THE COMMITTEE ON ENERGY AND COMMERCE

MEMORANDUM

July 16, 2013

To: Members of the Subcommittee on Commerce, Manufacturing, and Trade

From: Majority Committee Staff

Re: Hearing on "Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?"

I. Summary

The Subcommittee on Commerce, Manufacturing, and Trade will hold an oversight hearing on "Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?" on Thursday, July 18, 2013, at 11:00 a.m. in 2123 Rayburn House Office Building. Witnesses are by invitation only.

II. Witnesses

Dan Liutikas
Chief Legal Officer
CompTIA

Debbie Matties
Vice President of Privacy
CTIA - The Wireless Association

Jeff Greene
Senior Policy Counsel, Cybersecurity and Identity
Symantec Corporation

Kevin Richards
Senior Vice President, Federal Government Affairs
TechAmerica

Andrea M. Matwyshyn
Assistant Professor of Legal Studies and Business Ethics
The Wharton School, University of Pennsylvania

David Thaw
Visiting Assistant Professor of Law
University of Connecticut School of Law

III. Background

While 46 States, the District of Columbia, and Puerto Rico have each enacted data breach notification requirements, there is no Federal data breach notification law except the Health Insurance Portability and Accountability Act, as amended, which is limited to certain health-related information. Most State regimes define a data breach as the unauthorized acquisition of personal information. They typically define personal information in terms of data that may lead to identifying a specific individual (e.g., a combination of first, middle, or last names; social security numbers; State identification numbers; addresses) and data that may lead to financial harm (e.g., financial account number; pins; passcodes).

This patchwork of breach notification laws creates an environment in which companies who suffer a breach must then wade quickly through dozens of different definitions of personal information, event triggers, and notification timeframes to determine how to proceed. One recent study estimated the average cost of notification at $188 per record breached.[1] Since 2005, when the Subcommittee first began oversight of the issue, over 3,800 data breaches have been made public with more than 608 million records breached according to the Privacy Rights Clearinghouse.[2]

A wide variety of data breaches has focused policymakers' attention on the issue in recent years: from retailers to restaurants, financial institutions to government agencies, and hospitals to academic institutions. The information these entities collect can be used by a nefarious actor to empty bank accounts and establish new lines of credit, wreaking havoc on consumer financial identities and credit ratings.

Legislative History

The Subcommittee's work on data security reaches back to the 109th Congress, when Congressman Stearns (the then-Chairman of the Subcommittee on Commerce, Trade, and Consumer Protection) introduced H.R. 4127, the Data Accountability and Trust Act (DATA) in the wake of the ChoicePoint data breach. The bill proposed replacing the various State regimes with a uniform Federal notification standard and charged the FTC with enforcement. The Committee reported H.R. 4127 on a bipartisan basis, but the bill did not proceed to the full House for a vote as a result of disagreements with other committees regarding jurisdiction that could not be resolved before the Congressional calendar expired.

In the 110th Congress, then-Chairman Rush re-introduced DATA as reported by the Committee in the previous Congress. H.R. 958 received no Committee action. In the 111th Congress, Rep. Rush again reintroduced DATA as H.R. 2221, which processed through the Committee on a bipartisan basis and passed the House, as amended, by voice vote on December 8, 2009. The Senate took no action.

[1] Ponemon Institute, 2013 Cost of Data Breach Study: Global Analysis (May 2013).
[2] The Privacy Rights Clearinghouse tracks publicly reported incidents occurring in the U.S. This number does not include a tally of breached records if the incident was not reported to consumers or a government agency.

In the 112th Congress, Rep. Bono Mack held two oversight hearings on the topic, resulting in H.R. 2577, the SAFE Data Act. The Subcommittee reported the bill favorably as amended, but the bill received no further Committee action.

IV. Questions for Consideration

- Is a Federal data breach notification regime necessary?
- What should a Federal data breach notification regime look like?
- What constitutes a breach and what types should be reported? How quickly should breaches be reported?
- How should policymakers define harm in the context of data breaches?
- What is a company's current obligation to consumers whose information has been breached?
- Without preemption, is there a need for a Federal law?

Please contact Brian McCullough, Gib Mullan, or Shannon Taylor at ext. 5-2927 with any questions.