MEMORANDUM

TO: **MEMBERS OF THE SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION**

FROM: **REPUBLICAN COMMITTEE STAFF**

DATE: **FEBRUARY 3, 2015**

RE: **SUBCOMMITTEE HEARING ON "GETTING IT RIGHT ON DATA SECURITY AND BREACH NOTIFICATION LEGISLATION"; THURSDAY, FEBRUARY 5, 2015; 10:00 A.M.; SR-253**

On Thursday, February 5, 2015, at 10:00 A.M., in SR-253, the Senate Committee on Commerce, Science, and Transportation will hold a Consumer Protection Subcommittee hearing to discuss the need for federal data breach legislation. Chairman Moran will preside.

The following witnesses will testify before the Committee:

- Ms. Cheri F. McGuire, Vice President, Global Government Affairs & Cybersecurity Policy, Symantec Corporation
- Mr. Mallory Duncan, Senior Vice President and General Counsel, National Retail Federation
- Dr. Ravi Pendse, Chief Information Officer, Brown University
- Ms. Yael Weinman, Vice President for Global Privacy Policy and General Counsel, Information Technology Industry Council
- The Honorable Lisa Madigan, Attorney General, State of Illinois

SUMMARY

For over a decade, the Commerce Committee has been working on issues surrounding data security and breach notification. In 2004, the Committee held its first hearings on this issue following the high-profile breach of ChoicePoint, a large data aggregation firm. In the 113th Congress, the Committee continued its examination of these issues, in the wake of high-profile breaches of Target, Home Depot and others. Nevertheless, Congress has been unable to reach consensus on federal standards for generally applicable data security or notice requirements that entities must meet in the event of a breach. While sector-specific federal requirements apply to financial institutions, companies that handle certain health information, and pay-TV providers, companies outside of these sectors are covered by a patchwork of state laws regarding requirements on securing data and how to notify consumers in the event of a breach.

Recognizing the efficiencies associated with a single, preemptive federal notification requirement as well as the consumer benefit of a predictable and uniform notice, President Obama recently called for data breach notification legislation with state preemption language,

despite that fact that key Democrats have previously opposed such proposals.[1] For these reasons, there is renewed optimism among stakeholders that some form of a data breach bill is possible, perhaps early in the current Congress.

This hearing will include discussion on the key elements of a federal data breach bill, including, among other things, whether such a bill should include data security requirements, who should be covered under such a bill, the extent to which a federal law should preempt existing state law, how requirements would be triggered and enforced, assessing the timeliness of notification to consumers, and how personally identifiable information should be defined.

BACKGROUND

While this will be the Commerce Committee's first hearing on the issue of data security in the 114th Congress, the Commerce committee has examined this issue in previous Congresses.[2] The Commerce Committee has broad jurisdiction over the regulation of consumer products and services, which encompasses how companies keep and store sensitive personal information about customers or employees. In 2014, the Senate Judiciary and Banking Committees also held hearings to examine recent data breaches, focusing on privacy and cybercrime and the safeguarding of consumer financial data, respectively.

Numerous data breaches have been disclosed by the nation's largest retailers, educational institutions, government agencies, health care entities, financial institutions, and internet businesses. Data breaches that compromise personal information can result in identity theft and may facilitate financial crimes (such as fraud related to credit cards, banks, mortgages, government benefits, phone or utilities, loans, and health-care). As of 2015, the Privacy Rights Clearinghouse has estimated that over 4,400 breaches involving more than 932 million records have been made public since 2005.[3] The Verizon 2014 Data Breach Investigations Report reviewed more than 63,000 security incidents and found 1,367 confirmed data breaches in 2013.[4] According to Verizon's review, while retailer data breaches received top billing in 2013, a comprehensive assessment of the information security environment suggests that threats are transitioning to include a range of incidents from geopolitical attacks to large-scale attacks on payment card systems.[5]

Laws addressing the handling and protection of sensitive personal information are generally comprised of two major portions – *data security requirements* and *breach notification*

---

[1] *See, e.g.,* Remarks by the President at the Federal Trade Commission (January 12, 2015), *available at*: http://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission ("First, we're introducing new legislation to create a single, strong national standard so Americans know when their information has been stolen or misused. Right now, almost every state has a different law on this, and it's confusing for consumers and it's confusing for companies -- and it's costly, too, to have to comply to this patchwork of laws.")

[2] *See, e.g., Protecting Personal Consumer Information from Cyber Attacks and Data Breaches*, 113th Cong. (March 24, 2014) (Comm. print forthcoming); *Privacy and Data Security: Protecting Consumers in the Modern World*, S. Hrg. 112-152, 112th Cong. (June 29, 2011).

[3] PRIVACY RIGHTS CLEARINGHOUSE, *available at* http://www.privacyrights.org/data-breach.

[4] VERIZON, THE 2014 DATA BREACH INVESTIGATIONS REPORT at 2 (2014),*available at* http://www.verizonenterprise.com/DBIR.

[5] *Id.* at 3.

requirements. Data security portions are designed to protect sensitive personal information from compromise and from unauthorized disclosure, acquisition, access, or other situations where unauthorized persons have access or potential access. Breach notification requirements typically require covered entities to implement specific procedures for notification of affected parties (and sometimes remediation) when a breach occurs, and include requirements for incident reporting to appropriate parties (usually a government regulator or law enforcement agency).

No single federal law or regulation governs the security of all types of sensitive personal information.[6] U.S. corporate obligations to implement security measures have been set forth in a patchwork of federal and state laws, regulations, enforcement actions, as well as common law. Determining which law applies depends in part on the entity or sector that collected the information, the type of information collected, and the use for which it was collected. This is commonly referred to as the "sectoral approach" to the protection of personal information. Specific federal laws on data security and breach notification include the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, and Section 631 of the Communications Act.

While there is no uniform federal data security standard for businesses, industry has developed voluntary guidelines and best practices. The major credit card companies created a global data security standard for businesses who accept payment cards called the Payment Card Industry Data Security Standard (PCI-DSS).[7] All major credit card companies require merchants to comply with the PCI standards by contract. The standard has evolved formally at least six times since its initial release in 2004. The PCI Security Standards Council, the global forum that develops and maintains the PCI-DSS standard, describes the standard as "an actionable framework for developing a robust payment card data security process – including prevention, detection and appropriate reaction to security incidents."[8]

The FTC currently enforces data security requirements under its existing Section 5 authority, which prohibits unfair and deceptive acts or practices. In January 2014, the Commission announced its 50th data security settlement.[9] Currently, two pending court actions involve challenges to the FTC's data security enforcement authority: *FTC v. Wyndham Hotels & Resorts, LLC*,[10] and *LabMD*.[11]

State Laws

Breach Notification - As of February 1, 2015, 47 states and the District of Columbia, Puerto Rico, U.S. Virgin Islands, and Guam have enacted legislation requiring notification of security breaches of personal information. Three states—Alabama, New Mexico, and South Dakota—have no such laws.

---

[6] GINA STEVENS, CONG. RESEARCH SERV., RL 34120, FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS 1 (2010).
[7] PAYMENT CARD INDUS., PCI SSC SECURITY STANDARDS OVERVIEW, *available at* https://www.pcisecuritystandards.org/security_standards/index.php.
[8] *Id*.
[9] Press Release, Fed. Trade Comm'n, Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.
[10] FTC v. Wyndham Hotels & Resorts, LLC, et al., No. 14-3514 (3d Cir. filed Nov. 5, 2014).
[11] LabMD, Inc., F.T.C. File No. 102-3099 (Jan. 2, 2015) (Compl. Counsel's Opp'n to Resp'ts Mot. To Admit).

According to CRS, state security breach notification laws generally follow a similar framework and can be categorized into several standard elements: (1) delineating who must comply with the law; (2) defining the terms "personal information" and "breach of security"; (3) establishing the elements of harm that must occur, if any, for notice to be triggered; (4) adopting requirements for notice; (5) creating exemptions and safe harbors; (6) clarifying preemption and relationships to federal laws; and (7) creating penalties, enforcement authorities, and remedies. Many businesses that must comply with the requirements of the various state laws have strongly advocated for a single national standard that preempts the state requirements.[12]

Data Security Requirements - Currently, only 12 states have enacted laws governing commercial data security. These states include: Arkansas, California, Connecticut, Florida, Indiana, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, Texas, and Utah. Of these states, most have opted to require entities to adopt "reasonable security measures" to protect sensitive data, recognizing that more prescriptive requirements are complicated by changing technology and variations among covered entities, including the size and scope of the entity and the sensitivity of the data at issue.

KEY ISSUES

Data Security Requirements: Legislation focused solely on creating a federal standard for breach notification *may* be a more achievable path forward than legislation that also prescribes data security standards for covered entities. As noted, the Obama Administration has proposed legislation that contemplates a notification-only approach and is silent on security measures. If Congress does not address data security standards now, however, it may ultimately need to revisit the issue, as states would be free to continue to adopt potentially conflicting state standards.

Preemption: Discussion of preemption necessarily revolves around whether a federal bill should just preempt state breach notification laws, or state data security standards as well. A related question is whether federal preemption should preempt common law tort litigation by affected individuals and firms.

Trigger: Data breach notification laws all describe the conditions under which notification obligations are triggered. A number of previous proposals have favored a tight trigger that focuses on whether a reasonable risk of identity theft or financial harm to consumers exists in the event of a breach. Looser triggers, including language in the President's proposal, contemplate whether there is a risk of harm or fraud, generally. At the extreme, three states (Connecticut, New Jersey, and Puerto Rico), require notification in instances where data was accessed improperly, *absent any harm nexus*. If the trigger is not appropriately tailored to harm, there is a danger of over-notification leading to notification fatigue by consumers whereby they will not recognize when a breach requires increased vigilance or action on their part.

Timeliness of Notification: Some data breach notification laws specify that, in the event of a breach, notice to consumers must be provided within a specified period. Under current state law, six states prescribe discrete notification periods which range from 5 days (Connecticut) to 45

[12] GINA STEVENS, CONG. RESEARCH SERV., R 42475, DATA SECURITY BREACH NOTIFICATION LAWS 5 (2012).

days (Ohio, Vermont, and Wisconsin). Previous proposals have called for notification to be made "without unreasonable delay." In 2011, the President's previous proposal included a 60-day notification period. The President's current proposal calls for a 30-day notification period.

Personally Identifiable Information (PII) Definition: Data breach laws generally specify what sensitive personal information is subject to protections. The standard definition for PII, as found in the bill introduced by Senator Toomey in the 113th Congress (discussed below), includes an individual's first name or first initial *and* last name plus one or more of the following data elements: (i) Social Security number, (ii) driver's license number or state-issued ID card number, (iii) account number, credit card number or debit card number *combined with* any security code, access code, PIN or password needed to access an account. Some states have adopted additional elements in defining PII, such as biometric and geolocation data.

Covered Entities: The FTC has economy-wide jurisdiction, with the notable exceptions of Title II communications service providers (common carriers) and not-for-profit entities. There are also existing sector-specific data security regulations for certain types of information (GLBA, HIPAA, and pay-TV providers). There has been discussion over which entities should be subject to a federal data breach law and whether to carve out or capture those entities the FTC does not have jurisdiction over or are otherwise already subject to federal data security and breach standards enforced by other regulatory agencies.

CONGRESSIONAL ACTIVITY

On January 13, 2015, Senator Nelson introduced S. 177, the "Data Security and Breach Notification Act of 2015." This legislation, which is similar to bills sponsored by Senator Rockefeller, Nelson and others in the 111th, 112th, and 113th Congresses, gives the FTC streamlined rulemaking authority (under the Administrative Procedures Act, or "APA") to issue security standards for companies that hold consumers' personal and financial information to protect that information from unauthorized access. The FTC also would have authority to expand the definition of protected personally identifiable information through APA rulemaking. The bill also sets up requirements for breach notification (30 days with certain exceptions) to individuals and to law enforcement. The bill provides enforcement authority to the FTC and state Attorneys General, including the availability of civil penalties, but does not preempt all related state laws. The bill also creates a criminal offense (enforceable by the U.S. Secret Service and FBI) for willful concealment of a reportable data breach. This bill would not create a private right of action.

In the 113th Congress, several data breach legislative proposals were introduced and referred to a variety of committees, including Senate Commerce. Staff anticipates a number of these bills may be reintroduced in the current congress, which include:

S. 1193, the "Data Security and Breach Notification Act" of 2013 (Senators Toomey, Blunt, Coats, Heller, King, Roberts, Rubio, and Thune) (referred to Senate Commerce): This legislation would require commercial entities to take reasonable measures to protect and secure data in electronic form containing personal information. It requires notice of any breach of security that the covered entity believes has caused or will cause identity theft or other actual financial harm.

It also provides enforcement authority to the FTC with civil monetary penalties. The bill also preempts the security practices of the Communications Act, exempts entities subject to HIPAA, and preempts all related state laws. It does not provide a private cause of action.

S.1897, the "Personal Data Privacy and Security Act of 2014" (Senators Leahy, Franken, Schumer, and Blumenthal) (referred to Senate Judiciary): The legislation, which Senator Leahy has introduced in every Congress since 2005, toughens criminal penalties for persons who conceal a damaging breach, requires companies that keep data to establish adequate security policies, and strengthens penalties in the Computer Fraud and Abuse Act for attempted computer hacking. This approach would be enforced by both the U.S. Attorney General and state attorneys general. This bill would not create a private right of action.

S. 1927, the "Data Security Act of 2014" (Senators Carper and Blunt) (referred to Senate Banking): This legislation, which is similar to bills introduced in previous Congresses, is modeled after the regime established under the Gramm-Leach-Bliley Act of 1999. This legislation requires entities, including financial institutions, retailers, and federal agencies, to better safeguard sensitive information, investigate security breaches, and notify consumers when there is a substantial risk of identity theft or account fraud. It also preempts all related state law, does not provide for state civil or criminal action, and does not provide for a private right of action.

H.R. 3811, the "Health Exchange Security and Transparency Act of 2014" (referred to Senate Health, Education, Labor, and Pensions): On January 10, 2014, by a vote of 291-122, the House passed legislation that would require notice within two business days of any breach of a system maintained by an Obamacare Health Exchange that results in the theft of (or unlawful access to) personally identifiable information. Advocates of timely breach notification may point to this bill to suggest support for short notification deadlines. The bill also underscores the importance of considering personal data held by the federal government when discussing security and notification standards.