Published on *The National Law Review* https://natlawreview.com

When are Public Companies Required to Disclose that They Have Experienced a Material Data Security Breach?

Article By:

Keir D. Gumbs

Recent discoveries of **data security breaches** have raised a perennial question for public companies: are public companies required by law or practice to provide material updates to their investors when bad things happen? The answer can be quite surprising.

Disclosure at the Time of the Event

As a threshold matter, federal securities law does not explicitly impose an affirmative duty on issuers to disclose data security breaches or failed attempts to breach a company's data security. There is no specific line item in any SEC disclosure document, rule or regulation that specifically requires such disclosures. In this regard, federal securities law does not require the disclosure of this, or other information, solely because it might be "material." Instead, the determination of whether material information is required to be disclosed depends on whether such information is required to be disclosed in the applicable form, or is necessary to make other statements made not misleading.

For example, Form 8-K, the form that is generally used to provide markets and investors with current information, is only required to be filed when one of the specific items included in the form are triggered. These include things such as entry or termination of material contracts, the acquisition or disposition of a material business or a material amount of assets, the appointment or termination of executive officers or directors and similar occurrences. Any events that do not involve one of the enumerated triggers may be filed under Item 8.01 as an "Other Event" or under Item 7.01 as "Regulation FD Disclosure," which is intended to allow companies to comply with Regulation FD, which generally requires that companies publicly disclose information that they intend to disclose privately to investors or others. Form 8-K does not include a specific line item relating to data security breaches or similar events - even if such events are material.

This is not to say that companies have a complete pass when they experience a data security breach. For example, if a company has publicly made a statement about its information technology systems or some other aspect of its business that is implicated by a data security breach and that was inaccurate or misleading at the time the statement was made, the company has an obligation to correct that statement. This is true whether the company knew that the statement was inaccurate at the time the statement was made, or the company learned about the inaccuracy at a later date. This is also true regardless of whether the statement was made directly to investors or to a company's

customers. If the information is made to the public, and an investor reasonably relies on such information, the company may find itself vulnerable to a securities claim based on the statement. Similarly, a company that is offering to sell or purchase its securities at a time that it discovers a breach of its data security will have to consider whether the breach needs to be disclosed to the persons to whom it is selling securities or the shareholders from whom it is buying securities. If material, the failure to provide investors with this information could create liability for the company under federal and state securities laws.

By contrast, if a company has publicly made a forward-looking statement that the company believed to be true, and was not untrue or misleading, at the time the statement was made, but the statement subsequently becomes inaccurate or misleading as a result of changes in circumstances, then the company does not have an obligation to update that prior statement (although it may choose to do so). *See, e.g.*, *Gallagher v. Abbott Labs.*, 269 F.3d 806, 810 (7th Cir. 2001) (Easterbrook, J.). However, some courts have (to the surprise of many securities lawyers) held to the contrary, and have imposed such a "duty to update" on companies. *See, e.g., In re Time Warner, Inc. Sec. Litig*., 9 F.3d 259 (2d Cir. 1993). Further discussion of the evolution – and subsequent limiting – of the duty to update doctrine may be found in Steven E. Bochner & Samir Bukhari, The Duty To Update and Disclosure Reform: The Impact of Regulation FD and Current Disclosure Initiatives, 7 STAN. J.L. BUS. & FIN. 225 (2002). Other courts have indicated that "definite positive projections" that become inaccurate as a result of intervening events must be updated, while "vague statements of optimism" need not require such updating. *Ill. State Bd. of Inv. v. Authentidate Holding Corp*., 369 Fed. Appx. 260, 263-64 (2d Cir. 2010). For instance, the Supreme Court recently ruled against a pharmaceutical company that had previously given concrete guidance indicating that the revenues from a particular drug were likely to rise by over 50% and that reports of the drug's link to a severe side effect were unfounded. In doing so the court noted that the company had some evidence of the link at the time of the disclosure and, when more information substantiating the link was later discovered, the company never corrected its previous guidance. *See Matrixx Initiatives, Inc. v. Siracusano*, 131 S. Ct. 1309 (2011).

Finally, if the company is listed on the NASDAQ or the NYSE, it may be required to provide notice of the event to the trading markets as appropriate. For example, companies listed on the NASDAQ Stock Market are required to disclose material news promptly to the public through any Regulation FD-compliant method or combination of methods. For these purposes, material news is defined as information that would "reasonably be expected to affect the value of a company's securities or influence investors' decisions." Based on these requirements, a company that experiences a material data security breach may have an obligation to notify the markets of this development if it concludes that investors would believe the information to be material.

Based on all of these requirements, a company that experiences a material data security breach may find itself in a conundrum. It may reasonably conclude at the first discovery of the breach that no press release Form 8-K is required, but that calculus can change as it discovers more information about the scope of the breach that may make it material to investors. Further, it may choose to make an initial disclosure, only to find out that the impact of the breach may be more or less significant than it originally thought, raising questions about whether it now has a duty to update its original statement. In fact, it would not be uncommon for a plaintiff to find fault with a company's original description of a major event that later proves to be incomplete. While this does not mean that a company should refrain from making an initial disclosure, it does mean that companies that choose to disclose a breach at the outset should make sure that any forward-looking statements about the breach have a reasonable basis and are identified as forward-looking statements.

Disclosure in the Next Periodic Report

Setting aside the initial disclosures, a company will have a similar, but easier question when it comes time for it to prepare its next quarterly or annual report. As a general matter, a company that has experienced a data security breach must evaluate its disclosures in its next quarterly or annual report to determine whether disclosure of the breach or costs related to the breach should be disclosed.

As discussed in greater detail in our advisory regarding cyber security disclosures, there are several disclosure items in a quarterly or annual report that may be implicated by a data security breach, including the risk factor disclosures, the management's discussion and analysis of financial condition and results of operation, legal proceedings disclosures, the description of business and potentially the notes to the financial statements. For a more fulsome discussion of when a cybersecurity breach should be disclosed in a company's quarterly or annual reports.

National Law Review, Volume IV, Number 134