The Evolving New Normal For Data Breach Responses

Law360, New York (April 18, 2014, 9:37 PM ET) -- The legal landscape is changing for how businesses prevent and respond to data breaches. The mass data breaches at the Target Corporation and Blue Cross Blue Shield of New Jersey ("Horizon") resulted in several state legislatures introducing bills that seek to impose greater obligations and penalties on businesses for their failure to adhere to stricter compliance programs. In addition, consumers have lodged a flurry of class actions against businesses for failing to adequately protect personal information and for failing to notify them of a data breach.

The new normal requires businesses to be more vigilant in protecting a consumer's personal information and in responding to any data breach. This article evaluates the significance of the Target and Horizon data breaches, analyzes the consequences of pending class action litigation and related legislative responses, and outlines the relative implications of the emerging corporate governance and compliance paradigm shifts.

Target and Horizon: Breaches of Historic Portions

The watershed moment for data security arrived last year when Target, the second largest discount retailer in the United States, confirmed the "unauthorized access" to approximately "40 million credit and debit card accounts."[1] Target reported that it "alerted authorities and financial institutions immediately" after it was made aware of the breach.[2] It also announced that it was partnering with "a leading third-party forensics firm" to investigate the incident and "examine additional measures" that the retailer can adopt to prevent a similar breach in the future.[3]

Target would later report that it "proactively reached out" to state attorney generals to apprise them of developments of their internal investigation. The company also confirmed that it was "actively partnering" with the United States Secret Service and the U.S. Department of Justice on its investigation into the breach that affected its point-of-sale system.[4]

Earlier this year, Target confirmed that its forensic investigation "determined that certain guest information — separate from the payment card data previously disclosed — was taken during the data breach."[5] Target stated that "the investigation has determined that the stolen information includes names, mailing addresses, phone numbers or email addresses for up to 70 million individuals."[6] The company reiterated that aside from its customers being guaranteed "zero liability" for costs arising from the breach it would also be offering one year of free credit monitoring and identify theft protection to all guests who shopped at its U.S. stores.[7]

Late last year, Horizon also reported a data breach effecting a significant number of policyholders. Horizon reported the theft of two unencrypted laptop computers from its corporate headquarters in Newark, N.J. Horizon reported the theft to local police approximately three days after learning about the incident.[8] About a month later, it issued a press release revealing that "a detailed review led by outside computer foreign

experts ... confirmed that the laptops may have contained files with differing amounts of member information (e.g., address, member identification number, date of birth), and in some instances, a Social Security number and/or limited clinical information."[9]

Horizon notified over 800,000 members of the breach and reported that those members whose Social Security numbers are believed to have been potentially compromised would be offered "free credit monitoring and identity theft protection."[10]

Horizon further stated that it would "continue[] to work with law enforcement to locate the laptops."[11] However, in an effort to prevent a similar event from happening again, the company would be "strengthening encryption processes and enhancing its policies, procedures and staff education regarding the security of company property and member information."[12]

The Target and Horizon data breaches differed in manner, size, and scope but are nevertheless similar in significance. Both reveal the real vulnerabilities companies of all sizes, across all industries, are facing. The consequences to both consumers and proprietors requires a nuanced, more responsive, and more uniform legal and regulatory framework.

That environment is being shaped by private actions, legislative and administrative responses, and various corporate initiatives. In this century of unprecedented global commerce and cyber susceptibilities, businesses must remain vigilant and ahead of the curve in adopting compliance protocols that are consistent with existing laws and developing trends.

Pending Data Breach Litigation

In the wake of widely reported data breaches, private actions across the country have been commenced seeking redress from companies for their alleged failure to adequately safeguard consumer financial information and related data.

On Dec. 27, 2013, Target became a party to such a suit filed in New Jersey federal court.[13] Two New Jersey residents brought a putative class action against the company over the data breach they had earlier confirmed. The putative class plaintiffs allege breach of fiduciary duty, negligence, negligence per se, breach of contract, and bailment.[14] The complaint alleges that Target breached its fiduciary duty to the plaintiffs and class members by "improperly storing, monitoring and/or safeguarding" sensitive personal information.[15]

In support of their negligence claim, plaintiffs charge that Target has a "duty to use reasonable means to destroy in a time manner, and not unnecessarily store, such information."[16] Moreover, plaintiffs contend that Target has a "duty to safeguard" consumers' personal information to keep it private and secure by complying with applicable standards, statutes, and regulations.[17]

Additionally, plaintiffs maintain that Target also had a duty to timely inform its customers of the breach and the fact that their personal information was comprised. The putative plaintiffs also allege that Target has a duty to protect and keep sensitive personal information from its customers private and confidential pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801.[18] The alleged deviation purportedly amounted to negligence per se.

Earlier this year, Target identified at least 75 additional actions asserting substantially the same allegations against it in courts across the country. For that reason, numerous petitions were submitted to the Judicial Panel on Multidistrict Litigation to consolidate these cases into a single multidistrict litigation.[19] The United States District Court for the District of New Jersey granted a stay pending a decision by the JPML regarding the MDL.[20] On March 27, 2014, Target urged the JPML panel to transfer the cases to Minnesota federal court, where the company is headquartered. A decision on the MDL is still pending.

Regardless if these suits against Target are consolidated into a single MDL, its disposition will have a real impact on businesses of all sizes across a variety of industries. This may prove to be the catalyst for new regulations that will usher in a new era of corporate governance and compliance. An enhanced fiduciary duty is likely to emerge that alters what has traditionally been deemed foreseeable. In this age of interconnectedness, corporate vulnerabilities can be exposed remotely. The consequence will be a heightened duty of care from businesses to its clients and customers regardless of the final disposition of pending suits.

Legislative Response

Business' prevention and response to data breaches is not just at issue in courts across the country, it is also the focus of bills before the United States Congress and several state legislatures. Presently, there is no overarching federal legislation that specifically regulates privacy and data security. Instead, these issues are regulated by industry and demographic specific federal laws, state laws and regulations, and the Federal Trade Commission and other agency regulations and enforcement actions.

Currently, 46 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have adopted laws requiring private and governmental entities to notify individuals of security breaches of personal information. These laws generally provide who must comply with the law, define personal information and what constitutes a breach, outlines requirements for notice of a breach, and sets forth various exemptions (e.g., for encrypted information).

In response to the recent high-profile and significant data compromises, at least 19 states have legislation pending that would either amend existing security breach laws or establish a legal framework to address the issue in their jurisdiction. New Jersey is one of the states that currently has four measures pending in the Assembly and Senate that would amend existing laws.

New Jersey's data breach notification law, N.J.S.A. 56:8-161 et seq., was first enacted in 2005 and is exemplary of some of the country's most consistent notification requirements. The statute requires companies doing business in New Jersey to disclose a data breach that affects New Jersey customers.[21] The statute requires businesses to immediately notify the Division of State Police, in the Department of Law and Public Safety, when the company learns that personal information "was or is reasonably believed to have been ... accessed by an unauthorized person."[22] A breach, however, does not occur if the personal information accessed is encrypted or if the information does not constitute "personal information" as defined by the statute.[23]

As soon as disclosure of the breach is made to law enforcement, customers must be notified "in the most expedient time possible and without unreasonable delay."[24] Notification must be made through written notice, electronic notice, or by substitute notice if the costs of providing said notice exceeds $250,000.[25] However, if the compromised company has a notification procedure in place, then the company satisfies its statutory requirement by following its own notification procedures.[26]

The four bills before the New Jersey Legislature, if enacted, would prohibit retailers from storing certain magnetic-strip data and would require reimbursement for costs incurred by financial institutions due to any related breach of security.[27] The legislation would also revise penalties imposed on businesses for failure to report data breaches.[28] This measure states that would subject companies to a defined civil penalties for each breach of computerized records that the business discovers but fails to disclose in the manner provided under the law.[29] Notably, violations can also result in the assessment of punitive damages under the state Consumer Fraud Act.

The most critical development, however, would come from a pending bill that would no longer allow businesses and public entities to provide notification through substitute notice.[30] If this measure becomes law, companies will need to provide notice that contains contact information, including a toll free telephone number, of a customer representative of the business or public entity who is available to give updates about the nature of the compromise and potential consequences of the breach.[31] The customer representative must also be able to explain how the company is addressing the breach, what steps the customer can take to safeguard the information compromised, and that the customer will have access to free credit reports.[32]

These measures, similar to the ones being debated in Congress and state houses across the country, will create a new compliance paradigm for companies of all sizes. Companies that fail to develop and implement internal governance and compliance protocols that allow them to quickly respond to breaches and notify those effected will face governmental enforcement actions and private suits that will certainly outweigh the costs of developing and implementing internal guidelines and procedures.

Compliance Implications

Companies afflicted by a data breach of any size must have a well-designed compliance program. Businesses should also have a breach response preparedness audit plan that reviews its protocols on a quarterly basis to identify areas in need of improvement. An effective data security compliance program today must incorporate lessons of the high-profiled compromises and statutory and regulatory developments across the country. Companies across industries must develop and incorporate rigid data security policies, monitor regularly the integrity of data security infrastructures, and develop a plan and a team to manage the fall out of an inevitable breach. They must also establish a reporting and notification system that recognizes the varied legal obligations across jurisdictions.

Businesses, however, should also revisit how they store personally identifiable information and assess whether all that information is indispensable to their business. At a minimum, companies must fully understand the scope of the personal information they retain, where it is kept, how long is it stored, and who can access it. Investing in such compliance programs are the best way to avoid class actions, government enforcement actions, and/or the penalties contemplated by the pending legislation in Congress and in various state legislatures.

—By Mark Salah Morgan and Andres Acebo, Day Pitney LLP

Mark Salah Morgan is a partner and Andres Acebo is an associate in Day Pitney's Parsippany, N.J., office.

[1] Press Release, Target Corporation, Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores (Dec. 19, 2013) available at http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores (last visited Apr. 2, 2014).

[2] Id.

[3] Press Release, Target Corporation, A message from CEO Gregg Steinhafel about Target's payment card issues (Dec. 20, 2013) available at http://corporate target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca (last visited Apr. 2, 2014).

[4] Press Release, Target Corporation, Target Data Security Media Update #2 (Dec. 23, 2013) available at http://pressroom.target.com/news/target-data-security-media-update-2 (last visited Apr. 2, 2014).

[5] Press Release, Target Corporation, Target Provides Update on Data Breach and

Financial Performance, (Jan. 10, 2014) available at http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance (last visited Apr. 2, 2014).

[6] Id.

[7] Id.

[8] Press Release, Horizon Blue Cross Blue Shield of New Jersey, Horizon Blue Cross Blue Shield of New Jersey Notifies Members, Offers Protection Following Office Theft (Dec. 6, 2013), available at http://www.horizonblue.com/about-us/news-overview/company-news/horizon-bcbsnj-notifies-members (last visited Apr. 2, 2014).

[9] Id.

[10] Id.

[11] Id.

[12] Id.

[13] Complaint, Santos, et al. v. Target Corp., et al., No. 2:13-cv-07866-SRC-CLW, (D. N.J. Dec. 27, 2013), ECF No. 1.

[14] Id. at 7-12.

[15] Id. at 8.

[16] Id. at 9.

[17] Id.

[18] Id. at 11.

[19]Stipulation and Order Staying Proceedings Pending MDL Consideration, Santos, et al. v. Target Corp., et al., No. 2:13-cv-07866-SRC-CLW, (D. N.J. Dec. 27, 2013), ECF No. 7 (citing In Re: Target Corp. Security Breach of Customers' Financial Data, MDL NO. 2522, ECF No. 90 (Jan. 30, 2014).

[20] Id.

[21] N.J.S.A. 56:8-163(a).

[22] Id.

[23] N.J.S.A. 56:8-161.

[24] N.J.S.A. 56:8-163(a).

[25] N.J.S.A. 56:8-163(d).

[26] N.J.S.A. 56:8-163(e). However, if the breach is deemed to likely effect more than 1,000 customers then the company must also provide notice to national customer reporting agencies pursuant to N.J.S.A. 56:8-163(f).

[27] N.J. Assembly No. 1239 (as introduced Jan. 16, 2014) and N.J. Senate No. 965 (as introduced Jan. 27, 2014)

[28] N.J. Assembly No. 1329 (as introduced Jan. 16, 2014).

[29] Id. ("The bill substitutes . . . current penalties by establishing defined monetary fines. Under the provisions of the bill, the fine for a first offense is $5,000, for a second offense, $10,000, and for a third offense or subsequent offense, $15,000.").

[30] N.J. Assembly No. 2480 (as introduced Feb. 10 2014).

[31] Id.

[32] Id.