The Committee on Energy and Commerce

Memorandum

January 23, 2015

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

From: Majority Committee Staff

Re: Hearing on "What are the Elements of Sound Data Breach Legislation"

On Tuesday, January 27, 2015, the Subcommittee on Commerce, Manufacturing, and Trade will convene a hearing at 10:00 a.m. in 2123 of the Rayburn House Office Building entitled "What are the Elements of Sound Data Breach Legislation." Witnesses are by invitation only.

I. Witnesses

- Ms. Elizabeth Hyman, Executive Vice President, Public Policy, Tech America, powered by CompTIA
- Ms. Jennifer Glasgow, Chief Privacy Officer, Acxiom Corporation
- Mr. Brian Dodge, Executive Vice President, Communications and Strategic Initiatives, Retail Industry Leaders Association
- Mr. Woodrow Hartzog, Associate Professor, Cumberland School of Law,

II. Summary

Since the Energy and Commerce Committee first examined this issue following the data breach of ChoicePoint ten years ago, data security and breach notification issues have been debated in this Subcommittee, other committees in both chambers, the Federal Trade Commission (FTC), and State legislatures.[1] Currently, there are forty-seven different State laws dealing with data breach notification and twelve state laws governing commercial data security. This patchwork of State laws creates confusion for consumers looking for consistency and predictability in breach notices as well as compliance issues for businesses in the midst of securing their systems after a breach.

Consumers face an environment that involves an increasing risk of financial fraud and identity theft created by criminals with varying motivations, but a common goal—to steal personal information for financial gain. This hearing will give the Subcommittee an opportunity to hear from a number of industries that comply with the patchwork of State laws about the key elements and benefits of Federal data security and breach notification legislation.

III. Background

A. *CMT Subcommittee activity*

[1] *See* http://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million.

During the 113th Congress, the Subcommittee held two oversight hearings regarding data security and breach notification. On July 18, 2013, the Subcommittee held a hearing entitled "Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?"[2] Witnesses included representatives for CompTIA, CTIA – The Wireless Association, Symantec Corporation, TechAmerica, Professor Matwyshyn of The Wharton School at the University of Pennsylvania, and Professor Thaw of the University of Connecticut School of Law.

On February 5, 2014, the Subcommittee held a hearing entitled "Protecting Consumer Information: Can Data Breaches Be Prevented?" in response to high-profile criminal attacks on retailers, which resulted in the theft of the personal and financial information of millions of Americans. At this hearing, the Subcommittee received testimony from the FTC, the Attorney General for the State of Illinois, the Secret Service, the Department of Homeland Security, The Neiman Marcus Group, Target Brands Inc., PCI Security Standards Council, and Trustwave Holdings.

B. *The financial impact of data breaches*

Over the past year, the attacks on systems at The Home Depot U.S.A. Inc.[3], J.P. Morgan Chase & Co.,[4] AT&T Inc.,[5] United Parcel Service of North America Inc.,[6] eBay Inc.,[7] NYC Taxi & Limousine Commission,[8] SuperValue Inc.,[9] Cox Communications, Inc.,[10] Municipal Bond Insurance Association Inc.,[11] Jimmy John's Franchise LLC,[12] Dairy Queen Corp.,[13] Kmart,[14] Sony,[15] and others reinforce the fact that both companies and consumers must remain vigilant and be prepared to mitigate data loss in the event of a breach.

---

[2] http://docs.house.gov/meetings/IF/IF17/20130718/101152/HHRG-113-IF17-20130718-SD002.pdf
[3] Customer update on data breach, The Home Depot, https://corporate.homedepot.com/mediacenter/pages/statement1.aspx.
[4] Larry Magid, "JP Morgan Chase Warns Customers About Massive Data Breach." Oct. 2, 2014, 5:56 PM, Forbes, available at http://www.forbes.com/sites/larrymagid/2014/10/02/jp-morgan-chase-warns-customers-about-massive-data-breach/ (last accessed Nov. 3, 2014).
[5] Ina Fried, "AT&T Apologizes After Worker Improperly Accesses Customer Info." Oct. 6, 2014, 11:21 AM PDT, <re/code>, available at http://recode.net/2014/10/06/att-apologizes-after-worker-improperly-accesses-customer-info/ (last accessed Nov. 3, 2014).
[6] "Data Security Incident Information" The UPS Store, available at http://www.theupsstore.com/security/Pages/default.aspx (last accessed Nov. 3. 2014).
[7] "Ebay Inc. to ask Ebay users to change passwords." May 21, 2014, Ebay.com, available at http://announcements.ebay.com/2014/05/ebay-inc-to-ask-ebay-users-to-change-passwords/ (last accessed Nov. 4, 2014). *See* http://www.ebayinc.com/in_the_news/story/faq-ebay-password-change.
[8] Michael Carney, "Are the hackers winning? 2014 is shaping up as a record year in security breaches." August 22, 2014, Pando Daily, available at http://pando.com/2014/08/22/are-the-hackers-winning-2014-is-shaping-up-as-a-record-year-in-security-breaches/ (last accessed Nov. 4, 2014).
[9] Tom Huddleston, Jr. "Supervalu announces another possible data breach, finds malware on point-of-sale systems." Sept. 29, 2014, Fortune.com, available at http://fortune.com/2014/09/29/supervalu-malware-point-of-sale/ (last accessed Nov. 4, 2014).
[10] Brian Krebs, "We Take Your Privacy and Security. Seriously." Sept. 29, 2014, Krebs on Security, available at http://krebsonsecurity.com/2014/09/we-take-your-privacy-and-security-seriously/ (last accessed Nov. 3, 2014).
[11] Brian Krebs, "Huge Data Leak at Largest U.S. Bond Insurer." Oct. 7, 2014, Krebs on Security, available at http://krebsonsecurity.com/2014/10/huge-data-leak-at-largest-u-s-bond-insurer/ (last accessed Nov. 4, 2014).
[12] "Data Security Incident: Jimmy John's Notifies Customers of Payment Card Security Incident." Sept. 24, 2014, available at https://www.jimmyjohns.com/datasecurityincident/ (last accessed Nov. 3, 2014).
[13] Aaron Smith, "Dairy Queen customers get hacked." October 10, 2014, 8:01 AM ET, CNN Money, available at http://money.cnn.com/2014/10/10/news/companies/dairy-queen-malware/index.html?iid=HP_LN (last accessed Nov. 3, 2014).
[14] Kmart is a wholly owned subsidiary of Sears Holdings Corporation. http://www.kmart.com/en_us/dap/statement1010140.html?adcell=hpnewsrelease
[15] Brian Krebs, "Sony Breach May Have Exposed Employee Healthcare, Salary Data" Krebs on Security, Dec. 2, 2014, available at http://krebsonsecurity.com/2014/12/sony-breach-may-have-exposed-employee-healthcare-salary-data/.

The 2014 Verizon Report outlined over 63,000 security incidents, over 1,300 confirmed data breaches, from 50 contributing organizations.[16] Over a ten year period, the Verizon Report found that breach discovery methods have shifted significantly over time. Unrelated third parties, such as threat researchers and journalists monitoring black markets, have been the first parties to break news about hacks in various industries. In addition, breaches are discovered increasingly by law enforcement and companies' internal monitoring systems, which is a departure from previous years when fraud detection was the primary breach discovery method.

Cyber crime is a persistent threat to both the public and private sector. According to the Privacy Rights Clearinghouse, over 4,400 data breaches involving more than 930 million records have been made public since 2005.[17] In 2014 alone, the Clearinghouse reports over 260 data breaches occurred at educational institutions; insurance companies; hospitals and medical provider offices; technology companies; nonprofit organizations; banks; retailers; and restaurant and hotel chains. These breaches occurred via phishing, theft of computer or other devices, and hacking.

The costs to consumers and businesses of these malicious data breaches are substantial. The Ponemon Institute calculated the actual costs to the 54 businesses included in its report were $188 per identity compromised at a total organizational cost of $5.4 million.[18] Symantec's 2012 Norton Cybercrime report calculated the total cost of global cybercrime to be $110 billion, affecting 556 million victims annually.

There are factors that can mitigate the costs of a breach for companies. The cost of a data breach was reduced by $12.77 per record if the company had an incident response plan in place prior to the breach, and the appointment of a Chief Information Security Officer reduced per breach cost by $6.59.[19] On the other hand, third party involvement in a breach increased per record costs by $14.80 and quick notification increased costs by $10.45 per record.[20]

C. *Data Security – Federal and State requirements*

The Federal government currently mandates data security in just a few sectors: the financial sector,[21] the health sector,[22] and operators of children's websites.[23] In other sectors, the FTC has brought cases treating the failure to secure customer data as a violation of the prohibition against "unfair or deceptive trade practices."[24] The FTC has provided businesses

---

[16] "2014 Data Breach Investigations Report" Verizon Enterprise Solutions, p.2. Available at http://www.verizonenterprise.com/DBIR/2014/. (The report is not exclusive to the U.S. market, but includes data from 95 countries.)
[17] http://www.privacyrights.org/data-breach/new.
[18] Ponemon Institute, "2013 Cost of Data Breach Study: United States." The Ponemon report studied 54 cases and excluded those with breaches over 100,000 records for statistical purposes. The average number of records breached at the 54 companies was 28,765.
[19] Ponemon Institute Cost of Data Breach Study, p. 2 (2014).
[20] *Id.*
[21] See, e.g., the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.) and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq. and enacting regulations 66 Fed. Reg. 8616 (Feb. 1, 2001) and 69 Fed. Reg. 77610 (Dec. 28, 2004) promulgating and amending 12 C.F.R. Part 30, app. B (OCC); 12 C.F.R. Part 208, app. D-2 and Part 225, app. F (Board); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS))
[22] See the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. § 17931 et seq.).
[23] See the Children's Online Privacy Protection Act (15 U.S.C. § 6502).
[24] Nearly all of the Commission's data security cases have focused on "deception," for example, where a company's data security practices were not consistent with its stated policy. The Commission recently announced that it had settled a 50th case in this area.

with some suggested best practices for protecting personal information,[25] among other situations (e.g. copier data security and mobile app development).[26] Additionally, a handful of States have enacted data security laws, which generally require businesses to implement "reasonable" data security procedures and practices.[27] The Federal Communications Commission brought its first data security case last year against two telecommunications services that collected information from consumers applying for the Lifeline program and stored names, addresses, Social Security numbers, driver's licenses, and other information on publically available servers without password protection or encryption.[28]

No Federal law governs data security for businesses generally; however, there are industry-developed best practices.[29] 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). 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."[30]

The FTC has been active with respect to data security under their current Section 5 authority. In January 2014, they announced their 50th data security settlement under their Section 5 authority of the FTC Act to protect against deceptive and unfair commercial practices.[31] At this point, there are two ongoing cases challenging the FTC's data security enforcement authority that are in early stages of litigation: FTC v. Wyndham Hotels & Resorts, LLC[32] and against LabMD.[33] It is clear that as more and more companies begin to hold information about individuals, particularly with the Internet of Things (e.g. wearables and other connected devices) emerging in the marketplace, that the FTC's enforcement actions under Section 5 will continue.

A small number of States have enacted legislation dealing with commercial data security.[34] The majority of those States have tied the standard to "reasonable" security, recognizing the challenges posed by technology proscriptive mandates in this space.

D. *Breach Notification – Federal and State requirements*

Separate from data security, 47 States, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted data breach notification requirements. There is no Federal

---

[25] http://www.business.ftc.gov/documents/bus69-protecting-personal-information-guide-business
[26] http://www.business.ftc.gov/privacy-and-security/data-security
[27] California, Connecticut, Florida, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, and Texas require businesses to protect the information of consumers in their State.
[28] "FCC: The New Data Security Sheriff In Town." The National Law Review, Oct. 29, 2014, available at http://www.natlawreview.com/article/fcc-new-data-security-sheriff-town (last accessed Nov. 3, 2014).
[29] This is distinct from the European Union's approach that is currently considering a sweeping
[30] https://www.pcisecuritystandards.org/security_standards/index.php
[31] http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf
[32] http://www.ftc.gov/enforcement/cases-proceedings/1023142/wyndham-worldwide-corporation
[33] http://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter
[34] Arkansas, California, Connecticut, Florida, Indiana, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, Texas, and Utah.

data breach notification law except the Health Insurance Portability and Accountability Act (HIPAA), which applies only to certain health-related information. In March 2005, the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice was issued, requiring banks to notifying their primary regulators and consumers after a breach incident of sensitive consumer information.[35] Earlier this month, President Obama released language for a single, national standard for data breach notification at the FTC.[36]

There is a delicate balance to strike on the notification issue that is complicated by several factors. First, there are estimates that over 227,000 new malware samples are created worldwide every day.[37] Second, there are reports of breach fatigue among consumers.[38] Finding the correct balance between transparency for consumers and notice fatigue remains a challenge.

Most State notification 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) and data that may lead to financial harm (e.g., financial account number; pins; passcodes). This structure has been the basis for the majority of Federal legislative proposals.

IV. Questions for Consideration

- What are the key elements of a Federal data security and breach notification bill?
  - What are important components of a trigger for notifying consumers after a breach?
  - When should companies notify consumers after a breach? What factors go into that decision?
  - Does including a data security requirement in this bill add value for consumers and businesses navigating the current patchwork of State laws?
- What types of information lead to identity theft? Financial fraud?
- What elements of a breach notification bill are most critical to reduce the complexity associated with the existing 47 different State laws?
- What can be done to protect against customer over notification?

Please contact Paul Nagle, Melissa Froelich, or Graham Dufault of the Committee staff at (202) 225-2927 with questions.

[35] Department of the Treasury (Office of the Comptroller of the Currency and Office of Thrift Supervision), Federal Reserve System, and Federal Deposit Insurance Corporation, available at http://www.occ.gov/news-issuances/news-releases/2005/nr-ia-2005-35a.pdf.

[36] http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families (Jan. 12, 2015)

[37] http://www.net-security.org/malware_news.php?id=2905

[38] http://www.emc.com/collateral/brochure/consumer-perceptions-on-security.pdf. *See* http://www.darkreading.com/breach-fatigue-sets-in-with-consumers/d/d-id/1317194