U.S. SENATE BANKING, HOUSING AND URBAN AFFAIRS COMMITTEE

MEMORANDUM

TO: Banking Committee Members and Staff
FROM: Milan Dalal, National Security and International Trade and Finance Staff
DATE: February 3, 2014
RE: Hearing: "Safeguarding Consumers' Financial Data"

On Monday, February 3, 2014, at 3:00 p.m., in room 538 of the Dirksen Senate Office Building, the Subcommittee on National Security and International Trade and Finance will hold a hearing entitled, "**Safeguarding Consumers' Financial Data**". The witnesses, who will appear on two panels, will be:

Panel I:

- **Mr. William Noonan**, Deputy Special Agent in Charge, United States Secret Service;
- **Ms. Jessica Rich**, Director, Bureau of Consumer Protection, Federal Trade Commission.

Panel II:

- **Mr. James Reuter**, Executive Vice President, FirstBank, on behalf of the American Bankers Association;
- **Mr. Mallory Duncan**, General Counsel, National Retail Federation;
- **Mr. Edmund Mierzwinski**, Consumer Program Director, U.S. PIRG;
- **Mr. Troy Leach**, Chief Technology Officer, PCI Security Standards Council.

Overview[1]

This hearing will examine the procedures for overseeing data security and breaches of data security by the United States Secret Service and the Federal Trade Commission. Specifically, the Secret Service and FTC have been asked to detail how data breaches of consumer financial data are investigated, and what steps are taken to notify merchants and/or financial institutions that data has been compromised. They have also been asked to describe what steps can be taken by merchants and financial institutions to prevent future breaches. The hearing will also probe the adequacy of current technology in securing consumer financial data and how new technology, including EMV or "chip and PIN," or other emerging payment systems, may affect the financial industry's ability to combat credit and debit card fraud. Finally, the hearing will examine recommendations, legislative or otherwise, for strengthening data protections for consumers in the financial marketplace.

[1] Portions of this hearing memo include contributions from Gina M. Stevens, Legislative Attorney, Congressional Research Service (x7-6006).

Summary of Recent High Profile Data Breaches at Merchants

A brief chronology of significant data breaches follows.[2] The term "data breach" generally refers to the unauthorized or unintentional exposure, disclosure, or loss of sensitive or personally identifiable information.

- In February 2005, the data broker ChoicePoint disclosed a security breach involving the personal information of 163,000 persons.

- In 2006, the personal data of 26.5 million veterans was breached when a VA employee's hard drive was stolen from his home.

- In 2007, the retailer TJX Companies revealed that 46.2 million credit and debit cards may have been compromised during the breach of its computer network by unauthorized individuals. In the end, over 94 million accounts were affected. TJX was subject to several class action lawsuits on behalf of both customers and financial institutions who suffered fraud losses as a result of the breach.

- In 2008, the Hannaford supermarket chain revealed that approximately 4 million debit and credit card numbers were compromised when Hannaford's computer systems were illegally accessed while the cards were being authorized for purchase.

- In 2009, 130 million records from credit card processor Heartland Payment Systems Inc. of Princeton, N.J., were breached.[3] Also, in 2009, personal information from Health Net on almost half a million Connecticut residents and 1.5 million patients nationally was breached.

- In 2011, another breach of patient data occurred when data for 20,000 emergency room patients from Stanford Hospital in California was posted on a commercial website for nearly a year.

- In late April of 2011, Sony, Inc. shut down its online PlayStation Network (PSN) in response to a data security breach.

- In January 2012, New York State Electric & Gas and Rochester Gas and Electric, subsidiaries of Iberdrola USA, sent notices to customers advising them of unauthorized access to customer data on the companies' customer information systems, which contained Social Security numbers, dates of birth, and financial institution account numbers.[4]

---

[2] CRS Report R42475, *Data Security Breach Notification Laws*, by Gina Stevens. See also, Privacy Rights Clearinghouse, Chronology of Data Breaches Security Breaches 2005 – Present, at https://www.privacyrights.org/data-breach.

[3] Cheney, Julia S., Heartland Payment Systems: Lessons Learned from a Data Breach (January 1, 2010). FRB of Philadelphia - Payment Cards Center Discussion Paper No. 10-1. Available at http://dx.doi.org/10.2139/ssrn.1540143.

[4] State of New York Public Service Commission, PSC Investigates Consumer Data Breach at NYSEG, RG&E (Jan. 23, 2012); at http://www3.dps.ny.gov/pscweb/WebFileRoom.nsf/ArticlesByCategory/1986D5ECA1917A8A8525798E005F81DD/$File/pr12007.pdf?OpenElement.

- The 2013 Target data breach compromised the credit and debit card account information of as many as 70 million Target customers over the holidays. Neiman Marcus disclosed a breach in January 2014 that involved 1.1 million credit and debit cards. Arts-and-crafts-supplies retailer Michaels Stores recently disclosed that a data-security attack on Michaels that may have affected its customers' payment card information.

Rights and Recourse for Consumers Whose Data is Compromised

Federal law limits consumer liability for unauthorized credit card charges to a maximum of $50 per account.[5] However, credit card companies and most credit card issuers have a "zero liability" policy that minimizes consumer liability.[6] With respect to ATM and debit card transactions, under the Electronic Funds Transfer Act,[7] and its implementing Regulation E,[8] consumer liability for unauthorized use of a lost or stolen card is generally limited to between $50 and $500.[9]

Target has pledged to its customers that they will have zero liability for the cost of any fraudulent charges arising from the breach, and is offering one year of free credit monitoring and identity theft protection to all customers who shopped at its U.S. stores.[10] Neiman's has done the same.

The Consumer Financial Protection Bureau (CFPB) has issued an alert for consumers outlining steps it recommends be taken if one's personally identifiable information is part of a large breach.[11] CFPB advises that consumers check their accounts for unauthorized charges or debits and monitor those accounts continuously; report suspicious charges or debits immediately; submit a complaint if there is an issue with the bank or card provider's response; and know when to ignore anyone contacting the consumer to verify account information by phone or email.

Many state data breach notification laws permit affected consumers to bring a civil action for violations of the state statute requiring notification of data security breaches, or as an unfair or deceptive trade practice.[12] At least seventy putative class actions have recently been filed against Target in various federal courts for damages allegedly caused by the massive security

[5] 15 U.S.C. § 1643.

[6] See, e.g., Zero Liability Protection for Lost & Stolen Cards, at http://www.mastercard.us/zero-liability.html.

[7] 15 U.S.C. §§ 1693 et seq.

[8] 12 C.F.R. Part 205.

[9] 15 U.S.C. § 1693(g) ; 12 C.F.R. §205.6.

[10] Http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1889763&highlight=.

[11] Http://www.consumerfinance.gov/blog/four-steps-you-can-take-if-you-think-your-credit-or-debit-card-data-was-hacked/.

[12] Alaska, California, Louisiana, Maryland, Massachusetts, Nevada, New Hampshire, North Carolina, Oregon, South Carolina, Tennessee, Texas, Virginia, Washington, District of Columbia, Puerto Rico, Virgin Islands. See also, National Conference of State Legislators, State Security Breach Notification Laws, Jan. 21, 2014, at http://www.ncsl.org/research/telecommunications- and-information-technology/security-breach-notification-laws.aspx.

breach of its customers' personal and financial information.[13]

Rights and Recourse for Merchants and Financial Institutions

Responsibility for the costs of security breaches and credit card fraud[14] is the subject of much attention and litigation.[15] Retailers, payments processors, banks, and card issuers are affected by data security breaches, and are incurring substantial costs.[16] In 2011, the Federal Reserve "Board estimated fraud losses to all parties (merchants, cardholders, and issuers) to be $1.38 billion in 2011." [17] The distribution of fraud losses was as follows:

> Signature transactions accounted for $1.13 billion of those losses while PIN accounted for $204 million. Prepaid card fraud losses were $51 million. The incidence of debit card fraud was 0.3 percent of transactions, down from 0.4 percent in 2009. Card-not-present and counterfeit card fraud continue to be the most common types of debit card fraud reported. Issuers bore 60 percent, merchants bore 38 percent, and cardholders bore 2 percent of debit card fraud losses. The distribution of fraud losses differed significantly by authentication method, with issuers bearing virtually all PIN debit fraud losses (96 percent) and slightly more than half (54 percent) of signature debit fraud losses. Merchants continued to bear the majority of card-not-present losses, and issuers bear most of the counterfeit card fraud losses.[18]

The payment card industry has issued security standards and reporting requirements for organizations that handle bank cards.[19] The Payment Card Industry Data Security Standard (PCI DSS) is an industry regulation developed by VISA, MasterCard, and other bank card distributors. It requires organizations that handle bank cards to conform to security standards and follow certain leveled requirements for testing and reporting. The core of the PCI DSS is a

---

[13] Law360, Measuring the Bull's-Eye on Target's Back, Jan. 17, 2014.

[14] Burns, Peter and Stanley, Anne, Fraud Management in the Credit Card Industry (April 2002). Federal Reserve Bank of Philla Payment Cards Center Discussion Paper No. 02-05. Available at SSRN: http://ssrn.com/abstract=927784 or http://dx.doi.org/10.2139/ssrn.927784.

[15] Antonio Olivero, On Heels of Security Breaches, The Independent Community Bankers of America (ICBA) Lashes Back at Retailer Group, American Banker, Jan. 22, 2014.

[16] Tim Stapleton, Data Breach Cost: Risks, Costs, and Mitigation Strategies for Data Breaches (2012), http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/products/securityandprivacy/data%20breach%20costs%20wp%20part%201%20(risks,%20costs%20and%20mitigation%20strategies).pdf; Ross Keber, Data Breach Could Prove Costly for Target's Payment Vendors (Jan. 15, 2014), http://www.claimsjournal.com/news/national/2014/01/15/242939.htm; Target Breach To Cost Credit Unions Estimated $25M-$30M, CUNA Study Shows, http://www.cuna.org/webassets/pages/newsnowarticle.aspx?id=67470.

[17] Board of Governors of the Federal Reserve System, 2011 Interchange Fee Revenue, Covered Issuer Costs, and Covered Issuer and Merchant Fraud Losses Related to Debit Card Transactions, March 5, 2013, at http://www.federalreserve.gov/paymentsystems/files/debitfees_costs_2011.pdf.

[18] Id.

[19] Available at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

group of principles and accompanying requirements designed to build and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, monitor and test networks, and maintain an information security policy. PCI DSS went into effect December 31, 2006. Entities that fail to comply with PCI DSS face fines and increase in the rates that the credit card companies charge for transactions, and potentially can have their authorization to process payment cards revoked. Legislation has been passed in the Texas House mandating compliance with the PCI DSS standard.[20]

Merchants and processors could also face class action lawsuits from both consumers and issuing financial institutions.[21] TJX Companies was sued by both consumers and VISA.[22]

Relevant Law Enforcement and Regulatory Agencies

The United States Secret Service is responsible for maintaining the integrity of the nation's financial infrastructure and payment systems.[23] The Secret Service implements and evaluates prevention and response measures to guard against electronic crimes as well as other computer related fraud. Criminal investigations can be international in scope. These investigations include: counterfeiting of U.S. currency (to include coins); counterfeiting of foreign currency (occurring domestically); identity crimes such as access device fraud, identity theft, false identification fraud, bank fraud and check fraud; telemarketing fraud; telecommunications fraud (cellular and hard wire); computer fraud; fraud targeting automated payment systems and teller machines; direct deposit fraud; investigations of forgery, uttering, alterations, false impersonations or false claims involving U.S. Treasury Checks, U.S. Saving Bonds, U.S. Treasury Notes, Bonds and Bills; electronic funds transfer (EFT) including Treasury disbursements and fraud within the Treasury payment systems; Federal Deposit Insurance Corporation investigations; Farm Credit Administration violations; and fictitious or fraudulent commercial instruments and foreign securities.

The United States Department of Justice's Computer Crime & Intellectual Property Section (CCIPS)[24] prosecutes a variety of computer crime cases,[25] focusing on those involving large scale data breaches, identity theft, and online payment systems.[26]

The Federal Trade Commission seeks remedies including permanent injunction, consumer redress, disgorgement, and other equitable relief for data security breaches for acts or practices in violation of Section 5(a) of the Federal Trade Commission Act (FTC) Act.[27] Section 5(a) of

[20] *See*, 2007 Tex. H. B. No. 3222 which mandates PCI DSS compliance, and provides a safe harbor under the statute if the business that suffered the data breach was in compliance with PCI DSS 90 days before the date of the security breach.

[21] Kim Phan, Assessing risk: Data breach litigation in U.S. courts, Nov. 1, 2012, The Privacy Advisor, https://www.privacyassociation.org/publications/2012_11_01_assessing_risk_data_breach_litigation_in_u.s._courts.

[22] Mark Jewell, TJX, Visa Reach $40.9M Settlement For Data Breach, USA TODAY, Nov. 30, 2007.

[23] 18 U.S.C. § 3056. See, http://www.secretservice.gov/criminal.shtml.

[24] Http://www.justice.gov/criminal/cybercrime/.

[25] Kimberly Peretti, *Data Breaches: What The Underground World of "Carding" Reveals*, 25 Santa Clara Computer & High Tech L.J. 375 (2009). Available at http://digitalcommons.law.scu.edu/chtlj/vol25/iss2/4.

[26] Brian Mahoney, Holder Confirms Target Breach Probe, Warns Of Cyberattacks, Law360, Jan. 29, 2014.

[27] 15 U.S.C. § 45(a).

the Federal Trade Commission Act, prohibits ''unfair or deceptive acts or practices, including deceptive statements and unfair practices involving the use or protection of consumers' personal information. The FTC has brought several data security cases alleging that the companies that have had a data breach have failed to use ''reasonable and appropriate'' safeguards to protect the personal information they collect and maintain, an alleged ''unfair'' business practice. Prior FTC enforcement actions, which resulted in over a dozen consent decrees, illuminate what constitutes ''reasonable'' security.[28]

[28] See, e.g., Scott, Michael D., The FTC, the Unfairness Doctrine and Data Security Litigation: Has the Commission Gone Too Far? (August 21, 2007). Available at SSRN: http://ssrn.com/abstract=1012232 or http://dx.doi.org/10.2139/ssrn.1012232.