Congressional Research Service
Informing the legislative debate since 1914

The Target and Other Financial Data Breaches: Frequently Asked Questions

N. Eric Weiss
Specialist in Financial Economics

Rena S. Miller
Specialist in Financial Economics

February 4, 2015

Congressional Research Service
7-5700
www.crs.gov
R43496

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

In November and December of 2013, cybercriminals breached the data security of Target, one of the largest U.S. retail chains, stealing the personal and financial information of millions of customers. On December 19, 2013, Target confirmed that some 40 million credit and debit card account numbers had been stolen. On January 10, 2014, Target announced that personal information, including the names, addresses, phone numbers, and email addresses of up to 70 million customers, was also stolen during the data breach. A report by the Senate Committee on Commerce in March 2014 concluded that Target missed opportunities to prevent the data breach.

Target. To date, Target has reported data breach costs of $248 million. Independent sources have made back-of-the-envelope estimates ranging from $240 million to $2.2 billion in fraudulent charges alone. This does not include additional potential costs to consumers concerned about their personal information or credit histories; potential fines or penalties to Target, financial institutions, or others; or any costs to Target related to a loss of consumer confidence. The breach was among the largest in U.S. history.

Consumer concern over the scale of this data breach has fueled further congressional attention on the Target breach and data security and data breaches more broadly. In the wake of Target's revelations, between February 3 and April 2, 2014, Congress held seven hearings by six different committees related to these topics. In addition to examining the events surrounding the Target breach, hearings have focused on preventing such data breaches, improving data security standards, protecting consumers' personal data, and notifying consumers when their data have been compromised.

Other financial data breaches. In addition to Target, there have been data breaches at Home Depot, JPMorgan Chase, Sony, and Adobe. Payment card information was obtained at Adobe and Home Depot. Hackers downloaded a wide range of company confidential information at Sony, and they obtained contact information in the JPMorgan Chase breach.

Policy options discussed in these hearings include federal legislation to require notification to consumers when their data have been breached; potentially increase Federal Trade Commission (FTC) powers and authorities over companies' data security; and create a federal standard for the general quality or reasonableness of companies' data security. The hearings also broached the broader question of whether the government should play a role in encouraging or even requiring companies to adopt newer data security technologies.

None of the legislation introduced in the 113th Congress that addressed these various issues became law. In 2014 and 2015, the Obama Administration encouraged Congress to pass legislation on data security and data breach notification. Attorney General Eric Holder issued a public statement in the wake of the Target breach on February 24, 2014, that urged Congress to pass a federal data breach notification law, which would hold entities accountable when they fail to keep sensitive information safe. The FTC also called on Congress to pass a federal data security law, including data breach notification and to increase the commission's explicit statutory authority over data security issues.

Key questions. This report answers some frequently asked questions about the Target and selected other data breaches, including what is known to have happened in the breach, and what costs may result. It also examines some of the broader issues common to data breaches, including

how the payment system works, how cybersecurity costs are shared and allocated within the payment system, who bears the losses in such breaches more generally, what emerging cybersecurity technologies may help prevent them, and what role the government could play in encouraging their adoption. The report addresses policy issues that were discussed in the 113th Congress to deal with these issues.

Updating. This report will be updated as warranted by legislative action in the 114th Congress and by further payment system developments.

Contents

Figures

Tables

Contacts

What Were Some Recent Financial Data Breaches?

In recent years, financial data breaches have exposed a variety of personal information concerning finances, personally identifiable information (PII), health care, legal issues, and more. The theft of this information was accomplished by outsiders hacking computer systems, insiders with and without authorized access to the files, loss of laptops and other physical media, and accidental publication. According to one source, 78% of all records compromised during the first six months of 2014 were exposed as the result of outsiders.[1]

Recent large financial data breaches affecting the payment system include[2]

- Target: 2013, 40 million payment cards, 70 million records of customer names, addresses, telephone numbers, and email addresses;
- Adobe: 2013, 152 million customer names, encrypted passwords, encrypted payment card information;
- Home Depot: 2014, 56 million customer email addresses and payment cards;
- Heartland: 2009, 130 million payment card records; and
- TJX: 2007, 94 million payment card records (credit card numbers and transactions).

This report concentrates on the loss of financial data, but there have also been nonfinancial data breaches, including

- Sony Corporation (PlayStation Network): 2011, 77 million names, addresses, email addresses, and other personal information;
- Sony Picture Entertainment: 2014, a large, but unknown number of files reportedly containing personal information, internal Sony discussions, and unreleased movies, and other;
- JPMorgan Chase & Co. (JPMorgan): 2014, 76 million household customer names, telephone numbers, and other information and 7 million small business records; and
- Tricare Management Activity: 2011, 4.9 medical records lost.[3]

Breaches have also occurred in other nations, including Korea (2014), the theft of 220 million records containing personal information and passwords, and China (2012), 150 million records stolen from Shanghai Roadway & Marketing.

[1] Risk Based Security, Open Security Foundation, *Data Breach Quick View: Data Breach Trends during the First Half of 2014*, https://www.riskbasedsecurity.com/reports/2014-MidYearDataBreachQuickView.pdf.

[2] Unless otherwise credited, this listing is based on Open Security Foundation, *Data Loss db*, http://datalossdb.org/.

[3] U.S. Department of Health & Human Services, *Health Information Privacy*, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

Target Breach

According to Target,[4] in November and December of 2013, information on 40 million payment cards (i.e., credit, debit, and ATM cards) and personally identifiable information (PII) on 70 million customers was compromised. The Secret Service has announced that it is investigating the data breach, but has released no details.[5] In congressional hearings, Target's executive vice president testified that an intruder used a vendor's access to Target's system to place malware on point-of-sale (POS) registers. The malware captured credit and debit card information before it was encrypted, which would render it more difficult (or impossible) to read. In addition, the intruder captured some strongly encrypted personal identification numbers (PIN).

It is very unlikely that all 40 million payment cards compromised at Target will be used in fraudulent transactions. Some cards will be canceled before they are used, some attempts to use valid cards will be denied by the issuing financial institutions, and there will be no attempt to make fraudulent use of some.

According to media reports, some financial institutions responded to the Target breach by issuing new cards to all of their cardholders, and others decided to depend on antifraud monitoring. Initially, Wells Fargo, Citibank, and JPMorgan Chase replaced debit cards, but not credit cards, and Bank of America and U.S. Bank are depending on fraud detection.[6]

Target Breach Timeline

Companies that suffer data breaches rarely publish detailed timelines. Target, possibly because senior management testified before Congress on the situation, is an exception to this rule.

According to testimony of John J. Mulligan, executive vice president and chief financial officer of Target, the key dates in the Target breach are as follows:[7]

- November 12, 2013—intruders breached Target's computer system. The intrusion was detected by Target's security systems, but the company's security professionals took no action until notified by law enforcement of the breach.

[4] Testimony of John J. Mulligan, executive vice president and chief financial officer, Target, before U.S. Congress, Senate, Committee on Commerce, Science, and Transportation, *Protecting Personal Consumer Information from Cyber Attacks and Data Breaches*, 113th Cong., 2nd sess., March 26, 2014, at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=c2103bd3-8c40-42c3-973b-bd08c7de45ef; U.S. Congress, Senate, Committee on the Judiciary, *Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime*, 113th Cong., 2nd sess., February 4, 2014, at http://www.judiciary.senate.gov/pdf/02-04-14MulliganTestimony.pdf, and U.S. Congress, House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, *Protecting Consumer Information: Can Data Breaches Be Prevented?*, 113th Cong., 2nd sess., February 5, 2014, at http://docs.house.gov/meetings/IF/IF17/20140205/101714/HMTG-113-IF17-Wstate-MulliganJ-20140205.pdf.

[5] Hilary Stout, "Target Vows to Speed Anti-Fraud Technology," *New York Times*, February 4, 2014, at http://www.nytimes.com/2014/02/05/business/target-to-speed-adoption-of-european-anti-fraud-technology.html.

[6] Jennifer Bjorhus, "Banks Have Replaced 15.3 Million Cards since Target Breach," *Minneapolis Star Tribune*, January 29, 2014, at http://www.startribune.com/business/242505661.html, and Nathaniel Popper, "Theft at Target Leads Citi to Replace Debit Cards," *New York Times*, January 16, 2014, p. B3, New York, at http://www.nytimes.com/2014/01/16/business/theft-at-target-leads-citi-to-replace-debit-cards.html?_r=0.

[7] Home Depot and JPMorgan have not released similar timelines.

- December 12, 2013—the Department of Justice (DOJ) notified Target that there was suspicious activity involving payment cards that had been used at Target.
- December 13, 2013—Target met with DOJ and the U.S. Secret Service.
- December 14, 2013—Target hired outside experts to conduct a thorough forensic investigation.
- December 15, 2013—Target confirmed that malware had been installed and that most of the malware had been removed.
- December 16 and 17, 2013—Target notified payment processors and card networks that a breach had occurred.
- December 18, 2013—Target removed the remaining malware.
- December 19, 2013—Target made a public announcement of the breach.
- December 27, 2013—Target announced the theft of the encrypted PIN data.
- January 9, 2014—Target discovered the theft of PII.
- January 10, 2014—Target announced the PII theft.

Target estimates that the 40 million payment card and 70 million PII data breaches have at least 12 million people in common, making 98 million the maximum number of customers affected.[8]

Fazio Mechanical Services, which provided heating, ventilation, and air conditioning (HVAC) services for Target, has said it was used to breach Target's payment system. A Fazio computer authorized to submit contract billing and project management information to Target reportedly was compromised by intruders. According to some media reports, Fazio was the victim of a phishing email containing malware that was used to install other malware in Target's network, including its POS system that records payment card transactions.[9]

Payment card companies require any business accepting payment cards to follow PCI rules regarding security of their payment card processing. Target has testified that its systems were reviewed in September 2013 and certified as compliant.

The magnetic stripes on the back of U.S. credit cards are not encrypted. According to media reports, malware known as a "memory scraper" captured information from customers' payment cards by reading the POS system's memory before it was encrypted.[10]

After the initial announcement of the Target data breach, other possibly related data breaches were reported, including at Neiman Marcus (a luxury retailer), Michaels (an arts and crafts

[8] Testimony of John J. Mulligan, executive vice president and chief financial officer, Target, before U.S. Congress, Senate, Committee on Commerce, Science, and Transportation, *Protecting Personal Consumer Information from Cyber Attacks and Data Breaches*, 113th Cong., 2nd sess., March 26, 2014, p. 5, at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=c2103bd3-8c40-42c3-973b-bd08c7de45ef.

[9] Brian Krebs, "Email Attack on Vendor Set up Breach at Target," *Krebs on Security*, February 14, 2014, at https://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.

[10] Jim Finkle and Mark Hosenball, "Exclusive: FBI Warns Retailers to Expect More Credit Card Breaches," *Reuters*, January 23, 2014, at http://www.reuters.com/article/2014/01/24/us-target-databreach-fbi-idUSBREA0M1UF20140124.

retailer), Home Depot, OneStopParking, and White Lodging (a hotel management company), which had been notified by law enforcement that they had suffered related data breaches.[11]

In summary,[12] it appears that

1. someone obtained a vendor's credentials to access the Target vendor billing and invoicing system,
2. access to the vendor billing and invoicing system was escalated to access into Target's POS system,
3. this was used to introduce malware into the system,
4. warnings about this malware were initially ignored,
5. Target software was used to spread the malware to virtually all of Target's POS devices,
6. the credit card data were stored in innocuously named files and sent to servers outside Target's system and then on to other servers, and
7. warnings about transmitting the data were ignored.[13]

JPMorgan Chase & Co. Breach

On October 2, 2014, JPMorgan Chase[14] reported to the Securities and Exchange Commission (SEC) that a cyberattack had compromised the PII of approximately 76 million households and 7 million small businesses. The compromised PII included names, addresses, phone numbers, email addresses, and "internal JPMorgan Chase information relating to such users."[15] According to the company's filing, there was no evidence that account information, user IDs, passwords, social security numbers, or birth dates for the affected customers were compromised.[16] The company said that it had not seen any unusual customer fraud related to the incident. It reassured customers that they would not be liable for any unauthorized activity on their accounts, if it were reported promptly.

[11] Nicole Perlroth, "Latest Sites of Breaches in Security Are Hotels," *New York Times*, January 31, 2014, p. B4, New York Edition, at http://www.nytimes.com/2014/02/01/technology/latest-sites-of-breaches-in-security-are-hotels.html.

[12] For a more detailed report on the Target breach, see U.S. Congress, Senate, Committee on Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach: Majority Staff Report for Chairman Rockefeller*, March 26, 2014, at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883.

[13] According to BloombergBusinessweek, Target security specialists in Bangalore detected the malware and reported the problem to Target's headquarters security, which did nothing. See Michael Riley, Ben Elgin, and Dune Lawrence, et al., "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," *BloombergBusinessweek*, March 13, 2014, at http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p1.

[14] This case study is intended to provide a detailed frame of reference for the subject matter in the memo. JPMorgan breach is one of several reported this year. Few of the other companies that reported cyber-attacks in 2014 are eBay, Google, Home Depot, Target, and UPS.

[15] JPMorgan Chase & Co., "Form 8-K," October 2, 2014, at https://www.documentcloud.org/documents/1308629-jpmorgan-on-cyberattack.html.

[16] Ibid., p. 2.

Prior to the October 2 filing, the firm's disclosure of the incident was general. In its regular report for the second quarter of 2014, JPMorgan Chase stated, "The Firm is also regularly targeted by unauthorized parties using malicious code and viruses, and has also experienced other attempts to breach the security of the Firm's systems and data which, in certain instances, have resulted in unauthorized access to customer account data."[17]

According to media reports, hackers gained access sometime in mid-June 2014 to JPMorgan servers storing contact information for current and former customers who had accessed the company's chase.com or jpmorgan.com websites or mobile applications in recent years.[18] According to media reports, the company learned of the data breach in mid-August and took steps to stop any unauthorized access at its servers.[19] On August 27, 2014, *Bloomberg* and *The Wall Street Journal* both reported that the Federal Bureau of Investigations (FBI) was investigating a possible computer hacking attack on JPMorgan and possibly other financial institutions.

The FBI later released a statement that it was "working with the United States Secret Service to determine the scope of recently reported cyberattacks against several American financial institutions."[20] On August 28, 2014, JPMorgan reiterated to customers that it was not seeing an "unusual fraud activity,"[21] in other words, it appears that the hackers have not used the information they obtained for fraudulent purposes. JPMorgan continued by stating that the hackers went to considerable effort, but were unable to monetize the information that they stole. Of course, it could be that they are simply waiting until a later date or that their monetization of the information has been undetected.

According to the *New York Times*, the same hackers—believed to be located overseas—who breached JPMorgan's network also infiltrated the website for the JPMorgan Corporate Challenge, run by an outside vendor for the bank on a server maintained by an outside Internet firm.[22] JPMorgan has not announced how hackers penetrated its network, but the bank said they did not gain access through the Corporate Challenge website.[23]

What Are the Cost Estimates of These Data Breaches?

This section looks at the costs reported by companies in three data breaches: Target, Home Depot, and JPMorgan. These costs typically include only direct costs, such as hiring consultants and staff

[17] JPMorgan Chase & Co., "Form 10-Q," June 30, 2014, p. 72, at https://www.documentcloud.org/documents/1311248-jpmorgan-on-hackers.html.

[18] Emily Glazer, "J.P. Morgan's Cyber Attack: How The Bank Responded," Dow Jones, October 3, 2014.

[19] Ibid.

[20] Ellen Nakashima and Andrea Peterson, "FBI probes hack into computers of JPMorgan Chase, other U.S. banks," Washington Post, August 27, 2014, available at http://www.washingtonpost.com/world/national-security/fbi-probes-hack-into-jpmorgan-chases-computers/2014/08/27/d42f992c-2e31-11e4-bb9b-997ae96fad33_story.html.

[21] Emily Glazer, "J.P. Morgan's Cyber Attack: How The Bank Responded," Dow Jones, October 3, 2014.

[22] Jessica Silver-Greenberg and Matthew Goldstein, "After JPMorgan Chase Breach, Push to Close Wall St. Security Gaps," New York Times DealBook, October 24, 2014, available at http://dealbook.nytimes.com/2014/10/21/after-jpmorgan-cyberattack-a-push-to-fortify-wall-street-banks/.

[23] Ibid.

to end the breach and to prevent future breaches, and contractually agreed compensation to business partners (such as payment card companies) for their losses. Not all companies include the savings from the tax deductibility of these costs or insurance claims. Many costs, especially those resulting from legal action against the companies, will not be known for many years after the data breach.

Target Cost Estimates

Target has reported that as of its quarter that ended November 1, 2014, it had cumulatively incurred $248 million in data breach related expenses and received (or expected to receive) $90 million from insurance policies.[24] This includes the cost of investigating the breach, providing credit-monitoring services, increasing call center staffing, other professional services, and "an accrual related to the expected payment card networks' counterfeit fraud losses and non-ordinary course operating expenses."[25] These costs include allowances for defending and/or settling more than 100 legal actions filed against Target. In addition, the payment networks have made claims for reimbursement for incremental expenses, such as counterfeit fraud losses and card reissuance.[26]

Jefferies, an investment bank, quotes an industry expert, Julie Conroy, who estimates that 4.8-7.2 million cards will be used to charge $1.4-$2.2 billion fraudulently.[27] Ms. Conroy said that card issuers are liable for the fraud except when the card is not present at the time of the purchase (e.g., telephone and online purchases).[28] Ms. Conroy is quoted by Jefferies as estimating that the Payment Cards Industry (PCI) Council, founded in 2006 by the main payment card companies (i.e., Visa, MasterCard, American Express, Discover, and JCB) to establish industry security standards, could fine Target between $400 million and $1.1 billion.

According to Jefferies, Ms. Conroy said that, in general, the largest payment card issuers are better at fraud detection than the other issuers. She estimated that 10%-15% of the cards issued by the financial institutions with the most sophisticated detection systems would have fraudulent charges, whereas 20%-30% of the cards issued by other financial institutions would have fraudulent charges.

Others have made lower forecasts of the volume of fraudulent transactions that will occur in the Target case. For example, Ellen Richey, chief enterprise risk officer of Visa, testified that 2%-5% of compromised Visa cards experience fraud.[29] Using the same $300 of fraud per card that Ms. Conroy used, fraudulent charges could be $240-$600 million.

---

[24] Target, "Form 10-K," November 21, 2014, at http://www.sec.gov/Archives/edgar/data/27419/000002741914000028/tgt-20140802x10xq.htm.

[25] Ibid., p. 17.

[26] Target has not identified the amount of these claims or the amount it has budgeted for these claims.

[27] Daniel Binder, "Jefferies Equity Research, Americas: Target," January 29, 2014. Jefferies credits the estimates to conversations with Julie Conroy of Aite Group, a payment cards industry expert.

[28] When the card is not present, the acquiring bank is responsible, but can seek to recovery from the merchant. See Randall Stross, "$9 Here, 20 Cents There and a Credit-Card Lawsuit," *New York Times*, August 22, 2010, p. BU3, New York edition, at http://www.nytimes.com/2010/08/22/business/22digi.html?_r=1&src=me&ref=business.

[29] Testimony of Ellen Richey, Chief Enterprise Risk Officer, Visa, Inc. before U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *Hearing on Protecting Personal Consumer Information from Cyber Attacks and Data Breaches*, 113th Cong., 2nd sess., March 26, 2014, p. 12, at http://www.commerce.senate.gov/public/?a=

(continued...)

To provide some context, Target has reported 2013 net income of $3.0 billion and stockholders' equity of $16.6 billion for the fiscal year ending February 1, 2014.[30] If Target's cost of the data breach were to be a $1.1 billion PCI fine that would be 37% of their 2013 net income and 7% of 2013 stockholder's equity. In contrast, combining Ms. Conroy's assumption that PCI fines could be 30%-50% of fraudulent charges with Visa's low-end estimate of 2% of cards being used fraudulently, the estimated PCI fine would be $72 million, which is 2% of 2013 net income and less than 1% of 2013 stockholders' equity.

Home Depot Cost Estimates

On September 18, 2013, Home Depot reported it had been notified by banks and law enforcement of unusual payment system activity, and on November 6, 2013, it announced that approximately 53 million customer email addresses had been compromised.[31] It was later announced that 56 million payment cards had been compromised.

Home Depot reports that at least 44 legal actions in the United States and Canada had been filed against it as a result of the data breach. As of the third quarter of 2014, Home Depot reported $43 million in data breach-related expenses and anticipated $15 million in insurance payments.[32] Home Depot reported $5.4 billion in net earnings for the fiscal year ending February 2, 2014.

Brian Krebs, a computer security research and blogger, has attributed the Home Depot data breach to the same malware used against Target.[33]

How Does the Payment Card System Work?

The payment card system encompasses cards that can be used as payment for purchases. Credit cards, debit cards, automatic teller machine (ATM) cards, and prepaid cards are the most widely used payment cards. The two basic approaches to payment card systems differ in the number of parties to the transaction. The most common is the four-party system, which is used by MasterCard and Visa. This system involves a *merchant*, an *acquirer* (the merchant's bank), the *issuer* (the customer's bank), and the *cardholder*.[34] The alternative called the three-party system—used by companies such as Diners Club, Discover, and American Express—consists of the merchant, the payment card company, and the cardholder.

(...continued)

Files.Serve&File_id=9d2d04c0-0aa2-4a07-9a11-81d74a7339a8.

[30] Target, "Form 8-K," February 26, 2014, at http://edgar.sec.gov/Archives/edgar/data/27419/000002741914000006/a2013q48k.htm.

[31] Home Depot, "The Home Depot Reports Findings in Payment Data Breach Investigation," news release, November 6, 2014, available at http://ir.homedepot.com/phoenix.zhtml?c=63646&p=irol-newsArticle&ID=1987135.

[32] Home Depot did not report any data breach expenses in its 2013 10-K.

[33] Brian Krebs, "Home Depot Hit by Same Malware as Target," September 7, 2014, at http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/.

[34] The term "four-party" is a bit misleading because it does not count the payment network (also called the network provider), e.g., the credit or debit card company.

Four-Party Transactions

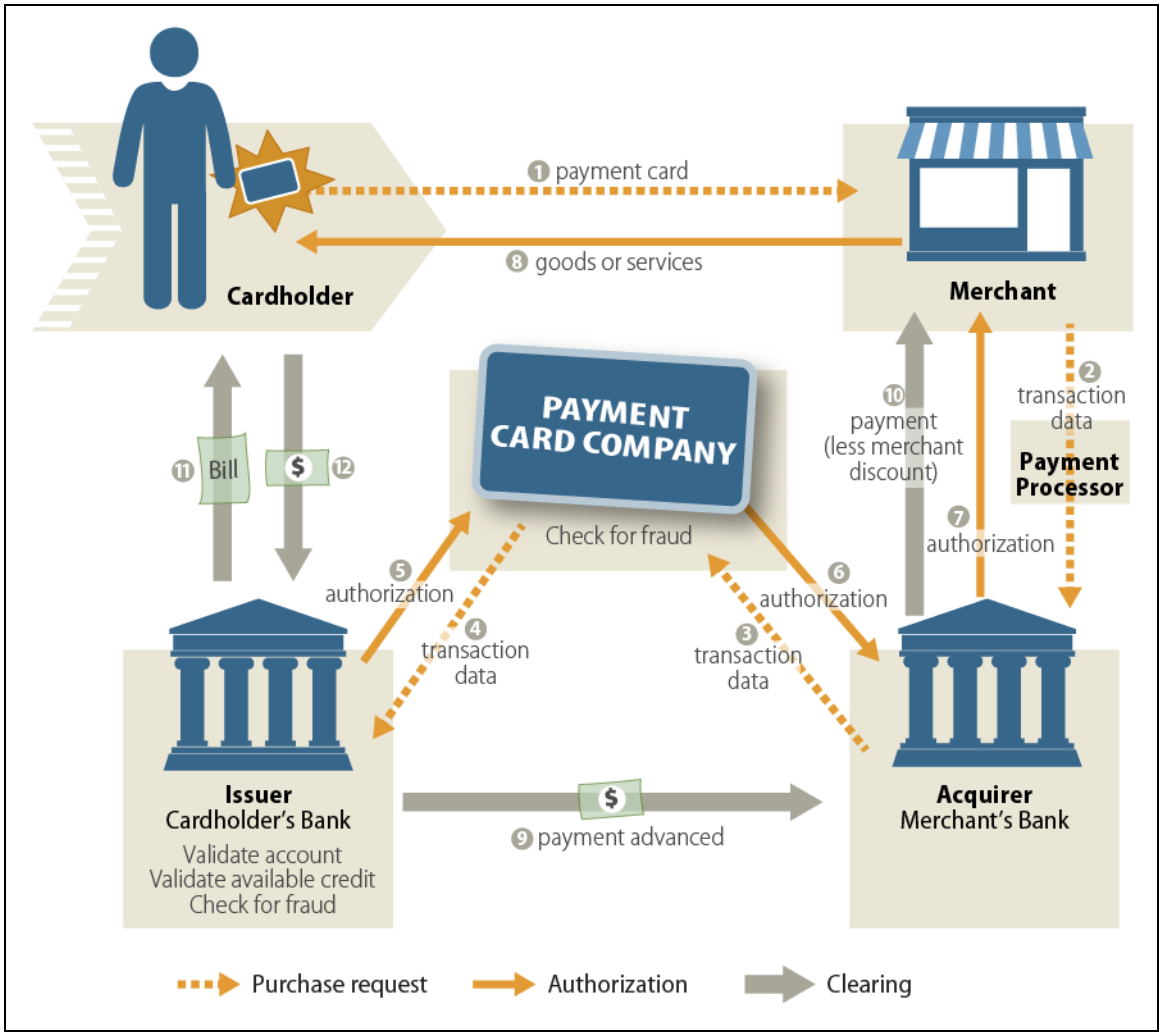
Figure 1 illustrates a typical purchase using the four-party system.

1. A *cardholder* presents a payment card to a retailer to pay for merchandise. The card is "swiped" and information about the card and the purchases is sent to the retailer's computers in a secured room.
2. This transaction is transmitted to the *acquirer* (i.e., the retailer's bank).
3. The acquirer relays the transaction information to the *payment card company*, which may conduct an anti-fraud analysis.
4. The payment card sends this information to the *issuer*, the bank that issued the payment card. The issuer verifies that the account is valid, that the cardholder has available credit, and it may perform additional anti-fraud analysis.
5. The issuer notifies the payment card company of its decision to authorize (or not to authorize) the transaction.
6. The payment card company notifies the acquirer of the issuer's authorization decision.
7. The acquirer notifies the merchant of the issuer's authorization decision.
8. The cardholder leaves with their purchases.
9. The issuing financial institution (bank, credit union, etc.) pays the acquirer and posts the amount of the purchase to the cardholder's account. The acquirer receives the amount minus an interchange fee charged by the payment network.
10. The acquirer deducts a fee[35] and credits the merchant with the balance.
11. The cardholder receives a monthly bill.
12. The cardholder makes a payment on the monthly bill.

Both the interchange fees and the merchant discounts depend on a number of factors related to risk and cost. Was the card physically present or was the transaction done by telephone or Internet? Was the receipt signed or was a PIN used? What business is the merchant in? What has been the card network's experience with the merchant? Is the customer in a foreign country? Do the funds have to be converted to another currency? Is the card a credit card, a debit card, or a prepaid card? Is the card a standard, premium, or affluent card? Is the cardholder an individual or a business?

[35] This fee is called the merchant discount fee.

Figure 1. Four-Party Payment Card Transaction



Source: CRS based on MasterCard 2013 Annual Report and Visa 2013 Annual Report.

Note: The "Payment Card" is also called the "network provider," especially in the case of ATM and debit card transactions.

Three-Party Transactions

In the three-party system, the merchant sends the transaction information directly to the payment card company, which sends the funds to the merchant (less fees) and lends the cardholder the funds for the purchase.

In 2013, four-party payment cards (Visa and MasterCard) dominated the payments system. In 2013, as measured in dollars, Visa's share was 56% and MasterCard's was 26%.[36] American Express's share in 2013 was 15% and Discover's was 3%.

[36] "Purchase Volume for U.S. General Purpose Brands," *Nilson Report*, February 2014.

Many merchants contract with outside payment processors to manage the payment process between the POS and the acquirer (four-party system) or the payment card (three-party system). The payment processors are approved by PCI. Payment processors include large international banks, such as JPMorgan Chase; financial services companies, such as Heartland Payments and First Data; technology startups, such as SquaredUp; and established technology firms, such as Google and Yahoo.

In theory, credit card security can be compromised anywhere in the system: at the point of sale, transmission of the information, at either of the banks, or at the payment card company. An attacker can come directly from the outside, or it can infiltrate an authorized user to obtain access.

Why Do Financial Data Breaches, Especially in the Retail Industry, Keep Happening?

There are economic, technological, and strategic reasons why payment card breaches continue to occur. The crime can be profitable and those involved are thought to have relatively little risk of arrest. For a group with an inclination toward crime, using the Internet to steal financial data would appear to offer large rewards, little cost, and relatively little risk of arrest.

Obtaining cardholder information has been profitable, and obtaining the information on thousands or millions of cardholders has been even more profitable. Although law enforcement authorities try to identify, arrest, and prosecute those responsible, international cooperation can be less than what might be desired, which reduces the risks to those responsible for the breaches.

Merchants, banks, and payment cards share costs and benefits, but the desire to minimize costs, including the cost of a new technology to deter payment card breaches, may involve shifting the expense to someone else. Cyber technology and business efficiencies for merchants, banks, payment cards, payment processors, and cybercriminals are constantly evolving.

Magnetic Stripe versus Chip Systems

The incentives to improve cybersecurity are divided along the transaction path of merchant, acquirer (the merchant's bank), payment card company, issuing bank, and cardholder. In the aftermath of the Target case, some merchants have complained that the current magnetic stripe and signature system should be replaced with a Chip and PIN system, which would use the EMV computer chip—named after EuroPay, MasterCard and Visa, which developed it—to encrypt payment information.[37] It presents a coordination problem: until the entire payment system—businesses accepting payment cards, issuing banks, acquiring banks, and the payment card companies—adopts CHIP and PIN or CHIP and Signature, there are the costs to those that adopt the heightened security, but no benefits. An additional concern is that some customers, perhaps

[37] For contrasting views, see Testimony of Mallory Duncan, General Council, National Retail Federation, before U.S. Congress, Senate Committee on Banking, Housing, and Urban Affairs, Subcommittee on National Security and International Trade and Finance, *Safeguarding Consumers' Financial Data*, 113th Cong., 2nd sess., February 3, 2014; and Clint Boulton, "Retail Association: Card Security Costs Outweigh Benefits for Many," *Wall Street Journal: CIO Journal*, March 26, 2014, at http://blogs.wsj.com/cio/2014/03/26/retail-association-card-security-costs-outweigh-benefits-for-many/.

from other countries, may have cards without a CHIP so businesses want a fall-back mechanism even after they have adopted CHIP reading terminals.

The payment card industry has announced that effective October 1, 2015, liability for fraudulent transactions (except for ATMs and gas stations) will be assigned to the merchant or issuer that is not Chip and Signature compliant.

For a number of years, payment card companies have argued that Chip and Signature was unnecessary in the United States because POS terminals[38] are connected to the payment system allowing for immediate (real-time) approval. One advantage of Chip and Signature/PIN is that it can be used to approve purchases even if no computer connection is available to the issuing bank and payment card company.[39]

Another advantage is that Chip-based systems are supposed to make it more difficult for unauthorized persons to duplicate payment cards compared with the cards used in the United States presently.

Some banks in the United States have begun issuing Chip and Signature cards to certain customers.[40] According to a multi-industry trade group, the Smart Card Alliance, Chip and Signature cards are currently issued by 17 financial institutions, including some of the largest volume issuers.[41] Outside of the United States, more than 75% of terminals and 45% of payment cards use an EMV chip.[42]

In short, chip-based cards could reduce the cost of fraud because they are more difficult (but not impossible) to forge, but they do not prevent the theft of account information. On the other hand, fraud involving Internet, telephone, and mail orders does not require a payment card to be present. Compared with signature-based authentication, PINs make it harder (but not impossible) to use a stolen card.

What Industry Best Practices Have Been Adopted?

The current payment card system in the United States is based on payment cards that have magnetic stripes on the back that contain the account number, cardholder name, service code, expiration date, and other information in an unencrypted format.[43] This unencrypted information

[38] A POS system includes a cash register, payment card terminal, and related computer hardware and software. More sophisticated systems can monitor inventory and produce various business reports.

[39] David Morrison, "Visa Emphasizing that New Cards Will Not Need Offline PINs," *Credit Union Times*, January 16, 2012, at http://www.cutimes.com/2012/01/16/visa-emphasizing-that-new-cards-will-not-need-offl. It is not clear how chip-based systems without payment network access can be kept up-to-date for credit limit availability.

[40] MasterCard, "Progress against Roadmap," June 20, 2013, at http://www.mastercard.us/_assets/docs/MasterCard_EMV_Timeline.pdf.

[41] EMV Connection, "U.S. EMV Issuers," at http://www.emv-connection.com/u-s-emv-issuers/. Issuers listed are AAA Visa, American Express, Andrews Federal Credit Union, Bank of America, Diners Club Chase, Citi, North Carolina State Employees' Credit Union, PSCU Financial Services, Silicon Valley Bank, Star One Credit Union, State Employees Credit Union, SunTrust, Travelex Cash Passport, United Nations Federal Credit Union, U.S. Bank, and Wells Fargo.

[42] EMV, "Worldwide EMV Deployment and Adoption," Q4 2012, at http://www.emvco.com/documents/EMVCo_EMV_Deployment_Stats1.pdf.

[43] PCI Security Standards Council, "PCI Data Storage Do's and Don'ts," October, 2008, at
(continued...)

is necessarily read into the merchant's payment processing system unencrypted and potentially vulnerable for a fraction of a second. A secure card reader encrypts the data before sending it to the merchant's server for transmission to the acquiring bank, but it is theoretically possible to intercept the information inside the card reader before it has been encrypted.

Current PCI standards require encryption only when cardholder data are transmitted over public networks such as the Internet and when they are stored.[44] The magnetic stripe and signature card suffers from a number of weaknesses:

- Card information on the magnetic stripe is not encrypted and can easily be read.
- It reportedly is easy to forge magnetic stripe cards.[45]
- The signature on the back of a card provides a criminal with an example of the authentic signature, electronic signature pads can be difficult to sign in a manner that resembles the signature on the card, and the payment cards do not allow merchants to decline a transaction based on the signature of additional identity information, such as a driver's license.[46]

A strength of the magnetic stripe and signature system used in the United States is that authorization is largely done online and in real time. If a card is known to be stolen or forged, purchases will not be authorized.

Although the magnetic stripe and signature system is the standard in the United States, in most of the rest of the world, a system thought to be more secure, the Chip and PIN system, has been adopted. Arguably, the system used in the United States is not the best practice, but for some the cost of converting has outweighed the expected cost of the fraud.[47]

The Chip (also known as an EMV card after Europay, MasterCard, and Visa, which developed the standard) transmits the card information using encryption. The Chip, actually a small computer, can change the encryption every time it is used, making it nearly impossible for a criminal to capture and use cardholder information as it is transmitted and processed through the system.

Many Chip and PIN (or Chip and Signature) cards provide compatibility with magnetic stripe systems by adding a magnetic stripe, which potentially weakens their security. Chip and PIN is not foolproof; British researchers have demonstrated that there are a number of ways to bypass

---

(...continued)

https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf. The service code specifies acceptance requirements and limitations on the card.

[44] PCI Security Standards Council, "Data Security Standard: Requirements and Security Assessment Procedures," Version 3.0, November 2013, p. 5, at https://www.pcisecuritystandards.org/security_standards/documents.php.

[45] Lisa Eadiccio and James Fanelli, "Not Much to Forging a Counterfeit Credit Card, Technology is Readily Available," *Daily News*, February 3, 2011, at http://www.nydailynews.com/news/forging-counterfeit-credit-card-technology-readily-article-1.133144?print.

[46] Testimony of Mallory Duncan, General Council, National Retail Federation, before U.S. Congress, Senate, Committee on Banking, Housing, and Urban Affairs, Subcommittee on National Security and International Trade and Finance, *Safeguarding Consumers' Financial Data*, 113th Cong., 2nd sess., February 3, 2014.

[47] For example, Clint Boulton, "Retail Association: Card Security Costs Outweigh Benefits for Many," *Wall Street Journal: CIO Journal*, March 26, 2014, at http://blogs.wsj.com/cio/2014/03/26/retail-association-card-security-costs-outweigh-benefits-for-many/.

the security features of Chip and PIN cards.[48] One response to Chip-based security has been to use cards stolen or forged in countries that do not use Chip.

According to congressional testimony,[49] Chip and Signature increases security in two ways: (1) the information is encrypted and (2) it is more difficult to duplicate the Chip card. PIN adds another security factor that is called two-factor authentication.

The payment card companies have announced that effective October 1, 2015, a merchant or issuer who does not support Chip and Signature will be liable for most counterfeit card transactions.[50] For gas stations and ATMs the shift is scheduled to occur October 1, 2017.

According to Chris McWilton, MasterCard's president of North America, the argument in favor of using a signature instead of a PIN like that on debit and ATM cards is that a signature is easier than a PIN for customers.[51] He has also noted that banks will decide if it is worth their time to convert their systems to use a PIN and to issue PINs to customers.

According to Al Vrancart, a payment card consultant, the cost of producing a magnetic stripe card is about $0.50 compared with $2.20 to produce a chip card.[52] New POS terminals could cost $300-$600 each. Mallory Duncan, general counsel of the National Retail Federation, has testified that new POS terminals cost "an average of $1,000 or more per unit,"[53] but this estimate appears to include the cost of modifying the system and training employees.[54]

Other Emerging Technology Solutions

A number of technology solutions are emerging. *Tokenization* is a solution in which transaction information is stored on extremely secure servers known as vaults.[55] Each transaction is indexed

[48] Mike Bond, Omar Choudary, and Steven J. Murdoch, et al., *Chip and Skim: Cloning EMV Cards with the Pre-Play Attack*, Computer Laboratory, University of Cambridge, UK, at http://www.cl.cam.ac.uk/~rja14/Papers/unattack.pdf. See, also, Mike Bond, "Chip and Skim: Cloning EMV Cards with the Pre-Play Attack," *Light Blue Touchpaper*, September 10, 2012, at http://www.lightbluetouchpaper.org/2012/09/10/chip-and-skim-cloning-emv-cards-with-the-pre-play-attack/, and Steven J. Murdoch and Ross Anderson, "Security Protocols and Evidence: Where Many Payment Systems Fail," Financial Cryptography and Data Security 2014, March 2014, at http://www.cl.cam.ac.uk/~sjm217/papers/fc14evidence.pdf.

[49] Testimony of Fran Rosch, Senior Vice President Security Product and Services, Endpoint and Mobility, Symantec Corporation, before U.S. Congress, Senate Committee on the Judiciary, *Hearing on Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime*, 113th Cong., 2nd sess., February 4, 2014.

[50] Visa, *Visa U.S. Merchant EMV Chip Acceptance Readiness Guide*, June 2013, p. 4, at http://usa.visa.com/download/merchants/visa-merchant-chip-acceptance-readiness-guide.pdf.

[51] Danielle Douglas, "MasterCard, Visa Explain Why Your Credit Card Isn't Safer," *Washington Post*, February 20, 2014, at http://www.washingtonpost.com/blogs/wonkblog/wp/2014/02/20/mastercard-visa-explain-why-your-credit-card-isnt-safer/.

[52] Dune Lawrence, "Hack-Resistant Credit Cards Bring More Safety—at a Price," *BloombergBusinessweek*, February 14, 2014, at http://www.businessweek.com/articles/2014-02-14/hack-resistant-credit-cards-bring-greater-security-at-a-big-price.

[53] Testimony of Mallory Duncan, General Council, National Retail Federation, before U.S. Congress, Senate Committee on Banking, Housing, and Urban Affairs, Subcommittee on National Security and International Trade and Finance, *Safeguarding Consumers' Financial Data*, 113th Cong., 2nd sess., February 3, 2014.

[54] A web search found many vendors (including Amazon.com) selling POS payment cardreaders for approximately $300.

[55] First Data, *Avoiding a Data Breach: An Introduction to Encryption and Tokenization*, 2013, at
(continued...)

by a token that is used to access it. This token is essentially a random number and designed so that outsiders cannot take a payment card or transaction and create the token. The token cannot be used as a credit card number, and it cannot be used by anyone but the merchant in the transaction. This places great reliance on the security of the vault and the tokenization process. It may make it more cumbersome for merchants to analyze customer records to send targeted messages about new products or sales. Presumably the gains from the vault and tokenization process will outweigh the potential losses if the process is compromised.

With *encryption*, transaction information is transformed from plain text into an unintelligible format called cipher text.[56] Secret keys are required for encrypting and decrypting the information. Most Internet transactions use session encryption known as https (hypertext transfer protocol secure) instead of the unencrypted http (hypertext transfer protocol). The actual transaction information can be separately encrypted instead of or in addition to using https. Separate data encryption is used when storing the information in a database.

Mobile payments and *mobile banking*[57] are evolving alternatives in which mobile phones and tablets replace payment cards in financial transactions. The mobile device could be the customer's or the merchant could use a mobile device to process the customer's credit card. This raises questions about the security of the system: if a mobile device is stolen, can the owner's financial information be obtained and decrypted? If the customer is using an account with the merchant, how secure is the implementation? Is the transmission between the customer and the merchant secure? What are the security issues for various transmission technologies such as Bluetooth and near field communications (NFC), both of which allow the transaction to be completed without physical contact between the mobile device and the POS terminal? If the merchant is using a mobile device, what are its security strengths and weaknesses?

How Big Are Credit Card Data Breach Losses?

Many types of costs affect merchants, banks, payment cards, payment processors, consumers, and the party whose information is compromised. The response of those affected has an impact on the cost per record and the total cost. In 2007, Forrester Research surveyed 28 companies and estimated data breach costs of $90 to $305 per record.[58] If this estimate is accurate for the Target

(...continued)

http://files.firstdata.com/downloads/thought-leadership/6203-Data-Breach-Market-Insight.pdf and First Data, *What Data Thieves Don't Want You to Know: The Facts about Encryption and Tokenization. A First Data White Paper*, 2012, at http://files.firstdata.com/downloads/thought-leadership/TokenizationEncryptionWP.pdf.

[56] First Data, *Avoiding a Data Breach: An Introduction to Encryption and Tokenization*, 2013, at http://files.firstdata.com/downloads/thought-leadership/6203-Data-Breach-Market-Insight.pdf and First Data, *What Data Thieves Don't Want You to Know: The Facts about Encryption and Tokenization. A First Data White Paper*, 2012, at http://files.firstdata.com/downloads/thought-leadership/TokenizationEncryptionWP.pdf.

[57] The Federal Reserve has defined mobile banking as "accessing your bank's web page through the web browser on your mobile phone, via text messaging, or by using an application downloaded to your mobile phone." See Board of Governors of the Federal Reserve System, "Consumers and Mobile Financial Services 2013," March 2013, p. 15, at http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201303.pdf. The report defines mobile payments similarly and includes payments made by telephone bill, credit card bill, or directly from a bank account. The definition could be expanded to include tablets.

[58] Sharon Guadin, "Security Breaches Cost $90 to $305 Per Lost Record," *InformationWeek*, March 3, 2007, at http://www.informationweek.com/security-breaches-cost-$90-to-$305-per-lost-record/d/d-id/1053922?.

case, the cost to Target's 40 million cards compromised could result in costs of $3.6 billion to $12.2 billion.

According to research by the Ponemon Institute,[59] factors influencing the losses in data breaches include industry, existence of a privacy and data protection security policy, the type of information handled, the most likely cause of a data breach, whether data are stored on laptops or removable devices, whether data are encrypted, whether there is a full-time information security manager, number of employees, where in the world the company operates, policies concerning remote access to sensitive data, user authentication technology, headquarters location, and the number of sensitive records.

Table 1 summarizes various estimates of the cost to Target its data breach. These estimates range from $4.9 billion down to Target's reported losses of $11 million after insurance and taxes.

Ponemon estimated that a 2013 data breach in the retail sector would cost an average of $122 per record as compared with an average of $254 per card in the financial sector, and $304 in the health care sector.[60] Costs included hiring outside experts, hiring a call center, the cost of cardholder credit monitoring, providing discounts to cardholders, reduced sales, and the cost of the staff response. If Target's cost turns out to be $122 per record, the total cost of the Target breach would be $4.9 billion. To date, Target has reported losses after insurance and taxes of $11 million.

[59] Symantec and Ponemon Institute, "Databreach Calculator: Estimate Your Risk Exposure," at https://databreachcalculator.com/Calculator/Default.aspx.

[60] Ponemon Institute, "2013 Cost of Data Breach Study: United States," p. 6, at http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-us-report-2013.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Jun_worldwide_CostofaDataBreach. The Ponemon Institute's estimates are based on a non-random sample of 54 companies and include all breaches, not just those targeting payment cards.

Table 1. Summary of Loss Estimates for Target Credit Card Data Breach

Loss Estimates			
Total per Incident	**Per Card**	**Source**	**Comments**
$4.9 billion	$122	Ponemon (2013)	Estimate based on 40 million cards at general retail cost of $122/card
$1.4-$2.2 billion fraud	$35-$55 fraud	Jefferies (2014)	Target, limited costs considered
	$10-$28 PCI fines		
$400 million-$1.1 billion PCI fines			40 million cards
$240-$600 million	$6-$10	Visa/Jefferies (2014)	Replace fraud rates used by Jefferies with Visa's fraud rates
			40 million cards
$61 million gross	$1.10	Target (2013)	Reported for fourth quarter 2013 only
$17 million after insurance	$0.28		40 million cards
$11 million after insurance and taxes			Total costs not yet known

Sources: Ponemon Institute, "2013 Cost of Data Breach Study: United States," p. 6, at http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-us-report-2013.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Jun_worldwide_CostofaDataBreach; Daniel Binder, "Jefferies Equity Research, Americas: Target," January 29, 2014; Testimony of Ellen Richey, Chief Enterprise Risk Officer, Visa, Inc. before U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *Hearing on Protecting Personal Consumer Information from Cyber Attacks and Data Breaches*, 113th Cong., 2nd sess., March 26, 2014, p. 12, at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=9d2d04c0-0aa2-4a07-9a11-81d74a7339a8; Target Corporation, "Form 10-K," Fiscal Year Ended February 2, 2013, p. 17, at http://edgar.sec.gov/Archives/edgar/data/27419/000104746913003100/a2213506z10-k.htm#da18701_part_i; and Global Payments, "Form 10-K for the Fiscal Year Ended May 31, 2013," p. 62, at http://www.sec.gov/Archives/edgar/data/1123360/000112336013000025/gpn20130531-10k.htm.

This section of the report continues by looking at who bears the various costs of the payment breach in the first instance. It looks at the costs unique to merchants, banks, the payment processor, and consumers. It also examines the costs to the party breached. Ultimately private contracts among the various parties in the payment system and lawsuits can reallocate these costs.

The cost of reversing fraudulent transactions follows the entire chain of processing a payment card transaction, but—assuming that the funds can be recovered—this cost is likely to be relatively small.

Costs Unique to Merchants

In the case of payment card fraud, the issuing bank may issue a *chargeback* and retrieve the funds paid to the merchant who is unlikely to be able to retrieve the merchandise. Chargebacks can affect both the merchant breached and other merchants.

Sales may decline if customers lose confidence in the merchant and shop less frequently or purchase less when they shop. Target reported that its fourth quarter 2014 U.S. sales decreased 2.5% and were "meaningfully softer following the announcement" of the data breach.[61] Among competing retailers not reporting recent data breaches, Walmart's comparable sales declined 0.4% in their fourth quarter 2014,[62] and Costco's comparable U.S. sales increased 4% in the 18 weeks ending January 5, 2014.[63]

Academic research in general finds that payment breaches have little long-lasting impact on a company's *stock price*, and this appears to be true for Target. Between December 18, 2013 (the day before the breach's public announcement), and March 3, 2014 (the first trading day in March 2014), Target's stock declined 0.3%, but Costco's stock declined 2.3% and Walmart's stock declined 4.9%.

Costs Unique to Card Issuers

One cost to issuers is the cost of issuing *replacement cards*. In the recent Target case, a figure of $10 per card issued has been widely used.[64] This estimate appears to include the cost of obtaining new blank cards, embossing the cards, modifying accounts with the new account numbers, notifying cardholders, delivering the cards, and using a call center to answer questions related to the cancellation of the old cards and the issuance of the new ones.

Card issuers face the decision of which cards should be replaced. There may be a difference between the cards potentially compromised and those actually compromised. Not all cards actually compromised will be used in fraudulent transactions. Issuers that are better at detecting and preventing fraudulent charges may choose to replace fewer cards than other issuers.

Costs Unique to Payment Processors

Some merchants contract out payment processing to third-party contractors that connect a merchant with the acquiring financial institution. Services offered by payment processors range from handling the entire credit card process from POS to payment to the merchant's account and accounting to assessments of a merchant's compliance with PCI standards. Small merchants use payment processors because they do not have the need for a full-time staff of computer security specialists, and large merchants use them as a form of outsourcing for greater efficiency or to concentrate on the basic business.

Payment processors can be the victims of payment card data breaches. For example, in March 2012, Global Payments, a merchant payment processor, reported a data breach. "Certain" card

[61] Target, "Target Reports Fourth Quarter and Full-Year 2013 Earnings," press release, February 26, 2014, at http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1903678&highlight=.

[62] Walmart, "Walmart reports Q4 underlying EPS of $1.60, Fiscal 2014 underlying EPS of $5.11," press release, at http://media.corporate-ir.net/media_files/IROL/11/112761/FY14Q4EarningsReleasefinal.pdf.

[63] Costco Wholesale Corporation, "Costco Wholesale Corporation Reports December Sales Results," press release, January 5, 2014, at http://phx.corporate-ir.net/phoenix.zhtml?c=83830&p=irol-newsArticle&ID=1889295&highlight=.

[64] See for example, Independent Community Bankers of America, "Community Banks Reissue More Than 4 Million Payment Cards Following Retailer Data Breaches," press release, February 19, 2014, at http://www.icba.org/news/newsreleasedetail.cfm?itemnumber=178594&pf=1.

networks temporarily suspended Global Payments as an authorized provider.[65] Global Payments reported that as of May 31, 2013, its costs (before insurance payments) were $156.9 million consisting of $121.2 million for professional fees for investigation and remediation, incentive fees to business partners, credit monitoring, and identity protection, and an additional $35.7 million in fraud losses, fines and charges imposed by the card networks. Insurance covered $20.0 million. A class action lawsuit filed against Global Payments was dismissed.

According to media reports,[66] about 1.5 million payment cards were affected, making the cost per card $104.

Costs Unique to Payment Cards

The four-party payment card companies (e.g., MasterCard and Visa) appear to largely avoid financial responsibility for data breaches and payment card fraud. In three-party payment systems, card companies (e.g., Diners Club, Discover, and American Express) bear credit risk from lending a cardholder the funds to pay the merchant. In the four-party system, the issuing bank, not the payment card company, bears the credit risk. Thus, the issuing bank, not the payment card company, in a four-party payment system, has potential exposure to the costs of payment card fraud. In the three-party network, the payment card company re-issues compromised cards, but in the four-party system it is the issuer's responsibility.

An examination of MasterCard's and Visa's annual reports found no explicit mention of expenses incurred because of fraud and data breaches. In contrast, American Express, Global Payments, and Heartland all mentioned these expenses.

Costs Unique to Consumers

Many costs to consumers can be difficult to value, but some are precisely known. Legally, the maximum cost to a consumer of a stolen credit card is $50.[67] By law, the maximum cost to a consumer of a stolen debit card varies depending on how quickly the consumer notifies the card issuer: $50 if the issuer is notified within two business days discovering the loss or $500 if the notification is made more than two days after discovery and less than 60 days after receiving a statement. In practice, the payment card issuers do not charge a cardholder for fraudulent transactions. The breached organization frequently absorbs all of the fraudulent charges and provides free credit monitoring; consumers are to identify the fraudulent transactions and notify the card issuer. Consumers may also be subject to increased identity theft risks. Additional consumer costs include the loss of privacy, the time to monitor card use more closely, and the inconvenience of getting new cards.

[65] Global Payments, "Form 10-K for the Fiscal Year Ended May 31, 2013," p. 62, at http://www.sec.gov/Archives/edgar/data/1123360/000112336013000025/gpn20130531-10k.htm. Visa has been publicly identified as one of the cards that suspended Global Payments. See Jessica Silver-Greenberg, "After a Data Breach, Visa Removes a Service Provider," *New York Times*, April 2, 2012, p. B6, New York edition, at http://www.nytimes.com/2012/04/02/business/after-data-breach-visa-removes-a-service-provider.html?_r=1&emc=tnt&tntemail0=y.

[66] Tracy Kitten, "Global Closes Breach Investigation: Processor Says Expenses Less than Originally Reported," *Bank Info Security*, April 15, 2013, at http://www.bankinfosecurity.com/global-closes-breach-investigation-a-5684/op-1.

[67] Federal Trade Commission, "Lost or Stolen Credit, ATM, and Debit Cards," at http://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards.

Costs Incurred by the Party Breached

The cost to the entity breached can include lost sales, a damaged reputation, forensic examination, hiring outside experts, notifying cardholders, creating or expanding call centers to answer cardholders questions, offering cardholders credit or identity monitoring, additional compensation to customers, hiring an external public relations firm for damage control, legal expenses, increased regulatory oversight, fines by regulators or industry groups, diversion of staff to dealing with the breach, and enhanced security.

Who Ultimately Bears the Losses?

In data breaches such as Target's, who is liable for the costs associated with such data breaches depends on a web of individual contracts among retailers, the banks that issue cards and handle payments, credit card companies such as Visa and MasterCard, payment processors authorized by the credit card companies to process payments at the point of sale, and even contracts between a retailer and its third-party service provider (such as Target's HVAC contractor).[68] These contracts allocate liability, the right to indemnification for breaches, and set certain duties and standards for cybersecurity protections, such as in the individually negotiated "representations and warranties" sections of such contracts.

Generally, the issuing financial institution pays the cost of card reissuance and for fraudulent charges made on compromised cards. Banks may sue the retailer for employing inadequate data security systems. A number of smaller financial institutions have filed class action lawsuits against Target under Minnesota state law, which reportedly has strict standards on data breach notification and minimum cybersecurity standards.[69] (Target is headquartered in Minnesota.) The financial institutions claim damages, among other things, for costs associated with notifying customers of issues related to the Target data breach, closing out and opening new customer accounts, reissuing cards, and refunding customer losses resulting from unauthorized charges.[70]

In some past data breach cases, merchants accused of using lax systems have paid significant costs of their own. For example, a data breach at T.J. Maxx was discovered in late 2006 and involved about 45 million debit and credit cards. To cover the eventual expenses of the breach, T.J. Maxx set aside $5 million in FY2007[71] and $198 million in FY2008, for a total of $203

[68] For more on this, see Ryan Tracy, "In a Cyber Breach, Who Pays, Banks or Retailers?; The Theft of Personal and Card Data at Target Has Rekindled Debate," *Wall Street Journal*, January 12, 2014, at http://online.wsj.com/news/articles/SB10001424052702303819704579316861842957106 and Tom Webb, "Analysts See Target Breach Costs Topping $1 Billion," *St. Paul Pioneer Press*, February 21, 2014, at http://www.twincities.com/business/ci_25029900/analyst-sees-target-data-breach-costs-topping-1.

[69] See First Choice Federal Credit Union v. Target, U.S. District Court for the Western District of Pennsylvania, Complaint filed January 31, 2014. For an overview, see Joel Schectman, "Banks Heap Suits on Target over Breach," *Wall Street Journal*, February 7, 2014, at http://blogs.wsj.com/riskandcompliance/2014/02/07/banks-heap-suits-on-target-over-data-breach/.

[70] First Choice Federal Credit Union v. Target, U.S. District Court for the Western District of Pennsylvania, Complaint filed January 31, 2014, p. 2.

[71] Most retailers use a fiscal year instead of a calendar year. T.J Maxx's FY2008 ended on January 26, 2008 and its FY2007 ended January 27, 2007. T.J. Maxx, "Form 10-K," March 31, 2009, p. F-32 at http://edgar.sec.gov/Archives/edgar/data/109198/000095013509002399/0000950135-09-002399-index.htm.

million. By way of comparison, T.J. Maxx's profit was $1.4 billion in FY2007 and $1.6 billion in FY2008.

In sum, courts have been called upon to play key roles in deciding who should bear losses from data breaches like Target's. This is often done on a case-by-case basis, and often litigated under a variety of state laws. This has led to a lack of uniformity in the outcomes.

This situation has led to calls from some academics and media observers for Congress to examine the issue of who ultimately is responsible for the losses and who is in the best position to prevent losses. Some have also called on Congress to craft policy solutions allocating liability to those best able to minimize the threat of cybercrime and thereby protect consumers at the least cost.[72] Because of the shared responsibility for cybersecurity over consumers' data, however, it may not be easy to determine which parties are in fact in the best position to minimize the threat of cybercrime and protect consumers.[73] This is because customers' data are necessarily shared by retailers, payment card companies, payment processors, and financial institutions. Because breaches may occur at any point along this chain, deciding who should bear the cost of cybersecurity may not be straightforward.

To date, congressional hearings on the Target breaches have tended to focus more on policy solutions, such as notifying consumers that data breaches have occurred, and increasing or clarifying the FTC's authority to sanction lax data security practices. They have not focused on whether or how to allocate shared responsibility to the parties best positioned to protect against cyber breaches.

What Policy Options Are Being Discussed?

This section discusses selected policy options that have been raised in congressional hearings held on data security and breaches following the Target breach.[74]

---

[72] See, e.g., Michael Riley, Ben Elgin, and Dune Lawrence et al., "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," *BloombergBusinessweek*, March 13, 2014, at http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p1. This call has been echoed by academics. For example, see. Richard A. Epstein and Thomas P. Brown "Cybersecurity in the Payment Card Industry," *The University of Chicago Law Review*, vol. 75, no. 1 (winter, 2008), pp. 203-223, which notes, " ... of equal importance is the allocation of losses among innocent parties who have suffered losses from various forms of theft," see http://www.jstor.org/stable/20141905.

[73] See Richard A. Epstein and Thomas P. Brown "Cybersecurity in the Payment Card Industry," *The University of Chicago Law Review*, vol. 75, no. 1 (winter, 2008), p. 206.

[74] These hearings included U.S. Congress, Senate Committee on Banking, Housing, and Urban Affairs, Subcommittee on National Security and International Trade and Finance, Safeguarding Consumers' Financial Data, 113th Cong., 2nd sess., February 3, 2014 and, *Oversight of Financial Stability and Data Security*, February 6, 2014; 113th Cong., 2nd sess., at http://www.banking.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=8a669045-f9b9-4c7e-b1df-1bb08e694e90, U.S. Congress, Senate, Committee on the Judiciary, *Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime*, February 4, 2014; 113th Cong., 2nd sess., at http://www.judiciary.senate.gov/hearings/hearing.cfm?id=138603a26950ad873303535a6300170f; U.S. Congress, House of Representatives, Committee on Energy and Commerce Committee, *Protecting Consumer Information: Can Data Breaches Be Prevented?,* 113th Cong., 2nd sess., February 5, 2014; at http://energycommerce.house.gov/hearing/protecting-consumer-information-can-data-breaches-be-prevented, the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit, *Data Security: Examining Efforts to Protect Americans' Financial Information*, March 5, 2014, at http://energycommerce.house.gov/hearing/protecting-consumer-information-can-data-breaches-be-prevented, and U.S. Congress, Senate, Committee on Commerce, *Protecting Personal Consumer*
(continued...)

Passing a Federal Data Breach Notification Law

In each of the hearings related to the Target breach, various Members of Congress raised the possibility of a federal data breach notification law. Bills were introduced in the 113th and earlier Congresses that would include some form of federal notification requirement for data security breaches. As will be discussed, 47 states presently have data breach notification laws.[75]

The phrase "data breach notification" is somewhat ambiguous, particularly when details such as personal information are introduced into the equation. Generally speaking, however, a data security breach occurs when there is unauthorized access to sensitive personally identifiable information (PII) that could compromise the confidentiality or integrity of data. "Data breach notification" involves mandating that the company holding the PII notify those whose PII was compromised.[76] Currently, only a few specific sectors of the private-sector economy are required by federal law to notify consumers when a data breach may have compromised their personal information, or PII.[77] These include certain financial institutions covered by the Gramm-Leach-Bliley Act[78] and certain health care entities covered by the Health Insurance Portability and Accountability Act (HIPAA)[79] and the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[80] There is no comprehensive federal law governing the protection of data held by private actors.[81] However, certain sectors are subject to cybersecurity obligations that may include data security.[82] Nor is there any comprehensive federal law requiring notification of breaches of such private data.

(...continued)

Information from Cyber Attacks and Data Breaches, 113th Cong., 2nd sess., March 26, 2014, at http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=082407f8-9740-4e43-b2d2-1520c5495014&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a; U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *Data Breach on the Rise: Protecting Personal Information from Harm*, 113th Cong., 2nd sess., April 2, 2014, at http://www.hsgac.senate.gov/hearings/data-breach-on-the-rise-protecting-personal-information-from-harm.

[75] For detailed background and information on data breach notification laws, including details on states' laws, please see CRS Report R42475, *Data Security Breach Notification Laws*, by Gina Stevens. For additional background and information on prior bills introducing a federal data breach notification standard, please see CRS Report R42474, *Selected Federal Data Security Breach Legislation*, by Kathleen Ann Ruane. For an update on the number of states with such laws, see National Conference of State Legislatures, "State Security Breach Notification Laws," April 11, 2014, at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[76] CRS Report R42475, *Data Security Breach Notification Laws*, by Gina Stevens.

[77] CRS Report R42474, *Selected Federal Data Security Breach Legislation*, by Kathleen Ann Ruane.

[78] 15 U.S.C. §§6801-6809.

[79] 42 U.S.C. §1320d et seq.

[80] P.L. 111-5.

[81] In addition to certain financial institutions and healthcare facilities, the FTC enforces several statutes and rules imposing obligations upon some businesses that collect and maintain consumer data. This includes the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§6501-6506), which requires reasonable security for children's information collected online. Also, the Fair Credit Reporting Act (FCRA) requires consumer reporting agencies to use reasonable procedures to ensure that those to whom they disclose sensitive information have a permissible purpose for it. Nevertheless, only a few segments of the private economy are subject to any data security requirements, much less data breach notification requirements. See "Prepared Statement Of The Federal Trade Commission" before U.S. Congress, House of Representatives, The Committee On Energy And Commerce Subcommittee On Commerce, Manufacturing, And Trade, *Protecting Consumer Information: Can Data Breaches Be Prevented?*, February 5, 2014, at http://docs.house.gov/meetings/IF/IF17/20140205/101714/HMTG-113-IF17-Wstate-RamirezE-20140205.pdf.

[82] For more on this, please see CRS Legal Sidebar, *Federal Securities Laws and Recent Data Breaches*.

According to the National Conference of State Legislatures, currently 47 states, the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands have passed laws requiring notification of security breaches involving personal information.[83] Three states have not passed such laws: Alabama, New Mexico, and South Dakota.[84] California in 2002 became the first state to pass such a law.[85]

Businesses have complained about the patchwork of numerous, separate data breach notification laws[86] they are required to comply with, citing burdensomeness and inefficiency.[87] Business groups representing the financial and retail sectors, such as the Financial Services Roundtable and the National Retail Federation, have recently called for passage of a federal data breach notification law.[88] Some state regulators, state attorneys general, and certain consumer groups have voiced concerns that a federal law could preempt state laws and prevent states from mandating stricter notification standards.[89] A stronger federal data breach notification law, by contrast, appears to be more attractive to consumer groups.[90] A number of businesses have called for enactment of a federal notification law as it may result in cost savings, by potentially

[83] National Conference of State Legislatures, "State Security Breach Notification Laws," April 11, 2014, at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. For a discussion of the differences in state data breach notification laws, see Reid J. Schar and Kathleen W. Gibbons, "Complicated Compliance: State Data Breach Notification Laws," *Bloomberg BNA*, August 9, 2013, at http://www.bna.com/complicated-compliance-state-data-breach-notification-laws/. For summaries of state data breach notification laws, see Perkins Cole, "Security Breach Notification Chart," October 2013, at http://www.perkinscoie.com/statebreachchart/ and Mintz, Levin, Cohn, Ferris, Glovsky & Popeo, P.C. "State Data Breach Notification Laws," December 1, 2013, at http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf.

[84] National Conference of State Legislatures, "State Security Breach Notification Laws," April 11, 2014, at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[85] Cal. Civ. Code §§1798.29, 1798.80 et seq.

[86] These state laws can have differing or conflicting requirements, as well. For instance, some states require immediate notification, while others, such as Ohio and Wisconsin, require notification within 45 days. For a side-by-side summary of the data breach notification requirements of the state laws, please see Scott & Scott, "State Data Breach Notification Laws," Sept. 21, 2007, at http://www.scottandscottllp.com/resources/state_data_breach_notification_law.pdf.

[87] For instance, see Testimony of James Reuter, President of First Data Corp., before U.S. Congress, Senate, Committee on Banking, Housing, and Urban Affairs, Subcommittee on National Security and International Trade and Finance, *Safeguarding Consumers' Financial Data*, 113th Cong., 2nd sess., February 3, 2014, "Consumers' electronic payments are not confined by borders between states. As such, a national standard for data security breach notification, as contained in Senate bill 1927, the Data Security Act of 2014, is of paramount importance." The National Retail Federation and the Financial Services Roundtable, among other business groups, have echoed the call for a national data breach notification law. For such calls from academics, see, e.g., Tom, Jacqueline May, "A Simple Compromise: The Need for a Federal Data Breach Notification Law," 84 *St. John's Law Review* 1569 (2010); Winn, Jane K., Are "Better" Security Breach Notification Laws Possible?" *Berkley Technology Law Journal*, vol. 24, June 8, 2009, at http://ssrn.com/abstract=1416222.

[88] National Retail Federation, Financial Services Roundtable, et al., "Merchant and Financial Trade Associations Announce Cybersecurity Partnership," press release, February 13, 2014, at http://nrf.com/modules.php?name=Documents&op=showlivedoc&sp_id=7818 or at http://fsroundtable.org/merchant-and-financial-trade-associations-announce-cybersecurity-partnership/.

[89] Testimony of Edmund Mierzwinski, Director, Consumer Program, U.S. Public Interest Research Group, before U.S. Congress, Senate, Committee on Banking, Housing and Urban Affairs, Subcommittee on National Security and International Trade and Finance, *Safeguarding Consumers' Financial Data*, Panel 2," February 3, 2014, at http://www.banking.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=3d7b11bb-d07c-41b2-9431-2cf39af48920 and http://www.cq.com/doc/congressionaltranscripts-4417795.

[90] Ibid. Mierzwinski stated, for instance, that he hoped any data breach notification law would trigger notification when personal data had been wrongfully acquired, rather than when actual harm had occurred to consumers.

eliminating the need to comply with 47 individual state laws.[91] In addition, the executive branch has voiced support for a federal data breach notification law.[92] Recent media reports have suggested that bipartisan consensus may be building around the necessity of a federal data breach notification law, although details remain divergent between various bills and proposals.[93]

Generally, data breach notification laws include several components and address topics such as (1) which entities must comply with the law; (2) what information is being protected, and how a security breach or data breach is defined; (3) what degree of actual harm must occur, if any, for notice to be triggered; (4) how and when must notice be delivered; (5) are there any exceptions or safe harbors; (6) to what degree does this preempt state law and how does the law relate to other federal laws; and (7) what penalties, enforcement authorities, and remedies for those harmed does it create.[94]

The data breach notification bills introduced in the 113th Congress (S. 1897, S. 1193, S. 1927, S. 1976, S. 1995, H.R. 1468, and H.R. 3990)[95] addressed these elements in various ways. Some of these bills contained express preemption clauses that could potentially displace certain state laws on data breach notification in order to create a uniform data breach notification standard.

Modifying Federal Trade Commission Statutory Powers

Some in Congress have called for passage of a law to strengthen the Federal Trade Commission's (FTC's) statutory authority to penalize businesses that fail to adequately protect consumers' personally identifiable information.[96] The FTC pursues enforcement actions against companies for failing to protect consumers' personal information.[97]

Currently, the FTC relies on its statutory powers under Section 5 of the Federal Trade Commission Act[98] to pursue data security violations. First, if a company makes materially misleading statements or omissions relating to an entity's data security practices and such statements or omissions are likely to mislead reasonable consumers, the FTC has argued that a company has engaged in unfair and deceptive practices prohibited by Section 5.[99] The company

[91] See, e.g., National Retail Federation, Financial Services Roundtable, et al., "Merchant and Financial Trade Associations Announce Cybersecurity Partnership," press release, February 13, 2014, at http://nrf.com/modules.php?name=Documents&op=showlivedoc&sp_id=7818 or at http://fsroundtable.org/merchant-and-financial-trade-associations-announce-cybersecurity-partnership/.

[92] U.S. Department of Justice, "Attorney General Holder Urges Congress to Create National Standard for Reporting Cyberattacks," press release, February 24, 2014, at http://www.justice.gov/opa/pr/2014/February/14-ag-194.html.

[93] Rob Margetta, "Data Breach Response May Be Limited to Notification," *Roll Call*, March 12, 2014, at http://www.rollcall.com/news/data_breach_response_may_be_limited_to_notification-231430-1.html?zkPrintable=true.

[94] CRS Report R42475, *Data Security Breach Notification Laws*, by Gina Stevens.

[95] H.R. 1468 is a companion bill to S. 1193, and H.R. 3990 is a companion bill to S. 1897.

[96] As discussed later in this section, bills such as S. 1193, S. 1897, S. 1927, S. 1976 and S. 1995 address providing the FTC with additional statutory authorities in various ways.

[97] See e.g., Patricia Cave, "Giving Consumers a Leg to Stand On," *Catholic University Law Review*, spring 2013, p. 781; and John A. Fisher, "Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach," *William & Mary Business Law Review*, 2013, at http://scholarship.law.wm.edu/wmblr/vol4/iss1/7.

[98] 15 U.S.C. §45.

[99] See Testimony of Federal Trade Commission before U.S. Congress, House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, *Protecting Consumer Information: Can Data*
(continued...)

can agree with the FTC, negotiate a consent agreement with the FTC, or deny the FTC's claim. In this latter situation, the FTC could sue the company, alleging they engaged in unfair and deceptive practices prohibited under Section 5.[100] The FTC has reported that it has settled more than 30 matters on these grounds alone, in challenging companies' express or implied claims that they provided reasonable security for personal data.[101] Second, if a company's data security practices either "cause or are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers nor are outweighed by benefits to consumers or to competition," the FTC has argued that those practices can be found to violate Section 5 of the Federal Trade Commission Act.[102] The FTC stated that it has settled more than 20 cases based on such allegations that a failure to reasonably safeguard consumer data was an unfair trade practice.[103]

Despite the FTC's total of 50 settlements broadly related to data security since 2001, the Federal Trade Commission Act does not contain explicit statutory power for the FTC to levy civil penalties specifically for unfair or deceptive trade practices related to data breaches.[104] The remedies agreed to in the settlements include the company agreeing to cease the unfair or deceptive trade practice but not paying extra penalties.[105] For example, the FTC reached a data security settlement with TRENDnet, which involved a video camera designed to allow consumers to monitor their homes remotely.[106] While TRENDnet marketed the cameras for in-home monitoring and claimed in product descriptions that the cameras were "secure," TRENDnet allegedly had software that left them open to online viewing by anyone with the cameras' web addresses, resulting in hackers posting 700 consumers' live feeds on the Internet.[107] Pursuant to a settlement with the FTC, TRENDnet must maintain a comprehensive security program, obtain outside audits, notify consumers about the security issues and about software updates to correct them, and provide affected customers with free technical support for two years.[108] But the FTC does not possess explicit statutory powers to impose monetary penalties or punitive fines on companies, such as TRENDnet or others, for unfair or deceptive trade practices related to a data breach.[109] The FTC has asked Congress to pass legislation making explicit its authority in this

(...continued)

Breaches Be Prevented? 113th Cong., 2nd sess., February 5, 2014, p. 3.

[100] Ibid.

[101] Ibid.

[102] Ibid.

[103] Ibid., p. 4.

[104] Ibid., p. 11.

[105] Jill Joerling, "Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data," *Washington University Journal of Law and Policy*, vol. 32 (2010), p. 485.

[106] TRENDnet, Inc., No. 122-3090 (September 4, 2013), at http://www.ftc.gov/opa/2013/09/trendnet.shtm.

[107] Testimony of Federal Trade Commission before U.S. Congress, House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, *Protecting Consumer Information: Can Data Breaches Be Prevented?*, 113th Cong., 2nd sess., February 5, 2014, p. 6.

[108] Ibid.

[109] *Prepared Statement of the Federal Trade Commission on Data Breach on the Rise: Protecting Personal Information from Harm,* Before the Committee on Homeland Security and Governmental Affairs, United States Senate, April 2, 2014, p. 10: "Under current laws, the FTC only has authority to seek civil penalties for data security violations with regard to children's online information under COPPA or credit report information under the FCRA. To help ensure effective deterrence, we urge Congress to allow the FTC to seek civil penalties for all data security and breach notice violations in appropriate circumstances," at http://www.ftc.gov/system/files/documents/public_statements/296011/140402datasecurity.pdf.

area.[110] The agency argues that having the explicit authority to impose fines or penalties as a result of an unfair or deceptive trade practice due to a data breach could provide a more useful deterrent effect.[111] The FTC has also requested that it be given express statutory authority to issue rules and regulations and jurisdiction over non-profit companies, which may also store consumers' personal data.[112]

The validity of the FTC's authority to pursue a company's data breach practices has recently been challenged in federal court.[113] Some had predicted that the outcome of the court case could have affected the FTC's current enforcement authority over data security.[114] In June 2012, following intermittent data breaches between 2008 and 2010, the FTC sued Wyndham hotel chains for allegedly misrepresenting the security measures the company took to protect consumers' personal information.[115] In response, Wyndham filed a motion to dismiss the lawsuit in 2013.[116] Wyndham claimed that "Section 5's prohibition on 'unfair' trade practices does not give the FTC authority to prescribe data-security standards for the private sector, particularly through selective enforcement actions that seek to impose after-the-fact Section 5 liability without any fair notice as to what the Commission believes Section 5 prohibits or requires."[117] Some had predicted that, if the court had ruled in Wyndham's favor, then, barring any legislative action by Congress, future such lawsuits by the FTC over data security could become more problematic for the independent agency.[118] However, on April 7, 2014, the U.S. District Court for the District of New Jersey denied Wyndham's motion to dismiss the FTC's lawsuit, ruling that the FTC had adequately stated claims that Wyndham engaged in unfair and deceptive practices.[119]

Several bills introduced in the Senate in the 113th Congress could have affected the FTC's powers. S. 1193 (Senator Toomey), S. 1897 (Senator Leahy), S. 1927 (Senator Carper and Senator Blunt), S. 1976 (Senator Rockefeller), and S. 1995 (Senator Blumenthal) would have given the FTC the express power to levy civil penalties on companies that fail to comply with certain data security standards. S. 1897 would have permitted the FTC to impose civil penalties for violations for failing to comply with federal cybersecurity standards. S. 1976 would have provided the FTC with explicit authority to promulgate "information security" regulations that could extend to certain non-profits. The bill would have further allowed the FTC to enforce violations of these regulations with various civil penalties. Likewise, S. 1995 would have given enforcement authority to the FTC. In several hearings related to the Target breach, some Members of Congress

[110] Ibid., p. 11.

[111] Ibid.

[112] Ibid.

[113] Federal Trade Commission v. Wyndham Worldwide Corporation et al., No. 13-1887 (D. N.J. filed March 26, 2013).

[114] Jessica Meyers and Erin Mershon, "Critical Breach Verdict Nears in FTC Case," *Politico*, February 24, 2014.

[115] Ibid.

[116] Notice of Motion to Dismiss by Defendants, Federal Trade Commission v. Wyndham Worldwide Corporation et al., No. 13-1887 (D. N.J. Apr. 26, 2013) ECF No. 91.

[117] Ibid.

[118] See "FTC Administrative Complaint Asserts Authority to Regulate Data Security Practices," *Tech Law Journal*, August 29, 2013, at http://www.techlawjournal.com/topstories/2013/20130829.asp; Jessica Meyers and Erin Mershon, "Critical Breach Verdict Nears in FTC Case," *Politico*, February 24, 2014; and Allison Grande, "FTC Unfairness Authority Designed To Be Broad, Brill Says," *Law 360*, February 19, 2014.

[119] Opinion, Federal Trade Commission v. Wyndham Worldwide Corporation et al., No. 13-1887 (D. N.J. Apr. 7, 2014). The court has not yet ruled on the merits of the FTC's claims at this stage.

broached the subject of increasing the FTC's powers to pursue data breach actions.[120] There were no similar bills in the House in the 113th Congress.

Creating Federal Standards for Data Security, Including for Businesses

Some contend that a federal data breach notification law on its own is insufficient to combat widespread data breaches, primarily because the notification comes after the fact of a breach.[121] Such critics advocate that in addition to data breach notification, the federal government might create standards for what represents a minimum acceptable level of data security. One study noted that a lack of clarity in terms of what precautions businesses should take to protect consumers' personal information has resulted in a patchwork of state data security standards.[122] Though the FTC has proposed some generic guidelines, the agency arguably does not have authority to promulgate official regulations which could detail such standards more fully.[123]

Creating a federal standard for data security has both proponents and opponents in Congress. On the one hand, critics voice concerns that a federal standard would be too rigid for such a rapidly evolving, technology-driven field as data security.[124] They fear that a federal standard could be burdensome and could lag behind new technological trends or even discourage businesses from adopting newer technologies to prevent fraud. On the other hand, proponents of creating federal data security standards argue that such a standard need not be specific nor advocate particular technologies.[125] According to this argument, the federal statute could, for example, consist of a

[120] See, for example, the comments of Senator Elizabeth Warren during questions and answers during the U.S. Congress, Senate, Banking, Housing, and Urban Affairs Committee hearing *Safeguarding Consumers' Financial Data,* February 3, 2014, Panel 1: "I think this is a real problem, that the FTC's enforcement authority in this area is so limited. The FTC should have the enforcement authority it needs to protect consumers, and it looks like to me it doesn't have that authority right now," at http://www.cq.com/doc/congressionaltranscripts-4417727.

[121] See, e.g., Patricia Cave, "Giving Consumers a Leg to Stand On," *Catholic University Law Review*, Spring 2013, p. 781; and John A. Fisher, "Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach," *William & Mary Business Law Review*, 2013, at http://scholarship.law.wm.edu/wmblr/vol4/iss1/7.

[122] Jill Joerling, "Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data," *Washington University Journal of Law and Policy*, vol. 32 (2010), p. 485.

[123] Ibid.

[124] See, e.g., Opening Statement as Prepared, of Representative Lee Terry, Chair of Subcommittee on Commerce Manufacturing and Trade, U.S. Congress, House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, Protecting *Consumer Information: Can Data Breaches Be Prevented?*, 113th Cong., 2nd sess., February 5, 2014, at http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/CMT/20140205/HHRG-113-IF17-IF03-MState-T000459-20140205.pdf, "I do not believe that we can solve this whole problem by codifying detailed, technical standards or with overly cumbersome mandates. Flexibility, quickness, and nimbleness are all attributes that are absolutely necessary in cyber security but run contrary to government's abilities.... The security of data itself is paramount in this conversation, but as I have said, cumbersome statutory mandates can be ill equipped to deal with evolving threats. Nonetheless, I think this subcommittee would benefit from hearing about how companies are dealing with this issue now, as well as in the future."

[125] See, e.g., Senator John D. Rockefeller IV, Chairman of the Senate Committee on Commerce, Science, and Transportation, "Rockefeller, Feinstein, Pryor, Nelson Introduce Data Security Bill to Protect Consumers from Data Breaches," press release, January 30, 2014, at http://www.commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=71a755fa-742d-4424-8523-5c53953cb5f6&ContentType_id=77eb43da-aa94-497d-a73f-5c951ff72372&Group_id=4b968841-f3e8-49da-a529-7b18e32fd69d&MonthDisplay=1&YearDisplay=2014, "Companies constantly collect personal information about their customers, like credit card information, financial account numbers and passwords. In return, I believe those companies should be responsible for securing this personal (continued...)

mandate that an organization[126] employ a level of data security that is "reasonable" for the size and complexity of its data operations, for the cost of available tools to reduce vulnerabilities, and for the volume and sensitivity of consumer information it holds.[127]

Bills in both the Senate and the House appear to create differing types of federal standards for data security, along with other changes, such as data breach notification. Bills on this subject include S. 1193, S. 1897, S. 1976, S. 1995, and S. 1927. S. 1193 and H.R. 1468 would require covered entities to "take reasonable measures to protect and secure data in electronic form containing personal information."[128]

Section 202 of S. 1897 and H.R. 3990 would establish broad information security standards and would further authorize the FTC to establish more detailed data security regulations. Such regulations would relate to the implementation of a personal data privacy and security program, vulnerability testing of data security by firms, periodic risk assessments, and employee training on data security.[129] To enforce these data security standards, both bills would provide for civil penalties for violations of the standards.[130]

S. 1927 sets forth a requirement that covered entities "implement, maintain, and enforce reasonable policies and procedures to protect the confidentiality and security of sensitive account information and sensitive personal information.... "[131] Rather than leaving it entirely to the FTC to promulgate rules on these standards, it would give that rulemaking authority, along with enforcement authority, to each institution's prudential regulator.[132] For financial institutions, that prudential regulator would be either the Office of the Comptroller of the Currency (OCC), the Federal Reserve, or the Federal Deposit Insurance Corporation (FDIC). For institutions that are registered investment advisers, investment companies, or broker-dealers, that regulator would be the Securities and Exchange Commission. For institutions that are futures commission merchants, commodity trading advisors, commodity pool operators, or introducing brokers, the regulator would be the Commodity Futures Trading Commission. For Fannie Mae or Freddie Mac, the regulator would be the Federal Housing Finance Agency. For any other business not covered by these categories, the regulator would be the FTC.

(...continued)

information throughout their systems that store this sensitive data," at http://www.commerce.senate.gov/public/index.cfm?p=Legislation&ContentRecord_id=40e0ad58-866a-41ea-bf00-750c17e1ee3a&ContentType_id=03ab50f5-55cd-4934-a074-d6928b9dd24c&Group_id=6eaa2a03-6e69-4e43-8597-bb12f4f5aede.

[126] In the broad term "organization," the FTC has urged the inclusion of not only private businesses but also non-profits, which it states have been subject to numerous data breaches. See Testimony of Federal Trade Commission before U.S. Congress, House of Representatives Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, *Protecting Consumer Information: Can Data Breaches Be Prevented?*, 113th Cong., 2nd sess., February 5, 2014, p.1, at http://docs.house.gov/meetings/IF/IF17/20140205/101714/HMTG-113-IF17-Wstate-RamirezE-20140205.pdf.

[127] Such a "reasonableness" standard was spelled out by Edith Ramirez, Chair of the FTC, in Testimony of Federal Trade Commission before U.S. Congress, House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, *Protecting Consumer Information: Can Data Breaches Be Prevented?* 113th Cong., 2nd sess., February 5, 2014, p. 4.

[128] S. 1193, Section 2.

[129] S. 1897, Section 202.

[130] S. 1897, Section 203.

[131] S. 1927, Section 3.

[132] S. 1927, Section 5.

S. 1976[133] would authorize the FTC to promulgate regulations providing detailed security standards and would set out four requirements for the FTC to analyze in its rulemaking, along with other requirements, such as a designated officer for information security and a written security policy regarding use and storage of personal information.[134]

S. 1995 would set out requirements for a personal data privacy and security program[135] and would give the FTC the right to promulgate rules further delineating these requirements.[136] The bill requires companies to conduct risk assessments, adopt risk controls, conduct employee training in data security, and conduct periodic vulnerability assessments.[137] It provides enforcement authority, and the right to levy civil penalties, to the Department of Justice, and in some cases, to state attorneys general, and also creates a private right of action.[138]

The executive branch has released a voluntary framework for data security among so-called critical infrastructure industries. On February 12, 2014, the National Institute of Standards and Technology (NIST), an agency within the Department of Commerce, issued its *Framework for Improving Critical Infrastructure Cybersecurity*, known more commonly as *The Cybersecurity Framework*. While the financial sector is considered to be part of the U.S. "critical infrastructure," the retail sector is not.[139] Thus, the "merchants" sector discussed in this report on the Target breach are not included in this voluntary framework. Target, however, owns a bank and after its data breaches used this to become the first retailer to join the financial services information sharing and analysis sector (FS-ISAC).[140] The NIST framework is discussed in more detail in the CRS Legal Sidebar *National Institute of Standards and Technology Issues Long-awaited Cybersecurity Framework*.[141] The impact of the NIST framework remains to be seen.[142] Being voluntary, the framework contains no direct means to enforce compliance. Some have argued, however, that the existence of the framework could potentially create a basis for a standard of conduct that could possibly become a benchmark for courts to evaluate liability relating to data security under tort and other law.[143]

[133] S. 1976 is co-sponsored by Chairman of the Senate Select Intelligence Committee Senator Feinstein, Chairman of the Commerce Subcommittee on Communications, Technology, and the Internet, Senator Pryor; and Chairman of the Commerce Subcommittee on Science and Space, Senator Bill Nelson.

[134] S. 1976, Section 2.

[135] S. 1995, Section 202.

[136] S. 1995, Section 202.

[137] S. 1995, Section 202.

[138] S. 1995, Sections 203-205.

[139] Presidential Policy Directive/PPD-21, "Critical Infrastructure Security and Resilience," February 12, 2013, at http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[140] Testimony of John J. Mulligan, executive vice president and chief financial officer, Target, before U.S. Congress, Senate, Committee on Commerce, Science, and Transportation, *Protecting Personal Consumer Information from Cyber Attacks and Data Breaches*, 113th Cong., 2nd sess., March 26, 2014, pp. 4-5, at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=c2103bd3-8c40-42c3-973b-bd08c7de45ef.

[141] Andrew Nolan, "National Institute of Standards and Technology Issues Long-awaited Cybersecurity Framework," CRS Legal Sidebar, March 5, 2014, at http://www.crs.gov/LegalSidebar/details.aspx?ID=829&Source=search.

[142] Ibid.

[143] Ibid.

Requiring Adoption of More Advanced Technologies

One issue that has been raised in hearings (but not pursued legislatively) has been the question of how costs for improved cybersecurity—including penalties and fees for breaches—are allocated across merchants, credit card companies, payment processors, and issuing and acquiring banks. This is problematic as customer PII is shared by these companies and must be protected through the payment chain.[144] To use a simple analogy, in a house shared by several roommates, each wants to see the house kept clean, but no one wants to clean the living room. Similarly, customer information is often protected by each of these parties to the payment system at different points along the way, including by the merchant, the payment card company, the issuing and acquiring banks, and the payment processor. This creates a similar problem of participants trying to shift the costs of cyber protection to the other participants.[145] How cybersecurity costs are allocated relates to the question of whether retailers, banks, and payment card companies have been willing to pay for, and adopt, new data security technology quickly enough.

These issues were raised in congressional hearings. Witnesses at times criticized parties representing merchants, banks, or payment card companies for inadequate payment card security, resulting in what the media called "finger-pointing."[146] Yet it is unclear whether a superior legislative solution to this shared property problem exists.[147] Currently, a web of negotiated agreements allocates liability for customer breaches among the various parties. Merchant trade groups, however, have complained that excessive market power of payment card companies, such as MasterCard and Visa, has forced an undue share of the costs of cybersecurity protections on the merchants, and that they also bear an unduly high share of the penalties and indemnifications to payment card companies and banks for breaches, while payment card companies are not spending enough to upgrade security technology, including moving from magnetic stripe and signature to Chip and PIN.[148] Banks, meanwhile, have complained that they pay most of the costs to reissue cards and reimburse for fraudulent charges and that often such breaches result from merchants' security errors.[149]

Could a legislative solution better allocate such costs compared with individually negotiated contracts? A 2010 Federal Reserve Bank of Philadelphia discussion paper[150] interviewed many

[144] For more on this, see Richard A. Epstein and Thomas P. Brown "Cybersecurity in the Payment Card Industry," *University of Chicago Law Review*, vol. 75, no. 1 (winter, 2008), pp. 203-223, at http://www.jstor.org/stable/20141905.

[145] Richard A. Epstein and Thomas P. Brown "Cybersecurity in the Payment Card Industry," *University of Chicago Law Review*, vol. 75, no. 1 (winter, 2008), pp. 203-223 at 207.

[146] Craig Newman and Daniel Stein, "Who Should Pay for Data Theft?" *Bloomberg BusinessWeek*, February 20, 2014, at http://www.businessweek.com/articles/2014-02-20/who-should-pay-for-data-theft. See also Marcy Gordon, "Target Breach Pits Banks against Retailers," *Associated Press*, February 4, 2014, at http://bigstory.ap.org/article/target-data-breach-pits-banks-against-retailers.

[147] Epstein and Brown argue that no such legislative solution exists and that private contract negotiations are a superior solution for allocating such shared costs, but concede that proper allocation is problematic.

[148] Doug Kantor, Counsel for the Merchants Payments Coalition, "Broken Payment System Guarantees another Breach like Target's," *American Banker*, January 9, 2014, at http://www.americanbanker.com/bankthink/broken-payment-system-guarantees-another-breach-like-target-1064784-1.html.

[149] Camden Fine, President and CEO of the Independent Community Bankers of America, and Richard Hunt, President and CEO of the Consumer Bankers Association, "Banks Pay Price for Retailers' Data Breaches," *The Hill*, February 11, 2014, at http://thehill.com/blogs/congress-blog/technology/197978-banks-pay-price-for-retailers-data-breaches.

[150] Julia S. Cheney, Robert M. Hunt, Katy R. Jacob, Richard D. Porter, and Bruce J. Summers, *The Efficiency and Integrity of Payment Card Systems: Industry Views on the Risks Posed by Data Breaches*, Federal Reserve Bank of Philadelphia, Payment Cards Center Discussion Paper, October 2012, at http://www.phil.frb.org/consumer-credit-and-(continued...)

payment system participants and found that, while merchants have a vested interest in protecting data to uphold their reputations and brands, as well as to avoid chargebacks, some did not feel they had ownership over the fraud mitigation system with which they contractually have to comply.[151] One concern voiced by banks and payment card companies was that if data security were to become a competitive factor, information sharing and cooperating on data security might be more difficult.[152] Consumers might view competition for superior data security as desirable. While the article raised questions such as to whether the costs of payment card fraud and of avoiding such fraud are borne by the appropriate parties in the payment system, it concluded only that, "The answers to these questions are not simple."[153]

A number of Members of Congress participating in the Target hearings raised the question of why the United States still had not moved to a Chip and PIN system (see "What Industry Best Practices Have Been Adopted?" for more information), as this technology is widely believed to make breaches more difficult.[154] Senator Warren pressed industry representatives to explain why they had not yet adopted this Chip and PIN technology, and she suggested that government action might be warranted to encourage adoption of new technology.[155] Senator Durbin stated that retailers and customers were actually paying one cent for each transaction to cover anti-fraud and security costs of payment cards, and questioned whether the technology upgrades were being adopted quickly enough, in light of this.[156] But, while Members raised the question often of why more advanced technology had not yet been adopted in America, in contrast to the European Chip and PIN standard, they generally stopped short of advocating that the federal government mandate any specific technology upgrades or changes at this point in time.

(...continued)

payments/payment-cards-center/publications/discussion-papers/2012/D-2012-Efficiency-and-Integrity-of-Payment-Card-Systems.pdf.

[151] Ibid.

[152] Ibid., p. 26.

[153] Ibid., p. 30.

[154] For example, U.S. Congress, Senate, Committee on Banking, Housing, and Urban Affairs, Subcommittee on National Security and International Trade and Finance, *Safeguarding Consumers' Financial Data*, 113th Cong., 2nd sess., comments of Senator Warner, Senator Kirk, Senator Warren, Senator Tester, Senator Menendez; and in the Senate Judiciary Committee, comments of Senator Hatch, Senator Durbin, and others. The same question was asked by Members in the other congressional committee hearings.

[155] U.S. Congress, Senate, Committee on Banking, Housing, and Urban Affairs, Subcommittee on National Security and International Trade and Finance, *Safeguarding Consumers' Financial Data*, 113th Cong., 2nd sess., comment of Senator Warren: "We understand why Chip and PIN works better. And it seems that we are years behind Europe in developing adequate technology. Technology we know is out there, but applying adequate technology here in the United States. So I was interested, in your testimony, Mr. Leach, you said that you think that standards are best left to private organizations such as yours. That's what we've done, and now we're now way behind in technology and have become the targets for data attacks from around the world.... So why should we leave this to organizations like yours? It sounds like to me we may need some pressure from the government to make sure that the toughest standards are used." at http://www.cq.com/doc/congressionaltranscripts-4417795.

[156] U.S. Congress, Senate, Committee on the Judiciary, *Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime*, 113th Cong., 2nd sess., February 4, 2014, Comments of Senator Durbin: "Retailers and customers in many cases are paying an additional one cent on every transaction for anti-fraud measures so they are, in fact, giving the issuing banks and card companies basically a subsidy to have anti- fraud technology. So it isn't as if we aren't paying already to move this technology forward," at http://www.cq.com/doc/congressionaltranscripts-4418420.

Where Can I Find Additional CRS Information on Cybersecurity Issues?

- CRS's reports on cybersecurity issues are in *Issues Before Congress: Homeland Security and Terrorism, Cybersecurity* at http://www.crs.gov/pages/subissue.aspx?cliid=4300&parentid=28&preview=False.
- CRS Report R42619, *Cybersecurity: CRS Experts*, by Eric A. Fischer, lists CRS's experts in various aspects of cybersecurity.

Glossary

Table 2. Glossary of Terms

Terms	Explanation
acquirer	The acquirer is the financial institution used by a merchant in a payment card transaction.
cardholder	A cardholder is the person having a payment card.
Chip and PIN	Chip and PIN is a payment card security system with an embedded microprocessor chip and requiring a personal identification number.
Chip and Signature	Chip and Signature is a payment card security system with an embedded microprocessor chip and requiring the cardholder's signature
clearing	Clearing is the process of settling a payment card transaction.
discount rate	The discount rate is the rate charged a merchant by its acquiring bank for processing.
EMV	EMV is a chip standard originally created by Europay, MasterCard, and Visa. It is used in chip-based systems around the world.
encryption	Encryption is using a computer program to scramble information into cipher text so that it makes no sense.
interchange fee	The interchange fee is the fee charged by a payment card for its role in processing a transaction. It is deducted from the funds paid by the issuer to the acquirer.
issuer	The issuer is the bank or other financial institution that issues a payment card to the cardholder.
merchant	A merchant is the organization selling goods or services and accepting a payment card.
payment card	A payment card is a credit card, debit card, prepaid card, or ATM card.
PCI Council	PCI Council is the Payment Card Industry Council, a standards setting group.
PCI DSS	PCI DSS is an acronym for Payment Card Industry data security standards. Currently at version 3.0.
PII	PII is an acronym for personally identifiable information.
PIN	PIN is an acronym for personal identification number, used to authenticate a cardholder in a financial transaction.
POS	POS is an acronym for point of sale, which frequently refers to the machine that reads a payment card.
payment processor	A payment processor is a company that connects a merchant with an acquiring bank in a payment card transaction. Payment processors can establish an account with an acquirer for a merchant.
tokenization	Tokenization is replacing a payment card account number with another number.

Source: The Congressional Research Service.

Author Contact Information

N. Eric Weiss
Specialist in Financial Economics
eweiss@crs.loc.gov, 7-6209

Rena S. Miller
Specialist in Financial Economics
rsmiller@crs.loc.gov, 7-0826