THE COMMITTEE ON ENERGY AND COMMERCE

MEMORANDUM

February 3, 2014

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

From: Majority Committee Staff

Re: Hearing on "Protecting Consumer Information: Can Data Breaches Be Prevented?"

I. Summary

On Wednesday, February 5, 2014, at 9:30 a.m. in 2123 Rayburn House Office Building, the Subcommittee on Commerce, Manufacturing, and Trade will hold a hearing entitled "Protecting Consumer Information: Can Data Breaches Be Prevented?" Witnesses are by invitation only.

II. Witnesses

- Edith Ramirez, Chairwoman, Federal Trade Commission;
- Lisa Madigan, Attorney General, State of Illinois;
- William Noonan, Deputy Special Agent in Charge, Criminal Investigation Division, Cyber Operations, United States Secret Service;
- Lawrence Zelvin, Director, National Cybersecurity and Communications Integration Center, Department of Homeland Security;
- Michael Kingston, Senior Vice President & Chief Information Officer, The Neiman Marcus Group;
- John J. Mulligan, Executive Vice President & Chief Financial Officer, Target Brands Incorporated;
- Bob Russo, General Manager, PCI Security Standards Council, LLC; and
- Phillip J. Smith, Senior Vice President, Trustwave.

III. Background

Recent Attacks

A series of recent data breaches at nationwide retailers have exposed the payment card or personal information of millions of consumers. Investigations are ongoing so few details are known and even fewer are public. According to news reports, however, the initial breach at Target occurred from late-November to mid-December and made vulnerable nearly 40 million

payment accounts,[1] while up to 1.1 million payment accounts were jeopardized at Neiman Marcus from July to October. Michael's, the arts-and-crafts retailer, has confirmed that it too suffered a recent data breach, but it has yet to disclose the number of payment accounts involved.

While it is unclear if these recent attacks were perpetrated by the same cyber criminals, the perpetrators reportedly used similar methods. In each of these incidents, the hackers appear to have used memory-parsing software, also called a RAM scraper, to infect the point-of-sale (POS) terminals in the retailers' physical stores, permitting the criminals to seize payment card data. While payment card data is usually encrypted, there is a brief period of time during the authorization process in which the data is unencrypted and temporarily stored in a payment system's live memory, making it vulnerable to unauthorized acquisition. This type of malware first appeared about a decade ago according to security experts and has been improved incrementally by cyber criminals over the years such that it is difficult for anti-virus software to detect. The software also is relatively inexpensive, making it widely accessible to would-be hackers; a version of the malware used in the Target attack – dubbed Kaptoxa – sold for a mere $2,000 on the black market earlier in 2013.[2]

Emphasizing the sophistication of these cyber criminals, one media report indicated that as cybersecurity firms learned of the popularity of this particular type of malware and developed defenses over the last year, the hackers quickly modified the code to evade detection.[3] Unfortunately, even more consumers may find their personal data taken in attacks that have yet to be reported in the press or made public by retailers. According to news reports, the FBI recently warned retailers that they discovered an additional 20 attacks that occurred in 2013 using the same malware that was employed against Target's point-of-sale (POS) terminals in November and December.[4]

Data Breaches, by the Numbers

Cybercrime targeting consumer information is a constant and growing threat. The issue of data breach hit public consciousness in 2005 when hackers gained access to 160,000 consumer records in the ChoicePoint data breach. Since then, American consumers have been inundated with reports of data breaches. According to the Privacy Rights Clearinghouse, over 4,100 data breaches involving more than 660 million records have been made public since 2005.[5] In December 2013 alone, the Clearinghouse reports over 52 data breaches occurred at hospitals and medical provider offices; educational institutions; insurance companies; technology

---

[1] As a result of the ensuing forensic investigation, Target discovered that besides the payment card information, other consumer information, such as names and e-mail addresses, had been taken in the same breach. These records related to as many as 70 million Target customers.

[2] http://online.wsj.com/news/articles/SB10001424052702304027204579335121871310960?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702304027204579335121871310960.html.

[3] http://online.wsj.com/news/articles/SB10001424052702304027204579335121871310960?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702304027204579335121871310960.html.

[4] http://www.reuters.com/article/2014/01/24/us-target-databreach-fbi-idUSBREA0M1UF20140124.

[5] http://www.privacyrights.org/data-breach/new.

companies; banks; retailers; and restaurant and hotel chains. These breaches occurred via phishing, theft of computer or other devices, and hacking. Last year also saw dozens of breaches involving data held by governments at the municipal, State, and Federal levels.

With an estimated 9 to 10 million merchants accepting payment cards in the U.S., it is not surprising that Trustwave identified payment card data as the primary target of data thieves in its "2013 Global Security Report."[6] According to the Federal Reserve, cardholders in the U.S. "used more than one billion debit and credit cards in 2011, making 69 billion transactions, valued at more than $3.9 trillion . . .."[7] To put that in perspective, the U.S. activity accounts for 30 percent of all credit and debit card transactions globally. Unfortunately, the U.S. is even more overrepresented when it comes to payment card fraud: in 2012, the $5.3 billion in fraud losses in the U.S. amounted to 47 percent of such losses worldwide.[8]

While data breaches include both malicious criminal attacks and non-criminal negligence (e.g., loss of a laptop), the Ponemon Institute reported that in 2013, for the first time, malicious or criminal attacks were the main cause of breaches in its study sample. 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.[9] More broadly, in testimony before this Committee last year, Symantec's 2012 Norton Cybercrime report calculated the total cost of global cybercrime to be $110 billion, affecting 556 million victims annually.

Existing Regulation

Data Security

The Federal government currently mandates data security in just a few sectors: the financial sector,[10] the health sector,[11] and operators of children's websites.[12] In other sectors, the Federal Trade Commission has brought cases treating failure to secure customer data as a violation of the prohibition against "unfair or deceptive trade practices."[13] Additionally, a

[6] Available for download at https://www2.trustwave.com/2013GSR.html?sl=gsr-2012.
[7] http://www.kansascityfed.org/publicat/econrev/pdf/13q1Sullivan.pdf .
[8] http://apps.washingtonpost.com/g/page/business/smart-banking-cards-catching-on-everywhere-but-us/749/
[9] 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.
[10] 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.).
[11] 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.).
[12] See the Children's Online Privacy Protection Act (15 U.S.C. § 6502).
[13] 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.

handful of states have enacted data security laws, which generally require businesses to implement "reasonable" data security procedures and practices.[14]

While there is no widespread State regulation of data security, nor any Federal law that governs data security for businesses generally, there are industry-developed 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). All major credit card companies require merchants to comply with the PCI standards by contract. The standard has formally evolved 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."[15] There are 12 specific requirements across six categories under the PCI-DSS:

Build and Maintain a Secure Network and Systems

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need to know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel[16]

Data Breach Notification

Distinct from data security, at least 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 data breach notification law except the Health Insurance Portability and

[14] California, Connecticut, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, and Texas require businesses to protect the information of consumers in their State.
[15] https://www.pcisecuritystandards.org/security_standards/index.php
[16] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

Accountability Act (HIPAA), as amended, which applies only to certain health-related information. 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; addresses) and data that may lead to financial harm (e.g., financial account number; pins; passcodes).

IV. Questions for Consideration

- What is the relationship between Federal law enforcement and the private sector in tracking and responding to breaches of consumer information?
- How do private sector entities work amongst themselves and with those involved in the Federal government's cybersecurity efforts to develop and maintain best practices?
- How have the tactics and efforts of cybercriminals changed over time?
- Is it possible or realistic for a company to be impervious to data breaches?
- Is additional regulation of data security necessary?

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