Akin®

Renewed Congressional Interest in Federal Data Security and Breach Notification Legislation

Jan 13, 2014

Reading Time : **4 min**

By: Francine E. Friedman, Matthew C. Thomas (Senior Public Policy Specialist)

Citing the Target data breach, 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 using its current authority. In a letter to the FTC on December 22, 2013, regarding the recent Target breach, Senator Richard Blumenthal (D-CT) wrote that "it appears Target may have failed to employ reasonable and appropriate security measures to protect personal information."

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 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, just this week, it was reported that Target will offer customers free credit monitoring and identity theft protection in response to the December breach. While some federal legislation may call for such a remedy, Target is not currently required by law to do so.

As the Snapchat breach has shown, data protection and breach notification are not problems for just retailers and financial institutions that handle sensitive consumer and financial data, but also social media companies that harvest troves of personal private data. Data privacy in this realm can lead to complicated legal quandaries.

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 premise 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.

Categories

Capital Markets | Corporate Governance | Policy & Regulation

Cybersecurity, Privacy & Data Protection

London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.