ILLINOIS BUSINESS LAW JOURNAL

WHEN TO DISCLOSE DATA BREACHES UNDER FEDERAL SECURITIES LAWS

❖ ARTICLE ❖

*Steven P. Wittenberg**

TABLE OF CONTENTS

I. INTRODUCTION

Hacking and cybercrime are on the rise.[1] From 2013 to 2015, twenty major data breaches were reported at Fortune 100 companies.[2] Publicly traded

[1] *The Rise of the Hacker*, ECONOMIST (Nov. 7, 2015), http://www.economist.com/news/business/21677638-rise-hacker.
[2] *How to Disclose a Cybersecurity Event: Recent Fortune 100 Experience*, DEBEVOISE & PLIMPTON (Sept. 12, 2016),

*J.D. Candidate, Class of 2018, University of Illinois College of Law.

companies who have securities disclosure obligations should be aware of their duties under the federal securities laws when it comes to data breaches and hacks.[3]

In 2011, the SEC Division of Corporation Finance issued guidelines for cyber incidents.[4] The SEC stated, "[A] number of disclosure requirements may impose an obligation on registrants to disclose such [cyber] risks and incidents," although there are no explicit requirements referring to data breaches.

While major data breaches may be material to reasonable investors of public companies, there is no duty to promptly disclose the occurrence of cyber incidents unless there have been selective disclosures, previous misstatements or circumstances making the omission of the hack misleading.[5] The federal securities laws also impose periodic disclosure duties on public companies.

II. MATERIALITY: A COMMON THRESHOLD

Often, the duty to disclose cyber incidents hinges on the severity or materiality of the hack (e.g. Regulation FD). A hack is material if there would be a "substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information available."[6] Put differently, a hack is material "if there is a substantial likelihood that a reasonable shareholder would consider [the undisclosed data breach] important in deciding how to vote."[7]

Cyber incidents are problematic for public companies because they may be material to investors. The effects of hacking might include reduced cash flow, product recalls, contractual obligations, legal liabilities, impairment of assets such as goodwill and software, and devalued intellectual property. Depending on the severity of the effect, hacks may qualify as "material," fulfilling one of the elements sometimes required for disclosure.

---

http://www.debevoise.com/~/media/files/insights/publications/2016/09/20160912_how_to_disclose_a_cybersecurity_event_recent_fortune_100_experience.pdf.

[3] Hacking, data breaches and cyber incidents are used synonymously here. They are incidents that cause personal information to be improperly taken without the individuals' consent.

[4] *CF Disclosure Guidance: Topic No. 2*, S.E.C., https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[5] Insider trading and fraud may also create an obligation to disclose data breaches, but are not discussed here.

[6] Basic, Inc. v. Levinson, 485 U.S. 224, 231–32 (1988).

[7] TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438, 499 (1976).

III. FORM 8-K: CURRENT REPORTS

Form 8-K requires disclosure upon the occurrence of certain enumerated triggering events. There are no events listed in Form 8-K's mandatory sections that would trigger a report for data breaches except for Section 7 (Regulation FD), which is discussed below. Companies should, however, be mindful that § 409 of the Sarbanes-Oxley Act of 2002 requires that public companies "disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer . . . as the Commission determines."[8] As data breaches become more prevalent and important to the investing public, the SEC might amend Form 8-K to require real time disclosure of cyber incidents.

IV. FORM 10-K AND FORM 10-Q: PERIODIC REPORTS

A. Business

Item 101 requires a description of "the business done and intended to be done," including the "principal products and services."[9] The SEC interprets this section as requiring disclosure "[i]f one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions."[10] The SEC's interpretation is broad, so companies should keep track of the effects of hacks on their business, determine if they are material, and disclose them if they are.

B. Risk Factors

The SEC instructs that risks of hacks should be disclosed if they are "among the most significant factors that make an investment in the company speculative or risky."[11] Companies must consider past incidents, the severity and frequency of those hacks, the probability of hacking and the likely magnitude of those hacks and costs. Risk prevention and the type of industry are countervailing considerations. Companies should find a balance between identifying the specific risks without exposing cybersecurity vulnerabilities and without using overly general "boilerplate" language.

A public company that does not rely on software is a clear example in which hacking is not a risk factor. However, because companies often collect vast

---

[8] 15 U.S.C. § 78m(l) (2012).
[9] 17 C.F.R. 229.101 (2016).
[10] S.E.C., *supra* note 3.
[11] *Id.*

databases of sensitive personal information from their vendors and customers, most companies should disclose their company's cyber incident history because it bears on future risks as well as other assessed cyber threats.

C. Legal Proceedings

Companies should describe "any material pending legal proceedings" resulting from data breaches, unless the potential liability is less than or equal to 10% of the company's total assets, including subsidiaries' assets.[12] The SEC provided the example of stolen customer information which results in material litigation.[13] In any legal proceeding description, the company should also present the underlying facts surrounding the hack, but should avoid exposing cyber vulnerabilities.

D. Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A)

In the MD&A narrative, companies must "[d]escribe any unusual or infrequent events or transactions or any significant economic changes that materially affected the amount of reported income" that they "believe[] to be necessary to an understanding of its financial condition, changes in financial condition and results of operation."[14] Additionally, companies must address past incidents or future risks when

> the costs or other consequences associated with [them] represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.[15]

The MD&A easily triggers disclosure because severe hacks adversely impact "financial condition and results of operation" and can be categorized as "infrequent events," "significant economic changes," and "material event[s] [or] trend[s]."

---

[12] 17 C.F.R. 229.103 (2016).
[13] S.E.C., *supra* note 3.
[14] 17 C.F.R. 229.303 (2016).
[15] S.E.C., *supra* note 3.

V. REGULATION FD: SELECTIVE DISCLOSURE

Regulation FD requires that whenever a public company discloses material nonpublic information to certain covered parties, including broker-dealers, investment advisors, investment companies or any investor reasonably expected to trade on the information, the company must also disclose to the public.[16] A serious hack would likely fall under a duty to disclose to the public if there was a nonpublic selective disclosure because serious hacks are often material to investors. Thus, companies should refrain from selectively disclosing major hack information to those who would be reasonably expected to trade by implementing no-trade and confidentiality policies.

VI. DUTY TO CORRECT

There is no continuous duty to *update* prior disclosures; however, there is a duty to *correct* prior inaccurate statements.[17] Courts formulate the duty to correct as "when a company makes a *historical statement* that, at the time made, the company believed to be true, but as revealed by *subsequently discovered* information actually was not."[18] For example, if a Form 10-K report falsely and affirmatively stated that there were no data breaches in 2014, the company would be required to correct that statement if it later learns that, in fact, there were data breaches in 2014.

VII. DUTY TO UPDATE

When a public company decides to issue securities, it must update its registration statement with an addendum disclosing material hacks through Item 11 of Form S–3 if they were not already described in Form 10-Q or Form 8-K.[19]

VIII. CONCLUSION

In September 2016, Yahoo announced that a massive hack of over 500 million user accounts occurred in 2014. United States Senator Mark Warner (D-VA) requested that the U.S. Securities and Exchange Commission (SEC) "investigate whether Yahoo, Inc. fulfilled its obligations under federal securities

---

[16] 17 C.F.R. 243.100 (2016).
[17] Gallagher v. Abbott Labs., 269 F.3d 806, 811 (2001).
[18] In re Burlington Coat Factory Sec. Lit., 114 F.3d 1410, 1431 (1997).
[19] *See also* 17 C.F.R. 229.512 (2016).

laws to keep the public and investors informed about the nature of a security breach."[20]

The Yahoo breach may become a catalyst to expand the scope of the disclosure requirements for hacks because of the notoriety of the hack.[21] Although the SEC has never initiated a data breach disclosure lawsuit, the Commission has "been looking for the right case to bring forward," according to Jacob Olcott, former Senate Commerce Committee counsel.[22] However, Congressional resolve to intervene appears to be lacking, as evidenced by the fact that the Personal Data Notification and Protection Act of 2015, which would have required disclosure of hacks within 30 days, did not pass.[23] Thus, Yahoo's hack may cause an expansion in the disclosure rules through the SEC's rulemaking authority or through the courts.

---

[20] *Sen. Warner Calls on SEC to Investigate Disclosure of Yahoo Breach*, MARK R. WARNER (Sept. 26, 2016), http://www.warner.senate.gov/public/index.cfm/2016/9/sen-warner-calls-on-sec-to-investigate-disclosure-of-yahoo-breach.

[21] *See* Dustin Volz, *Yahoo Hack May Become Test Case for SEC Data Breach Disclosure Rules*, REUTERS: TECH. NEWS (Sept. 30, 2016), http://www.reuters.com/article/us-yahoo-cyber-disclosure-idUSKCN1202MG.

[22] *Id.*

[23] H.R. 1704, 114th Cong. (2015-2016).