MINTZ

To 8-K, or not to 8-K? For Target, that is indeed the question.

January 17, 2014 | Blog | By **Cynthia J. Larose**, Adam Veness

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

Written by Adam Veness and Cynthia Larose

As anyone with a pulse and a computer, television or carrier pigeon knows, Target Corporation (NYSE: TGT) suffered a major data breach in December – the extent of which **is still being uncovered** – and pegs the latest number of customers that have had their personal information stolen anywhere from **70 to 110 million**. As a public company, a breach of this magnitude should be material enough to warrant a Form 8-K filing, right? As of this post, Target doesn't seem to think so.

Form 8-K contains mandatory disclosure requirements when certain enumerated events occur, as in the entry into a material definitive agreement (Item 1.01) or the resignation of a director (Item 5.02). Reporting an event such as the Target data breach would likely fall under Item 8.01 of Form 8-K, which is used to report "Other Events." Item 8.01 permits the registrant, at its option, to disclose any events not otherwise called for by another Form 8-K Item that the registrant "deems of importance to security holders," and is an entirely *voluntary* filing.

Although filing under Item 8.01 of Form 8-K is voluntary, other companies that have suffered smaller data breaches have opted to file an 8-K to disclose such breaches, including The TJX Companies, Inc.'s (NYSE: TJX) **breach disclosed in an 8-K in January, 2007**, and Morningstar, Inc.'s (NASDAQ: MORN) **more recent breach disclosed in an 8-K in July, 2013**. Target's securities lawyers may believe that the breach is not "important to security holders," or is not sufficiently ***material*** enough to the roughly $38 billion company to warrant the filing of an 8-K, but 70 to 110 million affected customers is hardly immaterial, even for Target. In a statement released January 10, Target warned that the costs related to the breach "may have a material adverse effect on Target's results of operations in fourth quarter 2013 and/or future periods."

Indeed, Target evidently determined when filing its **Form 10-K** for 2012 that the *risk* of a data security breach was material enough to warrant disclosure in its risk factors:

"**If our efforts to protect the security of personal information about our guests and team members are unsuccessful, we could be subject to costly government enforcement actions and private litigation and our reputation could suffer.**

The nature of our business involves the receipt and storage of personal information about our guests and team members. We have a program in place to detect and respond to data security incidents. To date, all incidents we have experienced have been insignificant. If we experience a significant data security breach or fail to detect and appropriately respond to a significant data security breach, we could be exposed to government enforcement actions and private litigation. In addition, our guests could lose confidence in our ability to protect their personal information, which could cause them to discontinue usage of REDcards, decline to use our pharmacy services, or stop shopping with us altogether. The loss of confidence from a significant data security breach involving team members could hurt our reputation, cause team member recruiting and retention challenges, increase our labor costs and affect how we operate our business." (emphasis added)

Of course, there is no time limit for filing under Item 8.01 of Form 8-K due to it being a voluntary filing, so a filing may still be forthcoming from Target. In any event, one can only imagine that the risk factor language above will look very different in Target's next Form 10-K filing in two months.

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.

Adam Veness