MEMORANDUM

TO: ESPC

FROM: Reed Freeman

Patrick Bernhardt

DATE: February 6, 2014

RE: Congressional Hearings Regarding Potential Federal Data Security Legislation

---

We write to summarize hearings this week in House and Senate Judiciary, Commerce, and Banking committees regarding data security in light of recent high-profile data breach incidents. The various committees heard testimony from representatives of the U.S. Department of Justice ("DOJ"), Federal Trade Commission ("FTC"), state attorneys general, cybersecurity firms, as well as from representatives of the retail and banking industries.

Here is the Bottom Line, from Our Perspective:

- There appears to be more support now than ever for a federal data breach notification law. Whether such a bill can actually pass this term; whether it would preempt the existing state data breach notification laws; what the notification triggers, timelines, and substance would be; and whether they would be enforceable by a private right of action, are not at all clear, though, at this stage.

- On the other hand, there does not seem to be strong bipartisan support for a substantive national data security standard that would require companies to adopt specific safeguards, enforceable by the FTC and state attorneys general, or even by private rights of action. (That said, some members of Congress were receptive to FTC Chairwoman Ramirez's repeated requests for new FTC authority to promulgate a trade regulation rule on data security, enforceable by the FTC, with the new tool of civil penalties). There seems to be broader support for the government to continue to work with industry on a voluntary, flexible substantive set of standards.

Senate Banking Committee – Subcommittee on National Security and International Trade and Finance – "*Safeguarding Consumers' Financial Data*"

Senator Mark Warner (D-VA), chairman of the subcommittee, opened the first hearing with a statement that "we don't need another long-term fight between the bankers, retailers, and card industry," but that government, industry and consumers all have a role to play to increase technological safeguards and protect consumer information.

Jessica Rich, Director of the Bureau of Consumer Protection at the Federal Trade Commission, noted the Commission's "bipartisan support for Congress to enact data security legislation that would (1) strengthen its existing authority governing data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to consumer where there is a security breach." She explained the FTC's current enforcement efforts under Section 5 of the Federal Trade Commission Act and its cooperation with state and federal agencies.

Senator Elizabeth Warren (D-MA) expressed her support for increased FTC enforcement authority and noted that the FTC's current limited authority was a "real problem."

Senate Judiciary Committee - *"Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime"*

Senator Patrick Leahy (D-VT), chair of the committee, opened the second hearing by noting that "[p]ublic confidence is crucial to our economy." He expressed support for his recently introduced legislation entitled the Personal Data Privacy and Security Act.

Senator Chuck Grassley (R-IA), ranking member of the committee, stated that he hoped to explore common ground in crafting a breach notification standard and emphasized that "our approach should provide flexibility and also account for businesses of different sizes and different resources." He expressed the need to avoid "over-notification" to consumers and supported a partnership between government and business in crafting a framework along the lines of the National Institute of Standards and Technology ("NIST") cybersecurity framework.

John Mulligan, Executive Vice President and Chief Financial Officer at Target Corporation, and ***Michael Kingston***, Senior Vice President and Chief Information Officer at The Neiman Marcus Group, testified regarding the sophisticated nature of the recent attacks and the need for government, law enforcement and businesses to share information about cybersecurity threats.

Edith Ramirez, Chairwoman of the Federal Trade Commission, urged Congress to (1) require companies to provide notification to consumers, in appropriate circumstances, when there is a security breach; (2) grant the FTC rulemaking authority under the Administrative Procedure Act; and (3) grant the FTC authority to seek civil penalties to help deter unlawful conduct. She noted that "the mere fact that a breach occurred does not mean that a company has violated the law."

Mythili Raman, Acting Assistant Attorney General, Criminal Division of the U.S. Department of Justice, highlighted the administration's 2011 data security proposal and expressed support for the "establishment of a strong, uniform Federal standard requiring certain types of businesses to report data breaches and thefts of electronic personally identifiable information."

In questions, ***Senators Chuck Grassley (R-IA)*** and ***Mike Lee (R-UT)*** expressed skepticism about whether a national data security standard would be flexible enough to accommodate

evolving security practices and malware, but generally agreed that breach notification legislation was necessary to provide incentives for businesses to increase security. Witnesses stated that in providing notification to consumers, businesses must balance speed, accuracy, and the ability to provide actionable information to consumers.

Senators Dianne Feinstein (D-CA), ***Amy Klobuchar (D-MN)***, ***Al Franken (D-MN)***, ***Richard Blumenthal (D-CT)***, ***Dick Durbin (D-IL)*** and ***Sheldon Whitehouse (D-RI)*** expressed support for a national standard on data security practices, in addition to a data breach notification requirement.

Senator Richard Blumenthal (D-CT) strongly endorsed a national security standard enforced by both the FTC and private individuals, along with a clearinghouse to share and exchange information.

Senators Orrin Hatch (R-UT) and ***Amy Klobuchar (D-MN)*** expressed interest in chip-and-PIN payment card technology while suggesting that future payment platforms, such as smartphones, will need to adapt to new security standards.

House Energy and Commerce Committee, Subcommittee on Commerce, Manufacturing and Trade – *"Protecting Consumer Information: Can Data Breaches Be Prevented?"*

Representative Lee Terry (R-NE), chair of the subcommittee, opened the third hearing with a statement that he "[does] not believe that we can solve this whole problem by codifying detailed, technical standards or with overly cumbersome mandates," but he expressed support for "a uniform data breach notification standard."

Representative Henry Waxman (D-CA), ranking member of the full committee, noted the current patchwork of state breach notification laws and supported federal legislation that would create a national standard for data security practices.

FTC Chairwoman Edith Ramirez appeared again to testify that federal legislation was necessary to increase FTC authority and establish national breach notification and data security standards. Responding to questions, she indicated her support for a flexible standard that would focus on the *processes* that businesses implement to protect consumer information and respond to cybersecurity threats. She agreed that breach notification legislation should address both the content and the timeline for notification and believed that businesses should be required to provide free credit monitoring to consumers after a breach, with limited exceptions. Finally, she believed that the national data security standard should preempt state law but nevertheless be subject to enforcement by state attorneys general. She did not express an opinion regarding whether the new law should contain a private right of action.

Lisa Madigan, Attorney General of the State of Illinois, emphasized that data security laws are critical to protect financial security and the economy. She called for federal legislation that does not preempt state law, but also indicated that it was not necessary to create a private right of action to enforce such a standard.