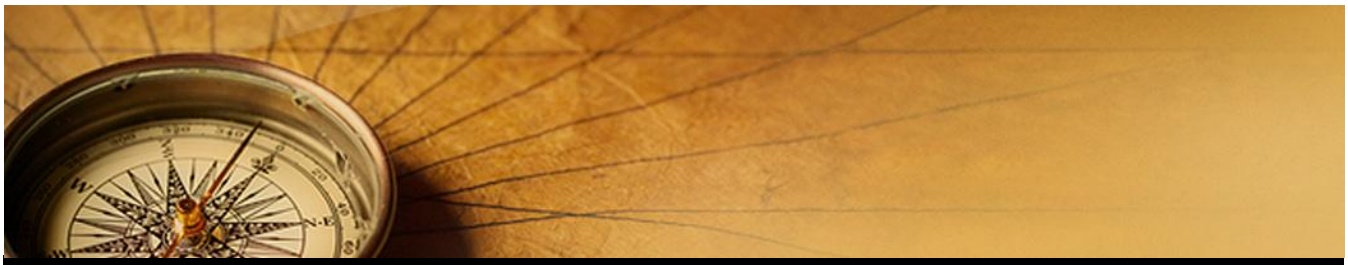

David Leiter, DJLeiter@mlstrategies.com
Jeremy Rabinovitz, JRabinovitz@mlstrategies.com
Bill Weld, BWeld@mlstrategies.com
Mo Cowan, MCowan@mlstrategies.com
Alex Hecht, ANHecht@mlstrategies.com
Abby Matousek, AMatousek@mlstrategies.com
Rachel Sanford, RMSanford@mlstrategies.com

Follow us on Twitter: @MLStrategies

ML Strategies, LLC
701 Pennsylvania Avenue, N.W.
Washington, D.C. 20004 USA
202 434 7300
202 434 7400 fax
www.mlstrategies.com

Legislative Alert: High Profile Security Breaches Spur Congressional Action

Recently, several large retailers, including Target and Neiman Marcus, announced that hackers had compromised credit card and other personal consumer data. At Target, 40 million debt and credit cards were impacted and the personal information of as many as 70 million additional customers exposed. Similarly, as many as 1.1 million debit and credit cards may have had their data stolen in the Neiman Marcus breach. These large scale data breaches follow other exposures in recent months, including those at Snapchat and Skype. Although concerns over the exposure of consumer data and cybercrime have existed for some time, in the wake of these breaches, Congress may be poised to impose additional security and regulatory requirements around customer security and notifications.

Despite a growing appetite on Capitol Hill to address these issues, data security and cybercrime face potential congressional turf wars as there are multiple committees of jurisdiction. Already, lawmakers from seven committees are considering holding hearings on data breach, including: the Senate Banking, Housing and Urban Affairs Committee; the Senate Judiciary Committee; the Senate Commerce, Science and Transportation Committee; the Senate Homeland Security and Governmental Affairs Committee; the House Financial Services Committee; the House Oversight and Government Reform Committee; and the House Energy and Commerce Committee.

Senate Action
The Senate Judiciary Committee deals with the legal issues involved with privacy and technology, while the Senate Banking Committee plays an oversight role for banking entities and financial regulators. The Senate Judiciary Committee's hearing will take place on February 4th and will feature witnesses from Target, the Consumers Union, and regulatory agencies including the Federal Trade Commission (FTC). A similar set of witnesses is expected to testify before the Senate Banking Committee at a still-to-be-determined date after Senators Chuck Schumer (D-NY), Mark Warner (D-VA), and Bob Menendez (D-NJ) urged committee Chairman Tim Johnson (D-SD) to hold a hearing on the Target breach.

Meanwhile, Commerce Committee Chairman Jay Rockefeller (D-WV) also asserted that committee's jurisdiction over commercial data practices and data security in a letter he and Senator Claire McCaskill (D-MO), Chairman of the Subcommittee on Consumer Affairs, Insurance, and Automotive Safety, sent to Target CEO Gregg Steinhafel. The letter requested that Target brief committee staff on the "cause and impact" of the breach. In addition, this week Rockefeller plans to reintroduce legislation he and Senator Mark Pryor (D-AR), Chairman of

the Subcommittee on Communications, Technology, and the Internet, have worked on for several congresses that would require companies to alert those impacted by a data breach within 60 days and provide up to two years of credit monitoring for victims. Senator Rockefeller may become a champion of the issue as data security is at the confluence of several measures championed by Senator Rockefeller—such as cybersecurity, personal data security, and online privacy. He may seek to make this a legacy project before his retirement at the end of this congress.

In addition to the Rockefeller-Pryor bill, other legislative proposals have been introduced in the Senate following the Target and Neiman Marcus announcements. Earlier this month, Senator Patrick Leahy (D-VT), Chairman of the Senate Judiciary Committee, introduced the *Personal Date Privacy and Security Act of 2014* (S. 1897), which would provide the federal government with additional tools under the Computer Fraud and Abuse Act (CFAA) to prosecute significant cyberthreats. Senators Tom Carper (D-DE) and Roy Blunt (R-MO) have also introduced the *Data Security Act of 2014* (S. 1927), which would require retailers, financial institutions, and regulators to implement policies to protect customers security, investigate data breaches should they occur, and inform consumers of any potential risk of identity theft or other fraud. Senator Carper, Chairman of the Homeland Security and Governmental Affairs Committee, will likely convene a hearing on cybersecurity and data security, focusing on both federal and private sector data breaches. Finally, Senator Pat Toomey (R-PA), a member of the Senate Banking Committee, introduced the *Data Security and Breach Notification Act of 2013* (S. 1193), which would require commercial entities to secure personal electronic data and to notify consumer of potential breaches.

House Action

On the House side, Target has committed to testify at a House Energy and Commerce Subcommittee on Manufacturing and Trade hearing on February 5th. Democratic leaders of the full committee requested more details about the Target breach in a letter to the CEO. The letter—signed by Ranking Member Henry Waxman (D-CA), Oversight and Investigations Subcommittee Ranking Member Diana DeGette (D-CO), and Commerce, Manufacturing, and Trade Subcommittee Ranking Member Jan Schakowsky (D-IL)—notes that "questions remain about how exactly this attack was carried out, who was responsible, whether it could have been prevented, how Target responded and how retailers and customers can protect themselves going forward." House Financial Services Committee Chairman Jeb Hensarling (R-TX) has also said his committee will examine the data breach issue in the context of the security of information collected by both financial institutions and government agencies. House Oversight and Government Reform Committee Ranking Member Elijah Cummings (D-MD) has also called on committee Chairman Darrell Issa (R-CA) to investigate Target's security measures with the same scrutiny it has given security concerns with HealthCare.gov.

Retailers vs. Banks

The Target and other recent high profile breaches have highlighted a divide between banks, credit and debit card issuers, and large retailers that are typically the objects of cybercrime. For example, banking institutions are responsible for supplying consumers impacted by data breaches with new cards, generally at a cost of $10 apiece. This can be a costly venture for banks. For example, JPMorgan Chase has supplied about two million reissued cards as a result of the Target breach.

While in the past banks have sued to recoup the costs of reissuing cards, the question of who should bear the cost of data breaches will likely continue to be controversial as Congress begins to debate the security of financial information. Although banking institutions have argued that the retailer impacted by the breach should cover the downstream costs of poor data security, retailers have charged that banks are ultimately responsible for their financial products and should improve technology within the cards themselves to protect them from bad actors.

Outlook

Although the second session of the 113th Congress is expected to be busy over the next few months with the debt limit, farm bill, Sustainable Growth Rate (SGR), and other issues, there is a reasonable expectation, given the recent high profile breaches, that Congress will focus on this matter in coming months.