KING & SPALDING

Client Alert

Privacy & Information Security Practice Group

February 3, 2014

Target and Neiman Marcus Face Government Probes and Litigation as a Result of Holiday-season Cyberattacks

The massive holiday hacking of consumer information belonging to Target and Neiman Marcus customers has the impacted retailers under a microscope. State Attorneys General across the country have banded together to launch a "national investigation" into the data breaches that, in the case of Target, impacted approximately 70 million customers.[1] The U.S. Secret Service and Department of Homeland Security are conducting their own investigations and have partnered with private-sector executives to identify the perpetrators, most recently believed to be teenage Russian cyberthieves.[2]

Within weeks of the Target data breach announcement, lawmakers on Capitol Hill introduced legislation designed to address the issue of data security to better protect Americans' personal information and ensure their privacy.[3] Legislation aimed at creating a national standard to protect consumer data is nothing new, but this time the legislation may gain traction.

On January 8, Senate Judiciary Chairman Patrick Leahy (D-VT) and four other Senate Democrats introduced the Personal Data Privacy and Security Act of 2014.[4] The legislation, which Senator Leahy has introduced in every Congress since 2005, would create a national standard for data breach notification and require businesses to keep the consumer information they collect safe from hackers. It also would toughen criminal penalties for persons who conceal a damaging breach, require companies that keep data to establish adequate security policies, and strengthen penalties for attempted computer hacking. Senator Leahy stated that the recent data breach at Target is "a reminder that developing a comprehensive national strategy to protect data privacy and cybersecurity remains one of the most challenging and important issues facing our Nation."[5]

One week after Senator Leahy introduced his bill, Senate Homeland Security and Government Affairs Committee Chairman Senator Tom Carper (D-DE) and Senator Roy Blunt (R-MO) introduced an additional piece of legislation: the Data Security Act of 2014.[6] The bipartisan bill is intended to help protect consumers from identity theft and account fraud, and is meant to establish clear and consistent rules for public and private institutions to prevent and respond to data breaches. In particular, the Data Security Act would require entities, including financial institutions, retailers, and federal agencies, to better safeguard sensitive information, investigate security

For more information, contact:

Barry Goheen
+1 404 572 4618
bgoheen@kslaw.com

J.C. Boggs
+1 202 626 2383
jboggs@kslaw.com

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

Christopher C. Burris
+1 404 572 4708
cburris@kslaw.com

Alexander K. Haas
+1 202 626 5502
ahaas@kslaw.com

John A. Drennan
+1 202 626 9605
jdrennan@kslaw.com

Sarah E. Statz
+1 404 572 2813
sstatz@kslaw.com

Elizabeth K. Hinson
+1 404 572 2714
bhinson@kslaw.com

King & Spalding

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

www.kslaw.com

breaches, and notify consumers when there is a substantial risk of identity theft or account fraud. The proposed requirements would apply to all businesses that take credit or debit card information, data brokers that compile private information, and government agencies that possess nonpublic personal information.

This week, Neiman Marcus and Target officers will testify before the Senate Judiciary Committee and the House Subcommittee on Commerce Manufacturing and Trade at hearings to address the cyberattacks. On January 29, in a letter to Neiman Marcus CEO Karen Katz, Representatives Henry Waxman (D-CA) and Jan Schakowsky (D-IL) requested extensive documentation of any efforts by Neiman Marcus in recent years to protect customer information. Specifically, the House Committee sought any "written policies or guidelines relating to threat monitoring, network security or point-of-sale system protection," and all documents detailing the budget and employees that the retailer dedicated to network security since 2007. The Committee also asked for any documents concerning Neiman Marcus's response to the breach and efforts to notify the public, including any formalized breach readiness plan and any emails, reports or analyses from the past two years that Neiman Marcus officials have sent that relate to memory-parsing malware or point-of-sale system security.[7] The House Energy and Commerce Committee demanded that Target provide a similar cache of documents prior to its February hearing.[8]

Target and Neiman Marcus also face lawsuits, including class actions brought on behalf of credit card issuing banks and consumers. For example, in Alabama, card-issuing banks have filed a class action lawsuit claiming that the Target breach defrauded their customers and that Target had inadequate data security and monitoring measures to protect customer information.[9] In California, a consumer lodged a putative class action alleging that Target violated state unfair competition laws, data-breach laws, and various consumer protections acts.[10] The California lawsuit also alleges that Target ignored requirements of the PCI Data Security Standard and disregarded warnings from a data security expert that its Point-of-Sale computer systems, which store credit card and debit card information, were susceptible to a data breach.[11] Similarly, on January 13, Neiman Marcus also was hit with a putative class action, filed in the U.S. District Court for the Eastern District of New York. In that case, the plaintiffs allege that Neiman Marcus failed to exercise reasonable care in safeguarding its customers' privacy interests.[12]

Target and Neiman Marcus have been criticized in the media for failing to provide timely notice to consumers regarding the breach and for not being forthright about the number of consumers impacted by the breach. These criticisms highlight the challenges facing organizations in responding to data breach incidents. They also highlight the need to balance conducting a thorough investigation and cooperating with law enforcement investigations if criminal activity is involved, with the need to notify affected customers as soon as possible.[13]

Recommendations

Clients should implement comprehensive incident response plans to ensure that internal policies and procedures allow the company to respond quickly and efficiently to a data breach incident. Clients should also provide frequent training of employees so that all members of the organization are on the lookout for potential breaches and know what to do in the event of a potential breach. In addition, it is increasingly important for companies to frequently review their privacy and data security policies and to assess and update their security measures to ensure that they are protecting sensitive data. Security measures should be commensurate with the volume and sensitivity of the data being processed and stored. Strong passwords, network segmentation, firewalls, and encryption of sensitive personal information are key steps to ensuring your security measures are reasonable. It is also important to frequently test data security systems and processes to ensure the measures your organization has implemented perform as expected – something Neiman Marcus and Target are accused of failing to do.

King & Spalding's Privacy and Information Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Privacy & Information Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security

programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 30 Privacy & Information Security lawyers in offices across the United States, Europe and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy.

* * *

---

[1] Press Release, New York State Office of the Attorney General, Statement From A.G. Schneiderman On Target Security Breach (Jan. 10, 2014).
[2] Danny Yadron, *Target Hackers Wrote Partly in Russian, Displayed High Skill, Report Finds*, WALL STREET JOURNAL (Jan. 16, **2014), http://online.wsj.com/news/articles/SB10001424052702304419104579324902602426862**.
[3] For additional information regarding the proposed legislation, see **http://www.kslaw.com/library/newsletters/WashingtonInsight/2014/Jan21/article7.html**.
[4] S. 1897, 113th Cong. (2014).
[5] Senator Patrick Leahy, Chairman, Comm. on the Judiciary, On the Introduction of the Personal Data Privacy and Security Act of **2014 (Jan. 8, 2014), *available at* http://www.leahy.senate.gov/download/010814privbillstatementreintroduction**.
[6] S. 1927, 113th Cong. (2014).
[7] Letter from Reps. Waxman and Schakowsky, U.S. House of Representatives Subcommittee on Commerce, Manufacturing and Trade, to Karen Katz, Chief Executive Officer of Neiman Marcus Group (Jan. 29, 2014), *available at* **http://democrats.energycommerce.house.gov/sites/default/files/documents/Katz-Neiman-Marcus-Data-Breach-2014-1-29.pdf**.
[8] Letter from Reps. Waxman, DeGette, Schakowsky, U.S. House of Representatives Committee on Energy and Commerce, to Gregg Steinhafel, Chairman, President and Chief Executive Officer of Target Corporation (Jan. 23, 2014), *available at* **http://democrats.energycommerce.house.gov/sites/default/files/documents/Steinhafel-Target-Data-Breach-2014-1-23.pdf**.
[9] *See Alabama State Employees Credit Union v. Target Corp.*, No. 2:13-cv-00952 (M.D. Ala. filed Dec. 30, 2013).
[10] *See Nancy L. Mancias et al v. Target Corporation*, No. 3:14-cv-00212 (N.D. Cal. filed Jan. 14, 2014).
[11] *Id*.
[12] *See Melissa Frank v. The Neiman Marcus Group, LLC*, No. 2:14-cv-00233 (E.D. N.Y. filed Jan. 13, 2014).
[13] A recent Ponemon Institute research report indicates that companies that quickly respond and notify consumers of breaches end up paying more for the breach than companies that take a more thoughtful approach after a thorough investigation. **http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf**.