January 16, 2014

Cybersecurity Update: Are Data Breach Disclosure Requirements on Target?

As discussed in Akin Gump's annual "Top Ten Topics for Directors in 2014," cybersecurity and data privacy are indeed among the hottest topics in the boardroom this year due to the dramatic rise in cyber attacks and data breaches. As part of a board's risk management oversight function, directors should assess the adequacy of their company's data security measures. Among other things, boards should have a clear understanding of the company's cybersecurity risk profile and who has primary responsibility for cybersecurity risk oversight and should ensure the adequacy of the company's cyber risk management practices, as well as the company's insurance coverage for losses associated with data breaches.

This week, Akin Gump delves further into cybersecurity risk factor disclosures as public companies head into annual reporting season, and takes a look at the renewed congressional interest in federal data security and breach notification legislation.

Recent Data Breaches

On December 19, 2013, Target issued a press release disclosing that approximately 40 million credit and debit card account numbers had been hacked from its system, a number that has since risen to potentially as many as 70 million accounts. The breach is currently being investigated by the U.S. Secret Service Electronic Crimes Task Force (ECTF). On New Year's Eve, an anonymous group or person hacked into Snapchat's servers and publicly released the usernames and phone numbers of more than 4.6 million Snapchat users. Additionally, on January 11, 2014, retailer Neiman Marcus confirmed that hackers had breached its servers and accessed customer payment information. The ECTF is also investigating the Neiman Marcus data breach, the extent of which is not yet known. The Senate Judiciary Committee announced yesterday that it has scheduled its hearing on data breaches for February 4, 2014.

Risk Disclosure Reminder

As calendar-year public companies approach annual reporting season, issuers should consider whether or not their current risk factor disclosures, as well as their "forward-looking statements" language, are adequate in light of these high-profile cybersecurity incidents. While there are currently no comprehensive federal laws explicitly mandating disclosure in connection with data security breaches, the emerging and existing business risks have not gone unnoticed by the Securities and Exchange Commission (SEC) or the Financial Industry Regulatory Authority (FINRA). In 2011 the SEC advised companies to approach cybersecurity as they would any other part of the business: if cybersecurity is a significant factor that makes an investment in the company speculative or risky, then issuers should address it in their risk factor disclosures. Similarly, if a past incident or current risk of cybersecurity is likely to have a material effect on operations or financial statements, then such incident or risk should be included in their Management's Discussion and Analysis of Financial Condition and Results of Operations. FINRA has

reiterated to broker-dealers that cybersecurity will remain a regulatory priority with a primary focus of firm policies, procedures and controls.

The recent incidents show just how relevant cybersecurity risks are to companies in the retail space. Target had previously disclosed data security risks in its 2012 annual report. In its discussion of risk factors, Target said that "[t]he nature of our business involves the receipt and storage of personal information about our guests . . . If we experience a significant data security breach or fail to detect and appropriately respond to a significant data breach, we could be exposed to government enforcement actions and private litigation." Furthermore, Target disclosed that malicious attacks and security breaches could cause them to incur substantial costs and they could encounter a loss of guest confidence, which could adversely affect their results of operations.

Target is apparently trying to mitigate these post-incident risks and potential damage to its reputation with consumers by staying out in front of the problem: publicly announcing the data breach, establishing a dedicated webpage for resources related to the breach, and offering free credit monitoring and identity theft protection to all Target customers. Earlier this week, Target's CEO Gregg Steinhafel posted an open letter on Target's official blog offering an apology to customers and setting forth a numbered list of remedial steps the company is taking post-breach. Target is also using social media to interact with its affected customers; the company's official Facebook and Twitter feeds have focused almost exclusively on the data breach since it was first publicly announced. Whether or not Target's risk factor disclosure is sufficient to ameliorate government action and private lawsuits and whether or not Target's handling of the breach can preserve its brand and reputation as well as manage the potentially substantial costs associated with the incident remain to be seen.

While not as robust as Target's risk factor disclosure, Neiman Marcus' identified cyber attacks and breach of information security as significant risks to the company's operations. Neiman Marcus has apologized to its customers via Twitter, but so far provided few details of the attack as they continue to investigate.

In light of these recent high-profile cyber attacks, companies may want to take a fresh look at the SEC's 2011 Disclosure Guidance to determine if their current risk factor disclosures should be supplemented to identify risks as technology evolves and more incidents occur. Companies should also review their standard "forward-looking statements" language to determine whether it needs refreshing. Target has already revised their forward-looking statements language to address the potential impacts of the data breach as factors which could cause its actual results to differ materially, including: "(i) loss of guest confidence in the Company's ability to protect their information because of the data breach, and the adverse impact such loss of confidence may have on sales, (ii) the outcome of our pending and ongoing investigation, including our discovery of additional information relating to the data breach and our guests' and other stakeholders' reactions to that additional information, and (iii) costs related to our investigation and resulting liabilities."

In doing so, companies should consider whether or not cyber attacks post a unique and material risk to their operations and should discuss these risks in a way that avoids boilerplate language and statements

of general risk applicable to all users of information technology. Although the disclosure should be tailored and company-specific and should provide enough information to allow investors to "appreciate the nature of the risks," companies need not provide potential cyber attackers with a "road map" of their security flaws or vulnerabilities, according to the SEC. And as Target's reaction to its data breach illustrates, disclosures may continue after a cyber incident as the company continues to investigate and update affected parties and investors.

Renewed Congressional Interest in Legislation

Meanwhile in Washington, legislators are renewing the call for new federal laws that would strengthen data security and notification requirements. Citing the Target data breach, last week Senate Judiciary Committee Chairman Patrick Leahy (D-VT) introduced the Personal Data Privacy and Security Act (S. 1897). The bill would create a national standard for data breach notification, require that companies engaging in interstate commerce keep consumer data they collect secure from outside intrusion or public release and allow the assessment of potential criminal and civil penalties. Additionally, Sen. Edward J. Markey (D-MA), a member of the Senate Commerce Committee, released a statement saying that the Target breach illustrates the need for stronger data security standards.

Sen. Tom Carper (D-DE) also announced that he plans to reintroduce similar legislation that would create a national reporting standard for data breaches that would apply to both retailers and financial institutions. Sen. Pat Toomey (R-PA) has had a similar bill, the Data Security and Breach Notification Act of 2013 (S. 1193), pending before the Senate Commerce Committee since June 2013. That bill would grant the Federal Trade Commission (FTC) new authority to establish and enforce regulations requiring companies to protect consumer data and notify consumers in the event of a breach.

Additionally, some lawmakers are calling on the FTC to investigate. In a letter to the FTC on December 22, 2013, regarding the recent Target breach, Sen. Richard Blumenthal (D-CT) wrote that "it appears Target may have failed to employ reasonable and appropriate security measures to protect personal information." Further, state attorneys general across the country said they will examine whether Target provided enough protection for its customers.

While the introduction of new legislation amid the Target and Snapchat breaches increases the likelihood that data breach notification requirements will gain some traction on Capitol Hill this year, it remains to be seen whether broader, more comprehensive action on consumer privacy rights and data security will occur. A broader privacy bill pitched by the Obama Administration, known as the "Consumer Privacy Bill of Rights," is also unlikely to see significant legislative action. That proposal would focus on giving consumers individual control of how their data is collected and used while requiring companies that collect consumer data to be more transparent about their use and protection of the data. The proposal would rely on a combination of increased FTC enforcement authority, along with new legislation to accomplish those goals.

So far, Congress's focus in this area in 2014 is centered on data protection and breach notification, as opposed to other topics, such as consumer privacy rights. Indeed, the House passed a bill on January 10,

2014, that focuses on data security rules for Healthcare.gov, the federal government website where the public can sign up for health insurance coverage under the Affordable Care Act. The bill, sponsored by Rep. Joe Pitts (R-PA), would require the Obama Administration to notify federal and state exchange users within two days if their personal data has been breached. While the bill was supported by 67 House Democrats, it is being seen more as a political measure than a policy shift toward support for a uniform federal breach notification standard for private companies. The bill is not expected to be taken up in the Senate.

Whether Congress will or should act on consumer data protection and breach notification remains open for debate. Given the current patchwork of state regulations concerning breach notification, some companies may welcome a single, reasonable federal standard. Some stakeholders argue, however, that such federal standards are unnecessary given companies' self-interest in protecting their customers' personal information. Indeed, in response to the December breach, Target has offered all of its customers free credit monitoring and identity theft protection for one year. While some federal legislation may call for such a remedy, Target is not currently required to do so by federal law.

As the Snapchat breach has shown, data protection and breach notification issues are not isolated to retailers and financial institutions that handle sensitive consumer and financial data, but also social media companies that harvest troves of personal data.

According to a statement by the Snapchat hacker(s), the breach was made in order to raise public awareness about Snapchat's inadequate privacy protections and force the company to fix the security flaws the hacker(s) exploited. Snapchat has apologized to its users and promised to remedy the security flaws that allowed the breach. Snapchat, whose focus is the sharing of photographs between mobile devices which are then automatically deleted after a user-specified amount of time, faced earlier scrutiny in May 2013, when the Electronic Privacy Information Center (EPIC) filed a complaint with the FTC, alleging that Snapchat misled its customers when it claimed their photos would "disappear forever." In practice, EPIC argued, the photos remain stored on users' phones and could potentially be accessed by someone with specialized knowledge.

While there will always be the threat of malicious actors seeking to obtain and manipulate personal, private data collected by companies for legitimate business purposes, it will ultimately remain in the self-interest of companies to try and stay as far ahead of the hackers as possible, whether or not federal lawmakers ultimately enact comprehensive data protection laws or some form of breach notification requirements. As the old adage goes, "an ounce of prevention is worth a pound of cure." Congress may decide to legislate greater preventative measures, and if it does, should do so in a way that gives companies the flexibility needed to respond to new threats.

Contact Information

If you have any questions regarding this alert, please contact:

Shar Ahmed
sahmed@akingump.com
713.220.8126
Houston

Carlos M. Bermudez
cbermudez@akingump.com
310.728.3320
Los Angeles – Century City

Garrett A. DeVries
gdevries@akingump.com
214.969.2891
Dallas

Alice Hsu
ahsu@akingump.com
212.872.1053
New York

Karol A. Kepchar
kkepchar@akingump.com
202.887.4104
Washington, D.C.

Paul Lin
pclin@akingump.com
949.885.4260
Irvine

Rosa A. Testani
rtestani@akingump.com
212.872.8115
New York

Lucas F. Torres
ltorres@akingump.com
212.872.1016
New York

Samuel Wolff
swolff@akingump.com
202.887.4462
Washington, D.C.

Tracy Crum
tcrum@akingump.com
214.969.2808
Dallas

Francine E. Friedman
ffriedman@akingump.com
202.887.4143
Washington, D.C.

Jo-Ellyn Sakowitz Klein
jsklein@akingump.com
202.887.4220
Washington, D.C.