly communicated to the company's management so management can make prompt decisions regarding disclosure.

As it pertains to cybersecurity threats and incidents, the 2018 guidance states companies should evaluate whether they have the proper controls and procedures in place to ensure that information regarding a cybersecurity threat or incident is properly reported to the appropriate company management, in order for management to make prompt decisions regarding disclosure of such threat or incident.

Furthermore, before a company's principal executive or financial officer certifies the effectiveness of the company's controls and procedures in accordance with Exchange Act Rules 13a-14 and 15d-14, the officer should consider whether such controls and procedures are sufficient for "assessing and analyzing" any potential cybersecurity threat or incident.

IV. Insider Trading

Companies should also be aware of insider trading laws as they pertain to cybersecurity threats and incidents. A corporate insider may not trade securities "on the basis of material nonpublic information" about that security or issuer. A corporate insider trading securities based on nonpublic information relating to a material cybersecurity threat or incident is in violation of insider trading laws. The SEC has stressed the importance of companies adopting policies and procedures to prevent such violations. Proactive measures used by a company can prevent violations of insider trading law and can also prevent the appearance of insider trading. The 2018 guidance recommended that companies impose a blackout period when investigating significant cybersecurity threats or incidents. This blackout period ensures company insiders are not trading company securities "on the basis of material nonpublic information" during a company's investigation of a cybersecurity threat or incident. Finally, companies should be aware of selective disclosure and make sure they are disclosing information in accordance with Regulation FD.

V. Conclusion

The SEC will be closely monitoring companies to ensure they are properly disclosing cybersecurity threats and incidents. Accordingly, companies should reassess their current controls and procedures to ensure they facilitate accurate, timely disclosures of cybersecurity threats and

incidents. Furthermore, companies should proactively adopt procedures to prevent corporate insiders from trading on nonpublic information during a cybersecurity threat or incident.

Please contact a Dinsmore attorney if you have any questions regarding disclosure of cybersecurity threats or incidents.