S. HRG. 113–531

PROTECTING PERSONAL CONSUMER INFORMATION FROM CYBER ATTACKS AND DATA BREACHES

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

MARCH 26, 2014

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PUBLISHING OFFICE

92–594 PDF WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

BARBARA BOXER, California	JOHN THUNE, South Dakota, *Ranking*
BILL NELSON, Florida	ROGER F. WICKER, Mississippi
MARIA CANTWELL, Washington	ROY BLUNT, Missouri
MARK PRYOR, Arkansas	MARCO RUBIO, Florida
CLAIRE MCCASKILL, Missouri	KELLY AYOTTE, New Hampshire
AMY KLOBUCHAR, Minnesota	DEAN HELLER, Nevada
MARK BEGICH, Alaska	DAN COATS, Indiana
RICHARD BLUMENTHAL, Connecticut	TIM SCOTT, South Carolina
BRIAN SCHATZ, Hawaii	TED CRUZ, Texas
EDWARD MARKEY, Massachusetts	DEB FISCHER, Nebraska
CORY BOOKER, New Jersey	RON JOHNSON, Wisconsin
JOHN E. WALSH, Montana	

ELLEN L. DONESKI, *Staff Director*
JOHN WILLIAMS, *General Counsel*
DAVID SCHWIETERT, *Republican Staff Director*
NICK ROSSI, *Republican Deputy Staff Director*
REBECCA SEIDEL, *Republican General Counsel and Chief Investigator*

CONTENTS

PROTECTING PERSONAL CONSUMER INFORMATION FROM CYBER ATTACKS AND DATA BREACHES

WEDNESDAY, MARCH 26, 2014

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 1:49 p.m., in room SR–253, Russell Senate Office Building, Hon. John D. Rockefeller IV, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA

The CHAIRMAN. This hearing will come to order. This hearing is in order. It doesn't have to come to order; it is.

We now live in the era of "big data."

You knew that, Senator McCaskill? That is not news to you, OK.

Whether we like it or not, companies are regularly collecting reams of information about us as we go about our daily lives.

I serve on the Intelligence Committee, and I have since before 9/11. And it just drives me absolutely wild sometimes to read—*The New York Times* and *The Washington Post* are the guilty parties, for the most part—but they talk about everybody's privacy is just about to be invaded, except nobody's has been. But if it could happen, then it has happened, you see. That is the way you keep people scared. And now people are reacting to it, saying, oh, we just have to get rid of that thing. We are not necessarily an intelligent Congress when it comes to our national security.

So, in any event, they are tracking us as we visit our websites, as we visit stores, as we purchase products. While some of the information may be mundane, a lot of it is highly sensitive. It might have to do with health, family problems, whatever.

I think we can all agree that if Target or any other company is going to collect detailed information about its customers, they need to do everything possible to protect them from identity thieves.

Because what, in fact, everybody was fearing about the NSA, which has never come to be true, has come to be true about the American private sector. That is the irony of the whole thing. This city is wrought with, you know, the terrible things that could happen from NSA, except nothing terrible has happened, but some terrible things are happening elsewhere.

So it is now well known that Target fell far short of doing this—that is, protecting their customers. Last November and December,

cyber thieves were able to infect their credit card payment terminals with a malicious software, loot their computer servers, access a staggering amount of consumer information, which they could pick and choose from and then sell them for something called a profit.

There has been a lot of anxiety recently about the kind of information the Federal Government—I am making my point here again; I like making this point—may be collecting about American citizens as part of their efforts to protect our country from the ongoing terrorist threat. But the truth is that private companies like Target hold vastly larger amounts of sensitive information about us than the government could ever think of doing. And they spend much less time and much less money protecting their sensitive data than the government does. You cannot penetrate the firewalls, all of the firewalls, around the NSA.

Senator Thune, welcome, sir.

So we learned yesterday that Federal agents notified more than 3,000 companies last year that their computer systems had been hacked. I am certain that there are many more breaches that we never hear about.

In my zeal a number of years ago, I asked the SEC if they would sort of make it a requirement that every time somebody was hacked into, that had to be reported to the SEC, put on their website, for the advantage of the shareholders, because that is the kind of information they need to know if they are going to buy or sell or whatever. That is haphazard at best.

So Target is going to tell us today that they take data security very seriously and that they followed their industry's data security standards, but the fact remains it wasn't enough. The credit card numbers of 40 million people and the e-mail addresses of nearly 70 million people were potentially stolen under their watch.

My staff has carefully analyzed what we know at this point about the Target breach. In a new report, they identify many precise opportunities Target had to prevent this from happening. It is a very interesting sort of a chart of where they could have—and I will hold it up.

And I ask unanimous consent that this be made a part of the record of this hearing.

[The information referred to follows:]

A "KILL CHAIN" ANALYSIS OF THE 2013 TARGET DATA BREACH

Majority Staff Report for Chairman Rockefeller

Executive Summary

In November and December 2013, cyber thieves executed a successful cyber attack against Target, one of the largest retail companies in the United States. The attackers surreptitiously gained access to Target's computer network, stole the financial and personal information of as many as 110 million Target customers, and then removed this sensitive information from Target's network to a server in Eastern Europe.

This report presents an explanation of how the Target breach occurred, based on media reports and expert analyses that have been published since Target publicly acknowledged this breach on December 19, 2013. Although the complete story of how this breach took place may not be known until Target completes its forensic examination of the breach, facts already available in the public record provide a great deal of useful information about the attackers' methods and Target's defenses.

This report analyzes what has been reported to date about the Target data breach, using the "intrusion kill chain" framework, an analytical tool introduced by Lockheed Martin security researchers in 2011, and today widely used by information security professionals in both the public and the private sectors. This analysis suggests that Target missed a number of opportunities along the kill chain to stop the attackers and prevent the massive data breach. Key points at which Target apparently failed to detect and stop the attack include, but are not limited to, the following:

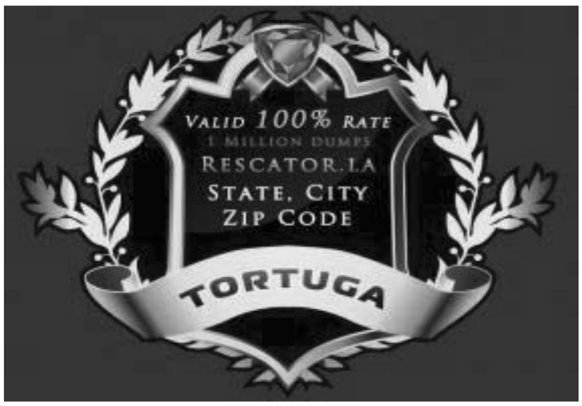
- Target gave network access to a third-party vendor, a small Pennsylvania HVAC company, which did not appear to follow broadly accepted information security practices. The vendor's weak security allowed the attackers to gain a foothold in Target's network.
- Target appears to have failed to respond to multiple automated warnings from the company's anti-intrusion software that the attackers were installing malware on Target's system.
- Attackers who infiltrated Target's network with a vendor credential appear to have successfully moved from less sensitive areas of Target's network to areas storing consumer data, suggesting that Target failed to properly isolate its most sensitive network assets.
- Target appears to have failed to respond to multiple warnings from the company's anti-intrusion software regarding the escape routes the attackers planned to use to exfiltrate data from Target's network.

A. The Target Data Breach

1. The Stolen Data

On December 19, 2013, Target publicly confirmed that some 40 million credit and debit card accounts were exposed in a breach of its network.[1] The Target press release was published after the breach was first reported on December 18 by Brian Krebs, an independent Internet security news and investigative reporter.[2] Target officials have testified before Congress that they were not aware of the breach until contacted by the Department of Justice on December 12.[3] The data breach affected cards used in U.S. Target stores between November 27 and December 18, 2013.[4]

Figure 1 - Advertisement for Stolen Target Cards



Source: Krebsonsecurity.com

[1] Target, *Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores* (Dec. 19, 2013) (online at *http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores*).

[2] Brian Krebs, *Sources: Target Investigating Data Breach*, KrebsOnSecurity (Dec. 18, 2013) (online at *http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/*).

[3] Testimony of John Mulligan, Target Executive Vice President and Chief Financial Officer, before the Senate Committee on the Judiciary, at 2 (Feb. 4, 2014) (online at *http://www.judiciary.senate.gov/pdf/02–04–14MulliganTestimony.pdf*).

[4] *Id.* at 2–3.

Thieves were able to sell information from these cards via online black market forums known as "card shops."[5] These websites list card information including the card type, expiration date, track data (account information stored on a card's magnetic stripe), country of origin, issuing bank, and successful use rate for card batches over time. The newer the batch, the higher the price, as issuing banks often have not had sufficient time to identify and cancel compromised cards. A seller, nicknamed "Rescator," at a notorious card shop even offered a money-back guarantee for immediately cancelled cards.[6] Those purchasing the information can then create and use counterfeit cards with the track data and PIN numbers[7] stolen from credit and debit card magnetic stripes. Fraudsters often use these cards to purchase high-dollar items and fence them for cash, and if PIN numbers are available, a thief can extract a victim's money directly from an ATM. Based on a reading of underground forums, hackers may be attempting to decrypt the stolen Target PIN numbers.[8]

On January 10, 2014, Target disclosed that non-financial personal information, including names, addresses, phone numbers, and e-mail addresses, for up to 70 million customers was also stolen during the data breach.[9]

2. The Attack

On January 12, Target CEO Gregg Steinhafel confirmed that malware installed on point of sale (POS) terminals[10] at U.S.-based Target stores enabled the theft of financial information from 40 million credit and debit cards.[11] This malware utilized a so-called "RAM scraping" attack, which allowed for the collection of unencrypted, plaintext data as it passed through the infected POS machine's memory before transfer to the company's payment processing provider. According to reports by Brian Krebs, a tailored version of the "BlackPOS" malware—available on black market cyber crime forums for between $1,800 and $2,300—was installed on Target's POS machines.[12] This malware has been described by McAfee Director of Threat Intelligence Operations as "absolutely unsophisticated and uninteresting."[13] This assessment is in contrast with the statement of Lawrence Zelvin, Director of the Department of Homeland Security's National Cybersecurity and Communications Integration Center, who describes the malware used in the attack as "incredibly sophisticated."[14]

According to unnamed investigators, the attackers first installed their malware on a small number of POS terminals between November 15 and November 28, with the majority of Target's POS system infected by November 30.[15] A report by *The New*

---

[5] Brian Krebs, *Cards Stolen in Target Breach Flood Underground Markets* (Dec. 20, 2013) (online at *http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/*).

[6] *Id.*

[7] Target initially denied that debit card PIN numbers had been stolen, but reports confirmed that encrypted PIN numbers had indeed been stolen. *See* Jim Finkle and David Henry, *Exclusive: Target hackers stole encrypted bank PINs—source,* Reuters (Dec. 25, 2013) (online at *http://www.reuters.com/article/2013/12/25/us-target-databreach-idUSBRE9BN0L220131225*).

[8] Adam Greenberg, *Hackers Seek to Decrypt PIN Codes Likely Stolen in Target Breach,* SC Magazine (Jan. 8, 2014) (online at *http://www.scmagazine.com/hackers-seek-to-decrypt-pin-codes-likely-stolen-in-target-breach/article/328529/*).

[9] Target, *Target Provides Update on Data Breach and Financial Performance* (Jan. 10, 2014) (online at *http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance*).

[10] A Point of Sale (POS) terminal is a physical device used by a merchant to process payments for goods and services purchased by a customer. Customized hardware and software is often used at a POS terminal, or cash register, part of which is used to swipe and process credit and debit card information.

[11] Becky Quick, *Target CEO Defends 4-Day Wait to Disclose Massive Data Hack,* CNBC (Jan. 12, 2014) (online at *http://www.cnbc.com/id/101329300*).

[12] Brian Krebs, *A First Look at the Target Intrusion, Malware,* KrebsOnSecurity (Jan. 15, 2014) (online at *http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/*).

[13] Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It,* Bloomberg Businessweek (Mar. 13, 2014) (online at *http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data*).

[14] House Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, *Protecting Consumer Information: Can Data Breaches Be Prevented?,* 113th Cong. (Feb. 5, 2014).

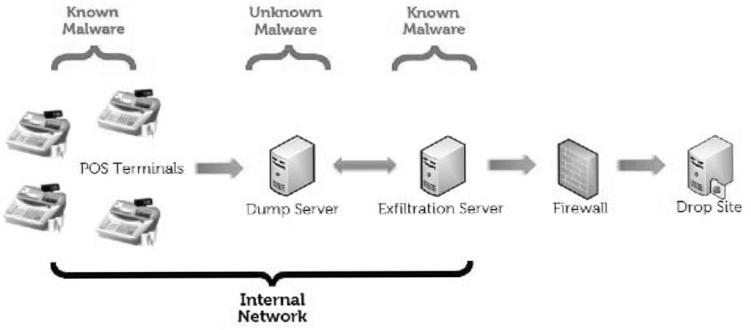
[15] Brian Krebs, *Target Hackers Broke in Via HVAC Company,* KrebsOnSecurity (Feb. 5, 2014) (online at *http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/*).

York Times states that the attackers first gained access to Target's internal network on November 12.[16]

A Dell SecureWorks report shows that the attackers also installed malware, designed to move stolen data through Target's network and the company's firewall, on a Target server.[17] The Dell SecureWorks team was able to analyze a sample of the actual malware used in the Target attack. The attackers reportedly first installed three variants of this malware on November 30 and updated it twice more, just before midnight on December 2 and just after midnight on December 3.[18] According to a *Bloomberg Businessweek* report, Target's FireEye malware intrusion detection system triggered urgent alerts with each installation of the data exfiltration malware.[19] However, Target's security team neither reacted to the alarms nor allowed the FireEye software to automatically delete the malware in question. Target's Symantec antivirus software also detected malicious behavior around November 28, implicating the same server flagged by FireEye's software.[20]

According to Seculert, a security company focused on advanced cyber threats, the malware started to send the stolen data to an external file transfer protocol (FTP) server via another compromised Target server on December 2, 2013.[21] Over the next two weeks, the attackers collected 11 GB of stolen information using a Russia-based server.[22] Analysis of the malware by Dell SecureWorks found that the attackers exfiltrated data between 10:00 a.m. and 6:00 p.m. Central Standard Time, presumably to obscure their work during Target's busier shopping hours.[23] Other sources describe a variety of external data drop locations, including compromised servers in Miami and Brazil.[24] The 70 million records of non-financial data were included in this theft, but public reports do not make clear how the attackers accessed this separate data set.

Figure 2 - Diagram of Data Exfiltration



Source: Dell SecureWorks

---

[16] Elizabeth A. Harris, Nicole Perlroth, Nathaniel Popper, and Hilary Stout, *A Sneaky Path Into Target Customers' Wallets* (Jan. 17, 2014) (online at *http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html*).

[17] A third type of malware was installed on intermediate servers which presumably stored stolen data inside Target's network before the next exfiltration step. However, this malware has thus far not been analyzed publicly. *See* Keith Jarvis and Jason Milletary, *Inside a Targeted Point-of-Sale Data Breach,* Dell SecureWorks, at 5 (Jan. 24, 2014) (online at *http://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf*).

[18] *Id.*

[19] Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It, Bloomberg Businessweek* (Mar. 13, 2014) (online at *http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data*).

[20] *Id.*

[21] Aviv Raff, *PoS Malware Targeted Target,* Seculert (Jan. 16, 2014) (online at *http://www.seculert.com/blog/2014/01/pos-malware-targeted-target.html*).

[22] *Id.*

[23] Keith Jarvis and Jason Milletary, *Inside a Targeted Point-of-Sale Data Breach,* Dell SecureWorks, at 6, 11 (Jan. 24, 2014) (online at *http://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf*).

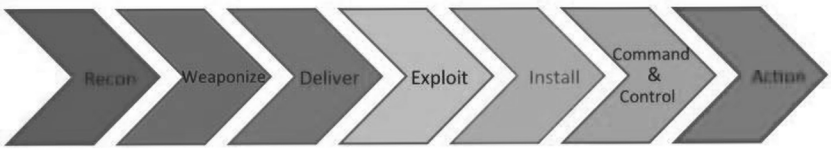
[24] Brian Krebs, *Target Hackers Broke in Via HVAC Company,* KrebsOnSecurity (Feb. 5, 2014) (online at *http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/*).

The attackers reportedly first gained access to Target's system by stealing credentials from an HVAC and refrigeration company, Fazio Mechanical Services, based in Sharpsburg, Pennsylvania.[25] This company specializes as a refrigeration contractor for supermarkets in the mid-Atlantic region [26] and had remote access to Target's network for electronic billing, contract submission, and project management purposes.[27]

Reports indicate that at least two months before the Target data breach began, attackers stole Fazio Mechanical's credentials for accessing Target's network via e-mails infected with malware.[28] According to a former Target security team member, Fazio would more than likely have had access to Target's Ariba external billing system;[29] however, reports do not make clear how the attackers gained access to Target's POS terminals from this initial foothold on the edge of Target's network. According to the same source, it is likely the outside portal was not fully isolated from the rest of Target's network.[30] Once inside, the attackers may have exploited a default account name used by an IT management software product by BMC Software to move within Target's network.[31] The attackers also disguised their data exfiltration malware as a legitimate BMC Software product.[32]

B. The Kill Chain

Figure 3 – Diagram of the Intrusion Kill Chain



Source: Lockheed Martin

1. The "Kill Chain" as a Cybersecurity Defense Tool

The conventional model of information security relies on static defense (*e.g.,* intrusion detection systems and antivirus software) and assumes that attackers have an inherent advantage over defenders given ever-shifting technologies and undiscovered software vulnerabilities. In 2011, the Lockheed Martin Computer Incident Response Team staff published a white paper explaining how these conventional defenses were not sufficient to protect organizations from sophisticated "advanced persistent threats" (APTs).[33] The paper proposed an "intelligence-driven, threat-focused approach to study intrusions from the adversaries' perspective" that could give network defenders the upper hand in fighting cyber attackers.[34]

Instead of installing static defense tools and waiting for the next attack, the paper argued, network defenders should continuously monitor their systems for evidence that attackers are trying to gain access to their systems. Any intrusion attempt reveals important information about an attacker's tactics and methodology. Defenders can use the intelligence they gather about an attacker's playbook to "anticipate and

---

[25] *Id.*

[26] Fazio Mechanical Services, *About Us* (accessed Mar. 12, 2014) (online at *http://fazio mechanical.com/about-us.html*).

[27] Fazio Mechanical Services, *Statement on Target Data Breach* (accessed Mar. 12, 2014) (online at *http://faziomechanical.com/Target-Breach-Statement.pdf*).

[28] Sources have identified malware known as "Citadel," which steals passwords on compromised machines. However, this has not been confirmed. *See* Brian Krebs, *E-mail Attack on Vendor Set Up Breach at Target,* KrebsOnSecurity (Feb. 12, 2014) (online at *http://krebs onsecurity.com/2014/02/e-mail-attack-on-vendor-set-up-breach-at-target/*).

[29] *Id.*

[30] *Id.*

[31] Brian Krebs, *New Clues in the Target Breach,* KrebsOnSecurity (Jan. 29, 2014) (online at *http://krebsonsecurity.com/2014/01/new-clues-in-the-target-breach/*).

[32] Keith Jarvis and Jason Milletary, *Inside a Targeted Point-of-Sale Data Breach,* Dell SecureWorks, at 6 (Jan. 24, 2014) (online at *http://krebsonsecurity.com/wp-content/uploads/ 2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf*).

[33] Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,* Lockheed Martin (2011) (online at *http://www.lockheedmartin.com/content/dam/lockheed/data/ corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf*).

[34] *Id.* at 2.

mitigate future intrusions based on knowledge of the threat."[35] When a defender analyzes the actions of attackers, finds patterns, and musters resources to address capability gaps, "it raises the costs an adversary must expend to achieve their objectives . . . [and] such aggressors have no inherent advantage over defenders."[36]

To illustrate how network defenders can act on their knowledge of their adversaries' tactics, the paper lays out the multiple steps an attacker must proceed through to plan and execute an attack. These steps are the "kill chain." While the attacker must complete all of these steps to execute a successful attack, the defender only has to stop the attacker from completing any one of these steps to thwart the attack.

Analyzing past attacks, utilizing threat intelligence, and improving defenses at all phases of the kill chain allow a defender to detect and deny future attacks earlier and earlier in the kill chain. This requires constant vigilance, but it can theoretically defend against even APTs using so-called "zero-day" exploits, which utilize previously unknown vulnerabilities and attack signatures that defense tools cannot detect.[37]

Figure 4 – Phases of the Intrusion Kill Chain

Source: Lockheed Martin

2. Analysis of the Target Data Breach Using the Kill Chain

John Mulligan, Target's Executive Vice President and Chief Financial Officer, testified that his company "had in place multiple layers of protection, including firewalls, malware detection software, intrusion detection and prevention capabilities and data loss prevention tools."[38] He further stated that Target had been certified in September 2013 as compliant with the Payment Card Industry Data Security Standards (PCI–DSS),[39] which credit card companies require before allowing merchants to process credit and debit card payments.

These steps were obviously not sufficient to prevent the breach. Based on public information about Target's breach reviewed in the previous section, this section

[35] *Id.*
[36] *Id.* at 3.
[37] *Id.* at 4–5.
[38] Testimony of John Mulligan, Target Executive Vice President and Chief Financial Officer, before the Senate Committee on the Judiciary, at 4–5 (Feb. 4, 2014) (online at *http://www.judiciary.senate.gov/pdf/02-04-14MulliganTestimony.pdf*).
[39] *Id.* at 5.

walks through the steps of the kill chain and analyzes what actions Target and its contractor, Fazio Mechanical Services, did or did not take to defend themselves.

A. Reconnaissance—Attacker Quietly Gathers Information About Victim

As discussed above, the attacker may have sent malware-laden e-mails to Fazio at least two months before the Target data breach began. According to analysis by Brian Krebs, the attacker may have found information on Target's third-party vendors through simple Internet searches, which, at the time of his writing, displayed Target's supplier portal and facilities management pages.[40] Files available on these sites provided information for HVAC vendors and, through a metadata analysis, allowed the attacker to map Target's internal network prior to the breach. To disrupt this step in the kill chain, Target could have limited the amount of publicly available vendor information. Target could have also shared threat information with its suppliers and vendors and encouraged collaboration on security within the community.

B. Weaponization—Attacker Prepares Attack Payload to Deliver to Victim

While unconfirmed, the attacker likely weaponized its malware targeting Fazio in an e-mail attachment, likely a PDF or Microsoft Office document. Fazio could have disrupted this step in the kill chain through the use of broadly accepted real-time monitoring and anti-malware software. However, according to investigators familiar with the case, Fazio used the free version of Malwarebytes Anti-Malware, which does not provide real-time protection and is intended only for individual consumer use.[41]

C. Delivery—Attacker Sends Payload to Victim

The attacker sent infected e-mails to Fazio in a so-called phishing attack. Phishing, or "spear phishing," when an attacker customizes e-mail messages using social engineering techniques (*e.g.,* checking Facebook or LinkedIn for a potential victim's business associates and relationships), is a well-known attack method. Fazio could have disrupted this step in the kill chain by training its staff to recognize and report phishing e-mails. Real-time monitoring and anti-malware software could have also potentially detected the infected file(s).

While reports are unconfirmed, the malware on Fazio's systems may have recorded passwords and provided the attackers with their key to Target's Ariba external billing system. In this phase of the kill chain, Target could have potentially disrupted the attack by requiring two-factor authentication for its vendors. Two-factor authentication includes a regular password system augmented by a second step, such as providing a code sent to the vendor's mobile phone or answering extra security questions. According to a former Target vendor manager, Target rarely required two-factor authentication from its low-level contractors.[42] PCI–DSS require two-factor authentication for remote access to payment networks and access controls for all users,[43] although the Ariba system is not technically related to Target's POS system.

However the attacker actually leveraged its access to this vendor's system to enter Target's, less security at the perimeter of Target's network may have contributed to the attacker's success in breaching the most sensitive area of Target's network containing cardholder data. Using the Fazio credentials to gain access to Target's inner network, it appears the attackers then directly uploaded their RAM scraping malware to POS terminals.

D. Exploitation—Attackers Payload Deployed in Victim's Network

Once delivered, the RAM scraping malware and exfiltration malware began recording millions of card swipes and storing the stolen data for later exfiltration. Target could have potentially blocked the effect of the exfiltration malware on its servers by either allowing its FireEye software to delete any detected malware, or, if not choosing the automatic option, by following up on the several alerts that were triggered at the time of malware delivery. According to *Businessweek,* the FireEye software sent an alert with the generic name "malware.binary" to Target security

---

[40] Brian Krebs, *E-mail Attack on Vendor Set Up Breach at Target,* KrebsOnSecurity (Feb. 12, 2014) (online at *http://krebsonsecurity.com/2014/02/e-mail-attack-on-vendor-set-up-breach-at-target/*).

[41] *Id.*

[42] *Id.*

[43] Standard 7.2 and 8.3 are most relevant to this discussion. Version 3.0 of the standard was released in November 2013, after the Target breach. As such, this report references the previous version 2.0. *See* Payment Card Industry Security Standards Council, *Payment Card Industry (PCI) Data Security Standard Version 2.0,* at 44, 47 (Oct. 2010) (online at *https://www.pcisecuritystandards.org/documents/pci__dss__v2.pdf*).

staff.[44] It is possible that Target staff could have viewed this alert as a false positive if the system was frequently alarming.

Another protective step could have been paying greater attention to industry and government intelligence analyses. According to an FBI industry notification, RAM scraping malware has been observed since 2011.[45] Furthermore, a *Reuters* report stated that Visa published in April and August of 2013 two warnings about the use of RAM scraping malware in attacks targeting retailers.[46] These warnings apparently included recommendations for reducing the risk of a successful attack. According to the *Wall Street Journal,* Target's security staff made their misgivings known about vulnerabilities on the company's POS system; however, it is unclear if Target took any action to address vulnerabilities before the attack.[47]

E. Installation—Attacker Establishes Foothold in Victim's Network

Reports suggest that the attacker maintained access to Fazio's systems for some time while attempting to further breach Target's network. It is unclear exactly how the attacker could have escalated its access from the Ariba external billing system to deeper layers of Target's internal network. But given the installation of the BlackPOS malware on Target's POS terminals, the compromise of 70 million records of non-financial data, and the compromise of the internal Target servers used to gather stolen data, it appears that the attackers succeeded in moving through various key Target systems.

Brian Krebs and Dell SecureWorks posit that the attackers may have exploited a default account name used in a BMC Software information technology management system;[48] however, it is unclear exactly how the attackers found the account password. If the theory is true, a protective step at this phase of the kill chain could have included the elimination or alteration of unneeded default accounts, as called for in PCI–DSS 2.1.[49]

In its recently filed 10K, Target states that in the fall of 2013, "an independent third-party assessor found the portion of our network that handles payment card information to be compliant with applicable data security standards."[50] One of those standards would have been PCI–DSS 11.5, which requires vendors to monitor the integrity of critical system files.[51] To achieve this standard, Target could have used a technique called "white listing," whereby only approved processes are allowed to run on a machine.

F. Command and Control (C2)—Attacker Has "Hands on the Keyboard" Remote Access to Victim's Network

Based on the reported timeline of the breach, the attackers had access to Target's internal network for over a month and compromised internal servers with exfiltration malware by November 30. While the exact method by which the attackers maintained command and control is unknown, it is clear the attackers were able to maintain a line of communication between the outside Internet and Target's cardholder network.

---

[44] Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It,* Bloomberg Businessweek (Mar. 13, 2014) (online at *http://www.businessweek.com/articles/2014–03–13/target-missed-alarms-in-epic-hack-of-credit-card-data*).

[45] FBI Cyber Division, *Recent Cyber Intrusion Events Directed Toward Retail Firms* (Jan. 17, 2014) (online at *http://krebsonsecurity.com/wp-content/uploads/2014/01/FBI-CYD-PIN-140117-001.pdf*).

[46] Jim Finkle and Mark Hosenball, *Exclusive: More Well-Known U.S. Retailers Victims of Cyber Attacks—Sources,* Reuters (Jan 12, 2014) (online at *http://www.reuters.com/article/2014/01/12/us-target-databreach-retailers-idUSBREA0B01720140112*).

[47] Danny Yadron, Paul Ziobro, Devlin Barrett, *Target Warned of Vulnerabilities Before Data Breach,* The Wall Street Journal (Feb. 14, 2014) (online at *http://online.wsj.com/news/articles/SB10001424052702304703804579381520736715690*).

[48] Brian Krebs, *New Clues in the Target Breach,* KrebsOnSecurity (Jan. 29, 2014) (online at *http://krebsonsecurity.com/2014/01/new-clues-in-the-target-breach/*); Keith Jarvis and Jason Milletary, *Inside a Targeted Point-of-Sale Data Breach,* Dell SecureWorks, at 5 (Jan. 24, 2014) (online at *http://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf*).

[49] Payment Card Industry Security Standards Council, *Payment Card Industry (PCI) Data Security Standard Version 2.0,* at 24 (Oct. 2010) (online at *https://www.pcisecuritystandards.org/documents/pci__dss__v2.pdf*).

[50] Target Corporation, SEC Form 10–K, at 17, 47 (Mar. 14, 2014) (online at *http://www.sec.gov/Archives/edgar/data/27419/000002741914000014/tgt-20140201x10k.htm*).

[51] Payment Card Industry Security Standards Council, *Payment Card Industry (PCI) Data Security Standard Version 2.0,* at 63 (Oct. 2010) (online at *https://www.pcisecuritystandards.org/documents/pci__dss__v2.pdf*).

In this phase of the kill chain, one protective step includes analysis of the location of credentialed users in the network. For example, if the attackers were still using Fazio's stolen credentials, an analyst would have reason to be concerned if that credential was being used in an unrelated area of the Target network. That the attackers were still using Fazio's credentials when installing malware or moving through the Target network is unlikely, but the analysis could have still proven useful.

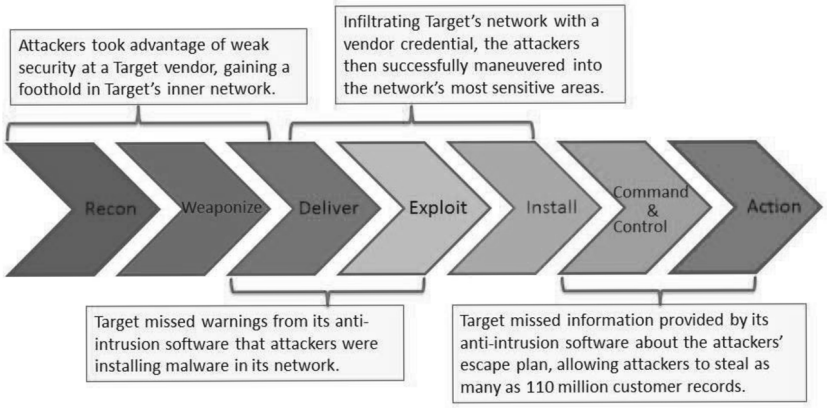
Another protective step at this phase would have been strong firewalls between Target's internal systems and the outside Internet (*e.g.,* routing traffic through a proxy) to help disrupt the attacker's command and control. Target could also have filtered or blocked certain Internet connections commonly used for command and control.

G. Actions on Objectives—Attacker Acts to Accomplish Data Exfiltration

The attackers transmitted the stolen data to outside servers—at least one of which was located in Russia—in plain text via FTP[52] (a standard method for transferring files) over the course of two weeks. At this phase of the kill chain, protective defensive steps could have included white listing approved FTP servers to which Target's network is allowed to upload data. For example, a white list could have dismissed connections between Target's network and Russia-based Internet servers. An analysis of data transmissions on Target's busy network may be like searching for a needle in a haystack, but an upload to a server in Russia presumably would have been flagged as suspicious if discovered.

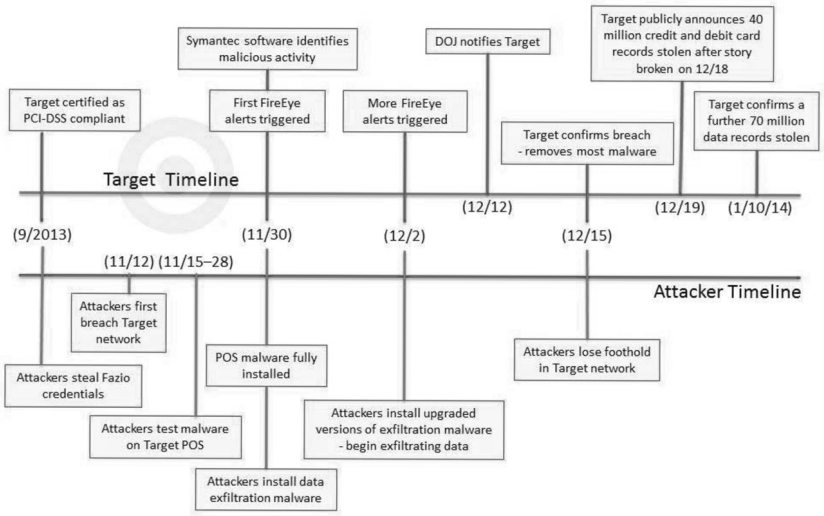
Target's FireEye software reportedly did detect the data exfiltration malware and decoded the destination of servers on which data for millions of stolen credit cards were stored for days at a time. Acting on this information could have stopped the exfiltration, not only at this last stage, but especially during the "delivery" step on the kill chain.

Figure 5 – Target's Possible Missed Opportunities



[52] McAfee, *McAfee Labs Threats Report Fourth Quarter 2013,* at 7 (2013) (online at *http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2013.pdf*).

Figure 6 – A Timeline of the Target Data Breach



The CHAIRMAN. And anybody who wants one of these is welcome to have it. I hope people at the press table have it.

It is increasingly frustrating to me that organizations are resisting the need to invest in their security systems. Target must be a clarion call to businesses, both large and small, that it is time to invest in some changes.

While I am disappointed that many companies have failed to take responsibility for their data security weaknesses, I am just as disappointed by Congress and our failure to create Federal standards for protecting consumer information. If you can imagine having stores in 45 or 35 states, and every state has different rules and regulations, it is just an impossible mess.

Recently, I put forth legislation that builds on the long, well-established history of the Federal Trade Commission and state attorneys general in protecting consumers from data breaches.

The bill set forth strong Federal consumer data security and breach notification standards by: one, directing the FTC to circulate rules requiring companies to adopt reasonable but strong security protocols; requiring companies to notify affected consumers in the wake of the breach—I mean, that should just be automatic; and authorizing both the FTC and state attorneys general to seek civil penalties for violations of that law.

For nearly a decade, we have had major data breaches at companies large and small. Millions of consumers have suffered the consequences. While Congress deserves its share of the blame for inaction, I am increasingly frustrated by industry's disingenuous attempts at negotiations.

So this is my message to the industry today: It is time to come to the table. Be willing to compromise. While I am willing to hear

their concerns about the legislation—my legislation or any other legislation—I am not willing to forfeit the basic protections that American consumers have a right to count on. And I will not.

Finally, I would be remiss if I did not publicly note that representatives from the company Snapchat declined my invitation to testify today. When people refuse to testify in front of this committee, my instincts, which may be skewed, are nevertheless that they are hiding something. In this instance, on this subject, I think it warrants closer scrutiny.

I call on my most distinguished good—I won't go through the usual drill.

[Laughter.]

STATEMENT OF HON. JOHN THUNE,
U.S. SENATOR FROM SOUTH DAKOTA

Senator THUNE. OK. Well, thank you, Chairman Rockefeller, for holding this afternoon's hearing on data breaches and protecting consumer information. Protecting consumers from identity theft, fraud, and financial harm is certainly a goal that all of us on this committee share.

I am glad that representatives from Target and the University of Maryland accepted our invitation to be here today to tell us of their recent and well-publicized breaches. While the forensic investigations into these incidents are still ongoing, it is clear that millions of individuals have unfortunately been affected.

I look forward to hearing about what lessons Target and the University of Maryland have learned from these breaches and what additional steps they are taking to prevent them in the future and to better safeguard individuals' personal information.

Yet data breaches clearly are not unique to Target and the University of Maryland. A data breach report from Verizon found that there were more than 600 confirmed data breach disclosures among private and government entities and at least 44 million compromised records in 2012 alone.

While we are here today primarily to discuss data breaches in the private sector, we can't forget that the U.S. Government also holds immense amounts of consumer financial data and personal information. It is estimated that the Federal Government spent more than $14.6 billion on IT security in Fiscal Year 2012, but it is not immune to cyber attacks and data breaches.

In 2012, Federal agencies reported more than 22,000 data breach incidents, a number that is more than double what was reported in 2009. In addition, a recent report by the Government Accountability Office, the government's watchdog, identified several instances where Federal agencies failed to notify affected individuals, even when the breach was determined to have a high risk of harm.

Breaches of personal information can affect individuals in many ways, ranging from the inconvenience of having a credit card replaced to the harm of identity theft, where a criminal runs up large debts or commits crimes in the victim's name.

When there is risk of real harm stemming from a breach, we need to make sure that consumers have the information they need to protect themselves. That is why I support a uniform Federal

breach notification standard to replace the patchwork of laws in 46 states and the District of Columbia.

A single Federal standard would ensure all consumers are treated the same with regard to notification of data breaches that might cause them harm. Such a standard would also provide consistency and certainty regarding timely notification practices, which benefits both consumers and businesses.

I also want to ensure that businesses appropriately secure information and are not burdened by outdated or ill-suited security requirements but, rather, are provided with the flexibility to develop effective and innovative tools to secure the information they are entrusted to protect.

For these reasons, I cosponsored Senate Bill 1193, the Data Security and Breach Notification Act of 2013, with Senator Toomey and a number of my colleagues on this committee. The bill would require companies possessing personal data to notify consumers in a timely manner if their information has been unlawfully taken.

Mr. Chairman, I know that you have also introduced legislation on this topic, and I look forward to working with you and our colleagues as we consider how best to promote the security of personal consumer information and ensure appropriate breach notification.

Of course, we should acknowledge that this issue is not a new one. The Committee reported data breach legislation in 2005 and again in 2007, but finding broad agreement on the path forward has proven difficult. We should heed the testimony of Mr. Wagner and not allow the perfect to become the enemy of the good.

Our recent experience advancing legislation on the role of the National Institute of Standards and Technology in the identification of voluntary best practices and standards for cybersecurity gives me reason for optimism. And I was pleased to see that several of the witnesses today have highlighted the good work done by NIST in that regard.

As we have noted in the past, legislation is also needed to enhance information-sharing of cyber threats, with liability protections. While not every data breach occurs because of a cyber attack, timely information-sharing of cyber threats is key to preventing and responding to cyber attacks, whether it is a breach of consumer data, theft of intellectual property, or an attack on critical infrastructure.

So I look forward to learning more about the new partnership between the merchant and financial associations that will focus on sharing more information on cyber threats and improving technology to protect consumers.

I also hope Visa and Target can elaborate on the work that they are doing to identify and prevent payment card fraud resulting from the recent breach so that the payment system is more secure and consumers are better protected.

I also look forward to hearing from Chairwoman Ramirez of the Federal Trade Commission about the work the agency is doing on enforcement and education to protect consumers from identity theft and fraud.

I also know that the Secret Service and the Federal Bureau of Investigation, in partnership with industry and government part-

ners, are working hard to detect and prosecute cyber criminals and fraudsters.

So, Mr. Chairman, I hope our witnesses can share their experiences, good or bad, working with Federal agencies on our shared goal of safeguarding consumers' personal information. And I want to thank you again for holding this hearing, and I look forward to hearing from our witnesses.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much, Senator Thune.

We are a very good combination. If you don't know that now, you will learn it.

Senator THUNE. It is true.

The CHAIRMAN. It is true. We both come from big states.

[Laughter.]

Senator THUNE. We are both tall people.

The CHAIRMAN. We are both tall people, that is right. And we both—and we love sports.

First, let's start with the Honorable Ramirez, Edith Ramirez, who is Chairwoman of the Federal Trade Commission.

And, once again, I issue the following words of comfort to you: Never fear that the National Gallery of Art is going to take you over. You are going to be there 1,000 years from now. Whether they will be or not, I don't know, but you will be.

[Laughter.]

STATEMENT OF HON. EDITH RAMIREZ, CHAIRWOMAN, FEDERAL TRADE COMMISSION

Ms. RAMIREZ. Thank you.

Chairman Rockefeller, Ranking Member Thune, and members of the Committee, I appreciate the opportunity to present the Federal Trade Commission's testimony on data security.

Under your leadership, Chairman Rockefeller, this committee has led critical efforts in Congress to protect consumers' privacy and data security. From the recent examination of the data-broker industry and its impact on consumers to proposing data security requirements for industry, you and the members of this committee have sought to advance the same goals as the FTC. And I want to thank you for your leadership.

As this committee is well aware, consumers' data is at risk. Recent data breaches remind us that hackers seek to exploit vulnerabilities in order to access and misuse consumers' data in ways that can cause serious harm to consumers and businesses.

These threats affect more than just payment card data. For example, breaches in recent years have also compromised Social Security numbers, account passwords, health data, and information about children. This occurs against the backdrop of identity theft, which has been the FTC's top consumer complaint for the last 14 years.

Today, I am here to reiterate the Commission's bipartisan call for the enactment of a strong Federal data security and breach notification law. Never has the need for legislation been greater. With reports of data breaches on the rise, Congress must act.

The FTC supports Federal legislation that would strengthen existing data security standards and require companies, in appro-

priate circumstances, to provide notification to consumers when there is a security breach. Reasonable security practices are critical to preventing data breaches and protecting consumers from ID theft and other harm. And when breaches do occur, notifying consumers helps them protect themselves from any harm that is likely to be caused by the misuse of their data.

Legislation should give the FTC authority to seek civil penalties where warranted to help ensure that FTC actions have an appropriate deterrent effect. In addition, enabling the FTC to bring cases against nonprofits, such as universities and health systems, which have reported a substantial number of breaches would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it.

Finally, APA rulemaking authority, like that used in the CAN–SPAM Act, would allow the Commission to ensure that as technology changes and the risks from the use of certain types of information evolve, companies would be required to give adequate protection to such data.

For example, whereas a decade ago it would have been difficult and expensive for a company to track an individual's precise location, smartphones have made this information readily available. And as the growing problem of child identity theft has brought to light in recent years, Social Security numbers alone can be combined with another person's information to steal an identity.

Using its existing authority, the FTC has devoted substantial resources to encourage companies to make data security a priority. The FTC has settled 50 cases against companies that we alleged put consumer data at risk.

In all these cases, the touchstone of the Commission's approach has been reasonableness. A company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.

The Commission has made clear that it does not require perfect security and that the fact that a breach occurred does not mean that a company has violated the law. As the Commission's case against the retailer TJX illustrates, the Commission's data security cases have alleged failures to implement basic, fundamental safeguards.

In 2007, TJX announced what was then one of the largest known data breaches. According to the FTC's subsequent complaint against TJX, a hacker obtained information from tens of millions of credit card and debit payment card information, as well as the personal information of approximately 455,000 consumers.

The FTC alleged that TJX engaged in a number of practices that, taken together, were unreasonable, such as allowing network administrators to use weak passwords, failing to limit wireless access to in-store networks, not using firewalls to isolate computers processing cardholder data from the Internet, and not having procedures to detect and prevent unauthorized access to its networks, such as procedures to update antivirus software.

In addition to our enforcement efforts, the Commission also undertakes policy initiatives to promote privacy and data security,

such as workshops on mobile security issues and child and senior ID theft. And for those consumers who may have been affected by recent breaches, the FTC has posted information online about steps they should take to protect themselves. The FTC also provides guidance to businesses about reasonable security practices.

Thank you for the opportunity to provide the Commission's views on data security. The FTC remains committed to promoting reasonable security for consumer data, and we look forward to continuing to work with the Committee and Congress on this critical issue.

Thank you.

[The prepared statement of Ms. Ramirez follows:]

PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

I. Introduction

Chairman Rockefeller, Ranking Member Thune, and members of the Committee, I am Edith Ramirez, Chairwoman of the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's testimony on data security.

Under your leadership, Chairman Rockefeller, this Committee has led critical efforts in Congress to protect consumers' privacy and data security. Throughout your tenure, the Committee has focused on a wide range of privacy and security concerns facing consumers in this increasingly interconnected economy. From the recent examination of the data broker industry and its impact on consumers;[2] to protecting our children's privacy as technology changes;[3] to promoting consumers' choices about online privacy;[4] to proposing baseline data security requirements for industry,[5] you and members of the Committee have shared the same goals as the Federal Trade Commission: to protect consumer privacy and promote data security in the private sector. The FTC thanks you for your leadership.

As this Committee is well aware, consumers' data is at risk. Recent publicly announced data breaches[6] remind us that hackers and others seek to exploit vulnerabilities, obtain unauthorized access to consumers' sensitive information, and potentially misuse it in ways that can cause serious harm to consumers as well as businesses. These threats affect more than payment card data; breaches reported in recent years have also compromised Social Security numbers, account passwords, health data, information about children, and other types of personal information.

Data security is of critical importance to consumers. If companies do not protect the personal information they collect and store, that information could fall into the wrong hands, resulting in fraud, identity theft, and other harm, along with a poten-

---

[1] This written statement presents the views of the Federal Trade Commission. My oral statements and responses to questions are my own and do not necessarily reflect the views of the Commission or of any other Commissioner.

[2] *See* Office of Oversight & Investigations Majority Staff Report, Senate Commerce Committee, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes* (Dec. 18, 2013), available at *http://www.commerce.senate.gov/public/?a=Files.Serve&File__id=bd5dad8b-a9e8–4fe9-a2a7-b17f4798ee5a.*

[3] *See, e.g.,* Press Release, *Rockefeller Says Modernized COPPA Rule Will Better Protect Children Online,* Dec. 19, 2012, available at *http://www.commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord__id=1a0ac4aa-bfbe-493e-a877-16035146562d&ContentType__id=77eb43da-aa94-497d-a73f-5c951ff72372&Group__id=4b968841-f3e8-49da-a529-7b18e32fd69d&MonthDisplay=12&YearDisplay=2012.*

[4] *See, e.g.,* Hearing Before the Committee on Commerce, Science, and Transportation, U.S. Senate, *A Status Update on the Development of Voluntary Do-Not-Track Standards,* Apr. 24, 2013, available at *http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord__id=1cf8fb1a-fb0b-4bf1-958b-1ea3c443a73c&ContentType__id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group__id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=4&YearDisplay=2013.*

[5] *See, e.g.,* Press Release, *The Data Security & Breach Notification Act,* Jan. 30, 2014, available at *http://www.commerce.senate.gov/public/index.cfm?p=Legislation&ContentRecord__id=40e0ad58-866a-41ea-bf00–750c17e1ee3a.*

[6] *See* Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow,* N.Y. Times, Jan. 10, 2014, available at *http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html* (discussing recently-announced breaches involving payment card information by Target and Neiman Marcus); Nicole Perlroth, *Michaels Stores Is Investigating Data Breach,* N.Y. Times, Jan. 25, 2014, available at *http://www.nytimes.com/2014/01/26/technology/michaels-stores-is-investigating-data-breach.html* (announcement of potential security breach involving payment card information).

tial loss of consumer confidence in the marketplace. As one example, the Bureau of Justice Statistics estimates that 16.6 million persons—or 7 percent of all U.S. residents ages 16 and older—were victims of identity theft in 2012.[7]

As the Nation's leading privacy enforcement agency, the Commission has undertaken substantial efforts for over a decade to promote data security and privacy in the private sector through civil law enforcement, education, and policy initiatives. The Commission is here today to reiterate its longstanding, bipartisan call for enactment of a strong Federal data security and breach notification law. Never has the need for legislation been greater. With reports of data breaches on the rise, and with a significant number of Americans suffering from identity theft, Congress must act. This testimony provides an overview of the Commission's data security efforts, and restates the FTC's support for data security legislation.

II. The Commission's Data Security Program

A. Law Enforcement

The Commission enforces several statutes and rules that impose obligations upon businesses to protect consumer data. The Commission's Safeguards Rule, which implements the Gramm-Leach-Bliley Act ("GLB Act"), for example, provides data security requirements for non-bank financial institutions.[8] The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,[9] and imposes safe disposal obligations on entities that maintain consumer report information.[10] The Children's Online Privacy Protection Act (COPPA) requires reasonable security for children's information collected online.[11] Reasonableness is the foundation of the data security provisions of each of these laws.

In addition, the Commission enforces the proscription against unfair or deceptive acts or practices in Section 5 of the FTC Act.[12] A company acts deceptively if it makes materially misleading statements or omissions.[13] Using its deception authority, the Commission has settled more than 30 matters challenging companies' express and implied claims about the security they provide for consumers' personal data. Further, a company engages in unfair acts or practices if its data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition.[14] The Commission has settled more than 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice.[15]

The FTC conducts its data security investigations to determine whether a company's data security measures are reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities. The Commission's 50 settlements with businesses that it charged with failing to provide reasonable protections for consumers' personal information have halted harmful data security practices; required companies to accord strong protections for consumer data; and raised awareness about the risks to data, the need for reasonable and appropriate security, and the types of security failures that raise concerns.[16] And they have addressed the risks to a wide variety of consumer data, such as Social Security numbers, health data, data about children, credit card information, bank account information, usernames, and passwords, in a broad range of sectors and platforms.

In each of these cases, the Commission has examined a company's practices as a whole and challenged alleged data security failures that were multiple and systemic. Through these settlements, the Commission has made clear that reasonable

---

[7] *See* Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), available at *http://www.bjs.gov/content/pub/pdf/vit12.pdf*.

[8] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).

[9] 15 U.S.C. § 1681e.

[10] *Id.* at § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

[11] 15 U.S.C. §§ 6501–6506; *see also* 16 C.F.R. Part 312 ("COPPA Rule").

[12] 15 U.S.C. § 45(a).

[13] *See* Federal Trade Commission Policy Statement on Deception, appended to *Cliffdale Assocs., Inc.,* 103 F.T.C. 110, 174 (1984).

[14] *See* Federal Trade Commission Policy Statement on Unfairness, appended to *Int'l Harvester Co.,* 104 F.T.C. 949, 1070 (1984) ("FTC Unfairness Statement").

[15] Some of the Commission's data security settlements allege both deception and unfairness, as well as allegations under statutes such as the FCRA, GLB Act, and COPPA.

[16] *See* Commission Statement Marking the FTC's 50th Data Security Settlement, Jan. 31, 2014, available at *http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf*.

and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; that the Commission does not require perfect security; and that the mere fact that a breach occurred does not mean that a company has violated the law.

In its most recent case, the FTC entered into a settlement with GMR Transcription Services, Inc., a company that provides audio file transcription services for its clients—which includes health care providers.[17] According to the complaint, GMR relies on service providers and independent typists to perform this work, and conducts its business primarily over the Internet by exchanging audio files and transcripts with customers and typists by loading them on a file server. As a result of GMR's alleged failure to implement reasonable and appropriate security measures or to ensure its service providers also implemented reasonable and appropriate security, at least 15,000 files containing sensitive personal information—including consumers' names, birthdates, and medical histories—were available to anyone on the Internet. The Commission's order prohibits GMR from making misrepresentations about privacy and security, and requires the company to implement a comprehensive information security program and undergo independent audits for the next 20 years.

The FTC also recently announced a case against TRENDnet, which involved a video camera designed to allow consumers to monitor their homes remotely.[18] The complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring. Although TRENDnet claimed that the cameras were "secure," they had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet address. This resulted in hackers posting 700 consumers' live feeds on the Internet. Under the FTC settlement, TRENDnet must maintain a comprehensive security program, obtain outside audits, notify consumers about the security issues and the availability of software updates to correct them, and provide affected customers with free technical support for the next two years.

The FTC also has brought a number of cases alleging that unreasonable security practices allowed hackers to gain access to consumers' credit and debit card information, leading to many millions of dollars of fraud loss.[19] The Commission's settlement with TJX provides a good example of the FTC's examination of reasonableness in the data security context.[20] According to the complaint, TJX engaged in a number of practices that, taken together, failed to reasonably protect consumer information. Among other things, it (1) failed to implement measures to limit wireless access to its stores, allowing a hacker to connect wirelessly to its networks without authorization; (2) did not require network administrators to use strong passwords; (3) failed to use a firewall or otherwise limit access to the Internet on networks processing cardholder data; and (4) lacked procedures to detect and prevent unauthorized access, such as by updating antivirus software and responding on security warnings and intrusion alerts. As a result, a hacker obtained tens of millions of credit and debit payment cards, as well as the personal information of approximately 455,000 consumers who returned merchandise to the stores. As this matter illustrates, the FTC's approach to reasonableness is process-based rather than a checklist of specific technologies or tools. The Commission looks to see whether companies have a general framework in place to develop, implement, and maintain appropriate safeguards that is reasonable and appropriate in light of the sensitivity and volume of the data it holds, the size and complexity of its data operations, and the cost of available tools.

B. Policy Initiatives

The Commission also undertakes policy initiatives to promote privacy and data security. For example, the FTC hosts workshops on business practices and technologies affecting consumer data. The FTC is in the midst of hosting its Spring Pri-

---

[17] *GMR Transcription Servs., Inc.,* Matter No. 112–3120 (F.T.C. Dec. 16, 2013) (proposed consent order), available at *http://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it.*

[18] *TRENDnet, Inc.,* No. C–4426(F.T.C. Jan. 16, 2014) (consent order), available at *http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.*

[19] *See, e.g., Dave & Buster's, Inc.,* No. C–4291 (F.T.C. May 20, 2010) (consent order), available at *http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2010/06/dave-busters-incin-matter; DSW, Inc.,* No. C–4157 (F.T.C. Mar. 7, 2006) (consent order), available at *http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2006/03/dsw-incin-matter; BJ's Wholesale Club, Inc.,* No. C–4148 (F.T.C. Sept. 20, 2005) (consent order), available at *http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2005/09/bjs-wholesale-club-inc-matter.*

[20] *The TJX Cos., Inc.,* No. C–4227 (F.T.C. July 29, 2008) (consent order), available at *http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2008/08/tjx-companies-inc-matter.*

vacy Series to examine the privacy implications of a number of new technologies in the marketplace.[21] The first seminar, held in February, included a panel of industry, technical experts, and privacy advocates and examined the privacy and security implications of mobile device tracking, where retailers and other companies rely on technology that can reveal information about consumers' visits to and movements within a location.[22]

In November, the FTC held a workshop on the phenomenon known as the "Internet of Things"—*i.e.,* Internet-connected refrigerators, thermostats, cars, and other products and services that can communicate with each other and/or consumers.[23] The workshop brought together academics, industry representatives, and consumer advocates to explore the security and privacy issues from increased connectivity in everyday devices, in areas as diverse as smart homes, connected health and fitness devices, and connected cars. Commission staff is developing a report on privacy and security issues raised at the workshop and in the public comments.

And last June, the Commission hosted a public forum on mobile security issues, including potential threats to U.S. consumers and possible solutions to them.[24] As the use of mobile technology increases at a rapid rate and consumers take advantage of the technology's benefits in large numbers, it is important to address threats that exist today as well as those that may emerge in the future. The forum brought together technology researchers, industry members and academics to explore the security of existing and developing mobile technologies and the roles various members of the mobile ecosystem can play in protecting consumers from potential security threats.

C. Consumer Education and Business Guidance

The Commission is also committed to promoting better data security practices through consumer education and business guidance. On the consumer education front, the Commission sponsors OnGuard Online, a website designed to educate consumers about basic computer security.[25] OnGuard Online and its Spanish-language counterpart, Alerta en Línea,[26] average more than 2.2 million unique visits per year. Also, for consumers who may have been affected by the recent Target and other breaches, the FTC posted information online about steps they should take to protect themselves.[27]

The Commission directs its outreach to businesses as well to provide education about applicable legal requirements and reasonable security practices. For example, the FTC widely disseminates its business guide on data security,[28] along with an online tutorial based on the guide.[29] These resources are designed to provide a variety of businesses—and especially small businesses—with practical, concrete advice as they develop data security programs and plans for their companies. First, companies should know what consumer information they have and what personnel or third parties have, or could have, access to it. Understanding how information moves into, through, and out of a business is essential to assessing its security vulnerabilities. Second, companies should limit the information they collect and retain based on their legitimate business needs, so that needless storage of data does not create unnecessary risks of unauthorized access to the data. Third, businesses should protect the information they maintain by assessing risks and implementing

---

[21] Press Release, *FTC to Host Spring Seminars on Emerging Consumer Privacy Issues,* Dec. 2, 2013, available at *http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues.*

[22] *See* Spring Privacy Series, *Mobile Device Tracking,* Feb. 19, 2014, available at *http://www.ftc.gov/news-events/events-calendar/2014/02/spring-privacy-series-mobile-device-tracking.*

[23] FTC Workshop, *Internet of Things: Privacy & Security in a Connected World* (Nov. 19, 2013), available at *http://www.ftc.gov/bcp/workshops/internet-of-things/.*

[24] FTC Workshop, *Mobile Security: Potential Threats and Solutions* (June 4, 2013), available at *http://www.ftc.gov/bcp/workshops/mobile-security/.*

[25] *See http://www.onguardonline.gov.*

[26] *See http://www.alertaenlinea.gov.*

[27] *See* Nicole Vincent Fleming, *An Unfortunate Fact About Shopping,* FTC Consumer Blog, *http://www.consumer.ftc.gov/blog/unfortunate-fact-about-shopping* (Jan. 27, 2014); Nicole Vincent Fleming, *Are you affected by the recent Target hack?,* FTC Consumer Blog, *https://www.consumer.ftc.gov/blog/are-you-affected-recent-target-hack.* In addition to these materials posted in response to recent breaches, the FTC has long published a victim recovery guide and other resources to explain the immediate steps identity theft victims should take to address the crime; how to obtain a free credit report and correct fraudulent information in credit reports; how to file a police report; and how to protect their personal information. *See http://www.consumer.ftc.gov/features/feature-0014-identity-theft.*

[28] *See Protecting Personal Information: A Guide for Business,* available at *http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business.*

[29] *See Protecting Personal Information: A Guide for Business (Interactive Tutorial),* available at *http://business.ftc.gov/multimedia/videos/protecting-personal-information.*

protections in certain key areas—physical security, electronic security, employee training, and oversight of service providers. Fourth, companies should properly dispose of information that they no longer need. Finally, companies should have a plan in place to respond to security incidents, should they occur.

The Commission has also released articles directed towards a non-legal audience regarding basic data security issues for businesses.[30] For example, because mobile applications ("apps") and devices often rely on consumer data, the FTC has developed specific security guidance for mobile app developers as they create, release, and monitor their apps.[31] The FTC also creates business educational materials on specific topics—such as the risks associated with peer-to-peer ("P2P") file-sharing programs and companies' obligations to protect consumer and employee information from these risks[32] and how to properly secure and dispose of information on digital copiers.[33]

III. Data Security Legislation

The FTC supports Federal legislation that would (1) strengthen its existing authority governing data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.[34] Reasonable and appropriate security practices are critical to preventing data breaches and protecting consumers from identity theft and other harm. Where breaches occur, notifying consumers helps them protect themselves from any harm that is likely to be caused by the misuse of their data. For example, in the case of a breach of Social Security numbers, notifying consumers will enable them to request that fraud alerts be placed in their credit files, obtain copies of their credit reports, scrutinize their monthly account statements, and take other steps to protect themselves. And although most states have breach notification laws in place, having a strong and consistent national requirement would simplify compliance by businesses while ensuring that all consumers are protected.

Legislation in both areas—data security and breach notification—should give the FTC the ability to seek civil penalties to help deter unlawful conduct, jurisdiction over non-profits, and rulemaking authority under the Administrative Procedure Act. Under current laws, the FTC only has the 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.[35] 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. Likewise, enabling the FTC to bring cases against non-profits[36] would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it.[37]

Finally, rulemaking authority under the Administrative Procedure Act would enable the FTC in implementing the legislation to respond to changes in technology.

---

[30] *See generally http://www.business.ftc.gov/privacy-and-security/data-security.*

[31] *See Mobile App Developers: Start with Security* (Feb. 2013), available at *http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.*

[32] *See Peer-to-Peer File Sharing: A Guide for Business* (Jan. 2010), available at *http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business.*

[33] *See Copier Data Security: A Guide for Business* (Nov. 2010), available at *http://business.ftc.gov/documents/bus43-copier-data-security.*

[34] *See, e.g.,* Prepared Statement of the Federal Trade Commission, "Privacy and Data Security: Protecting Consumers in the Modern World," Before the Senate Committee on Commerce, Science, and Transportation, 112th Cong., June 29, 2011, available at *http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-privacy-and-data-security-protecting-consumers-modern/110629privacytestimonybrill.pdf;* Prepared Statement of the Federal Trade Commission, "Data Security," Before Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce, 112th Cong., June 15, 2011, available at *http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110615datasecurity house.pdf;* FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), available at *http://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf;* President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), available at *http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021 taskforcereport.pdf.*

[35] The FTC can also seek civil penalties for violations of administrative orders. 15 U.S.C. § 45(*l*).

[36] Non-profits are generally outside the FTC's jurisdiction. 15 U.S.C. §§ 44 & 45(a).

[37] A substantial number of reported breaches have involved non-profit universities and health systems. *See* Privacy Rights Clearinghouse Chronology of Data Breaches (listing breaches including breaches at non-profits, educational institutions, and health facilities), available at *http://www.privacyrights.org/data-breach/new.*

For example, whereas a decade ago it would be incredibly difficult and expensive for a company to track an individual's precise geolocation, the explosion of mobile devices has made such information readily available. And, as the growing problem of child identity theft has brought to light in recent years, a child's Social Security number alone can be used in combination with another person's information, such as name or date of birth, in order to commit identity theft.[38] Rulemaking authority would allow the Commission to ensure that as technology changes and the risks from the use of certain types of information evolve, companies would be required to give adequate protection to such data.

IV. Conclusion

Thank you for the opportunity to provide the Commission's views on data security. The FTC remains committed to promoting reasonable security for consumer data and we look forward to continuing to work with the Committee and Congress on this critical issue.

The CHAIRMAN. Thank you very much.

We are very honored to have the President of the University of Maryland here, Dr. Wallace Loh.

Thank you for taking the time, sir. I am sure that testifying before a congressional committee must be something you look forward to.

[Laughter.]

STATEMENT OF DR. WALLACE D. LOH, PRESIDENT, UNIVERSITY OF MARYLAND

Mr. LOH. Thank you, Chairman Rockefeller and Ranking Member Thune and members of the Commerce Committee. I spend most of my time testifying before the Maryland legislature, so I hope that is good preparation for today.

On February 18, after a major snowstorm paralyzed this region that weekend—that was President's Day weekend—we had a very sophisticated cyber attack. Somebody basically uploaded a Trojan horse into the website of one of our colleges. This website, about 10 years old, invites the uploading of photographs, but instead they uploaded this malware.

Once they got into that website, they were able to pierce into central systems, and they were actually coding in order to do that. And they were able to get to the directory of the management of IT, find their passwords, and then change these to issue orders.

So they downloaded 310,000 names, Social Security numbers, university IDs. They intentionally left out photographs, so on and so forth, that kind of information, because that would have slowed the exfiltration of the data. And they did it using Tor (software allowing online anonymity), which means that they were able to hide the point of origin of the attack.

It turns out, because we have never been hacked before, we were just flying by the seat of our pants.

And it just so happens that we did exactly what your bill proposes to do. With regard to notification, we announced it within 24 hours. Within 24 hours, we also contacted credit rating agencies, set up call centers, and notified the entire university community, all 38,000 students, all 12,000 faculty and staff. And within 4 or 5 days, we e-mailed, called, sent letters to everybody else, a total

[38] FTC Workshop, *Stolen Futures: A Forum on Child Identity Theft* (July 12, 2011), available at *http://www.ftc.gov/news-events/events-calendar/2011/07/stolen-futures-forum-child-identity-theft.*

of 310,000 because some of them are alumni going back for 20 years.

The reason, of course, is that what they got were the university IDs, but, remember, until about the year 2000, every university in this country was using Social Security numbers as identification. And we have thousands of databases, and they just took that one database where we had both the university ID and the Social Security.

So, in terms of notification, not only did we notify, we offered to pay 5 years of protection—credit card protection—to all the affected parties. That is approximately $20 per person, multiplied by 310,000 over 5 years. To date, approximately 60,000 have signed up for this free 5-year protection.

What we also did in terms of data security is very much along the lines of what your bill has proposed. What we have done immediately was to purge all of the unnecessary data. We have purged approximately 225,000 names from our records. We didn't purge all of them because you need Social Security numbers for a student's financial aid, for payroll purposes. We are trying to reinforce the security for those Social Security numbers that remain.

So what we are trying to do, with the help of the FBI, the Secret Service, private security companies, are two things. One is to strengthen perimeter defenses and hire firms to do periodic, on a regular basis, penetration testing. And then, also, assuming they still are able to penetrate, because people who play offense will always be one step ahead of those who are playing defense, is to tighten the security around the sensitive databases.

So what we have done in just one month is we have migrated almost all of our websites to the cloud. We have purged, as I said, lots of information. We have engaged firms to do penetration testing. We have isolated information that is sensitive from information that is less sensitive and so on. And the cost is very, very high.

Let me just conclude by saying that 3 weeks later we had another major intrusion. Fortunately, of course, the FBI was working with us. All I can say at this point is that within 36 hours the FBI was able to identify and, in their parlance, successfully mitigate that intrusion. No data was released, except that the data of one individual was posted on the Web for everybody to see just because the intruder wanted everybody to know that they were successful.

So that is where we are at. And thank you very much for all of your work in terms of requiring data notification and data security. This is a very important issue.

And I will conclude by saying this. Security in a university is very different than data security in the private sector, because a university is an open organization. There are many points of access because it is all about the free exchange of information. By definition, that is the Internet. In the private sector, you can centralize cybersecurity. You cannot do that at a university.

So we have to find that proper balance between security and access. And that is the challenge for all universities because, as you know, in the past 12 months 50 universities have had major data breaches, and not all of them even bothered to report it.

[The prepared statement of Mr. Loh follows:]

PREPARED STATEMENT OF DR. WALLACE D. LOH, PRESIDENT,
UNIVERSITY OF MARYLAND

My name is Wallace Loh and I am the President of the University of Maryland. From its beginnings as a small, land-grant institution to its current status as a major presence in higher education, the University of Maryland has a long and distinguished history of excellence and innovation, evidenced by being #38 in the 2013 Academic Ranking of World Universities.

I am grateful for this opportunity to discuss an issue that is not only important to the higher education community but to all of us who participate in online activities on a daily basis. As the state's flagship institution, the University of Maryland has 37,000 students, 12 colleges and schools, 9000 faculty and staff, and an annual $1.7 billion operation budget. To safeguard such a large and complex operation, we recently doubled the number of our IT security engineers and analysts as well as our investment in top-end security tools. However, as our recent data breach reveals, more remains to be done.

On February 18, 2014, the University of Maryland was the victim of a sophisticated computer security attack that exposed records containing personal information of faculty, staff, students and affiliated personnel from the College Park and Shady Grove campuses. Fortunately, no financial, academic, health or contact (phone and address) information was compromised, but we are not taking any chances. I have ordered five years of credit protection services at no cost to every person affected by this breach. This is above and beyond the protection measures taken by other organizations and institutions, and so far nearly 30,000 persons affected by the breach have registered, which is also well ahead of projections. In addition, all sensitive records in the breached database that are no longer required have been removed.

As evidence of our efforts, the University of Maryland IT security staff, working with the U.S. Secret Service, the FBI, and the campus police, mitigated another intrusion which occurred on Saturday, March 15, 2014. There was no public release of any information and no damage to the institution, except for the release of personal data of one senior university official.

Our experience highlights a serious and growing threat. In fact, in the past decade, some 20 large universities across the country have also reported major data breaches. Fortunately, there are steps that can be taken to minimize our risk and vulnerability.

Over the past month, the University of Maryland has handled the situation in a deliberate and thorough manner, working with computer forensic investigators to determine how our sophisticated, multi-layered security defenses were bypassed, to track down the perpetrators, and most importantly to ensure there is no repeat of these intrusions. The steps we are taking now should serve as both a warning and a model for other institutions.

First, many university databases were created years ago when the environment for cyber threats was different. Consequently, they need to be explored, updated and secured. A comprehensive review of all personal information across all databases is underway, which has already led to the removal of all sensitive records in the breached database that are no longer required. Second, to maintain protection, universities should perform penetration tests of security defense on an ongoing basis to seal any possible technological gaps. At the moment, we are evaluating cyber security consulting firms that can assist with this process. Finally, there must be an appropriate balance between centralized (University-operated) versus decentralized (unit-operated) IT systems. Technical fixes must be reflected in policy changes to ensure that safeguards at central and local levels are equally robust and tightly coordinated. This includes examining national cybersecurity policies, procedures and best practices. The University of Maryland is performing each of these steps and recommends that other universities follow suit. And while such changes may be pricey, being proactive in safeguarding sensitive information is worth the investment.

To execute this threefold mission, I have formed an 18-member Task Force on Cybersecurity. The Task Force includes experts from our campus, including members from our Maryland Cybersecurity Center. It also includes students since their perspective is unique and essential. The first meeting of the Task Force took place March 12 and I have charged them to complete an investigation and submit recommendations to me by June 12. The Task Force has the full support of my office and the resources it needs to complete its task. I will take all necessary actions based on the Task Force's recommendations and the results of the forensic analysis now underway.

Concurrently, the University IT staff with the support of outside consultants are working virtually non-stop to protect better the vast information systems in our network that are accessible to students, faculty, staff and others. In the past month, they have identified and closed the pathways utilized in the February 18, 2014, breach and the incursion on March 15, 2014, changed the passwords for all databases and applications, and conducted an initial audit to detect vulnerabilities in individual websites within web hosting environments. Plans have also been accelerated to migrate web hosting to a more secure environment.

Equally important, it is not enough to rely on others to defend against cyber threats. Each of us must do our part and take reasonable steps to ensure our own information security. Therefore, the University of Maryland will also present a series of identity theft seminars to our students, faculty, staff and alumni. These seminars, which will also be recorded and made available online for viewing at a later time, will feature Jeff Karberg from the Maryland Attorney General's Identity Theft Unit.

It is clear that there is no impregnable barrier against every cyber-attack. There is an arms race between hackers playing offense and universities playing defense. Nonetheless, as the threat evolves, so can we. It will require higher investments in cyber security and greater diligence on our part, but as we become more adept at defense, we will inevitably create a good offense, and cyber criminals will have to be the ones who are worried.

Thank you.

WALLACE D. LOH

The CHAIRMAN. Excellent testimony, and I thank you very much.

Mr. John Mulligan is Executive Vice President and Chief Financial Officer of the Target Corporation.

We welcome you.

STATEMENT OF JOHN J. MULLIGAN, EXECUTIVE VICE PRESIDENT AND CHIEF FINANCIAL OFFICER, TARGET CORPORATION

Mr. MULLIGAN. Good afternoon, Chairman Rockefeller, Ranking Member Thune, and members of the Committee. My name is John Mulligan, and I am the Executive Vice President and Chief Financial Officer of Target. It is a pleasure to be with you here today.

As you know, Target experienced a data breach resulting from a criminal attack on our systems. Let me begin by once again reiterating how deeply sorry we are for the impact this incident has had on our guests, your constituents.

Our top priority is always taking care of our guests. They should feel confident about shopping at Target. We work hard to protect information about them, but the reality is we experienced a data breach. Our guests expect more, and we are working hard to do better. We know this has shaken their confidence, and we intend to earn it back.

My written statement provides additional details about the breach and Target's response. Like you, we are asking hard questions about whether we could have taken different actions before the breach was discovered that would have resulted in different outcomes.

In particular, we are focused on what information we had that could have alerted us to the breach earlier, whether we had the right personnel in the right positions, and ensuring that decisions related to operational and security matters were sound. We are working quickly to answer these questions.

This afternoon, I would like to provide an update since I last testified, including the actions we are taking to further strengthen our security and potential policy solutions we support.

From the outset, our response to the breach has been focused on supporting our guests and taking action to protect them against constantly evolving cyber threats. We are taking a hard look at security across our network.

While we don't know everything yet, we have initiated the following steps to further protect our perimeter and better secure our data: We are enhancing our security systems. We are increasing segmentation of key portions of our network. We have accelerated the installation of additional anti-malware tools. And we are hardening our network perimeter by expanding two-factor authentication.

Earlier this month, Target became the first retailer to join the Financial Services Information Sharing and Analysis Center. The center shares critical information and facilitates detection, prevention, and response to cyber attacks and fraud activity.

We are accelerating our $100 million investment in the adoption of chip technology because we believe it is critical to enhancing consumer protection. We have already installed approximately 10,000 chip-enabled devices in Target stores and expect to complete this installation in all Target stores by September, 6 months ahead of schedule. We also expect to begin to issue and accept chip-enabled cards by early 2015.

We have offered one year of free credit monitoring and identity theft protection to anyone who has ever shopped at our U.S. Target stores. And we have informed our guests that they have zero liability for any fraudulent charges on their cards arising from this incident.

We believe that responsible policy measures can help further enhance security for our guests and all consumers. Mr. Chairman, I know that you and other members of the Committee have introduced legislation designed to enhance data security. Although I am not a policy expert, I have discussed the principles of your bill with our team. We agree that a uniform standard would help provide clarity and predictability to consumer notifications. While the standard would be uniform, we would support continued state attorneys general enforcement.

We also believe that data security standards, if appropriately structure by the Federal Trade Commission, could provide additional protection for consumers. We have learned that even robust security can't completely shield a company from a criminal breach. However, the more that data security can be improved across the economy, the better protected consumers will be.

For many years, Target has invested significant capital and resources in technology, personnel, and processes. Prior to the data breach, we had in place multiple layers of protection and continually made enhancements to meet evolving threats. And in September 2013, our systems were certified compliant with Payment Card Industry data security standards, meaning that we met approximately 300 independent requirements of the assessment.

Yet the reality is that criminals breached our system. To prevent breaches like this from happening again, none of us can go it alone. All businesses and their customers are facing frequent and increasingly sophisticated attacks by cyber criminals. Protecting American

consumers is a shared responsibility, and Target remains committed to being part of that solution.

Senators, I want to once again say to you and to our guests how sorry we are this happened. We are committed to getting things right.

Thank you.

[The prepared statement of Mr. Mulligan follows:]

PREPARED STATEMENT OF JOHN MULLIGAN, EXECUTIVE VICE PRESIDENT AND CHIEF FINANCIAL OFFICER, TARGET

I. Introduction

Good afternoon Chairman Rockefeller, Ranking Member Thune, and Members of the Committee. My name is John Mulligan and I am the Executive Vice President and Chief Financial Officer of Target. I appreciate the opportunity to be here today to discuss important issues surrounding data breaches and cybercrime.

As you know, Target experienced a data breach in late 2013 resulting from a criminal attack on our systems. Let me reiterate how deeply sorry we are for the impact this incident has had on our guests—your constituents. Our top priority is taking care of our guests. They should feel confident about shopping at Target. We work hard to protect their information. But the reality is we experienced a data breach. Our guests expect more and we are working hard to do better. We know this has shaken their confidence and we intend to earn it back.

We are asking hard questions about whether we could have taken different actions before the breach was discovered that would have resulted in different outcomes. In particular, we are focused on what information we had that could have alerted us to the breach earlier; whether we had the right personnel in the right positions; and ensuring that decisions related to operational and security matters were sound. We are working diligently to answer these questions.

This afternoon, I'd like to provide an update since I last testified, including actions we are taking to further strengthen our security and potential policy solutions we support. Because the government's investigation regarding the intruders remains active and ongoing, I may not be able to provide specifics on certain matters. We continue to work closely with the U.S. Secret Service and the U.S. Department of Justice—to help them bring to justice the criminals who perpetrated this wide-scale attack on Target, American business and consumers.

II. What We Know

We are further strengthening our data security based on learnings from an end-to-end review of our systems. We are not finished with that review, and additional facts may affect our findings, but we are certainly developing a clearer picture of events and want to share with you some key facts we have learned.

Like any large business, we log a significant number of technology activities in our system—more than 1 billion on average each day. These activities range from relatively insignificant, such as a team member logging onto a laptop, to more significant, such as removal of a virus from a computer. Using technology tools, those activities are narrowed to a few hundred events that are surfaced to the professionals staffing our Security Operations Center (SOC). As a result of their review of these events, dozens of cases are opened daily for additional assessment.

It appears that intruders entered our system on November 12. We now believe that some intruder activity was detected by our computer security systems, logged and surfaced to the SOC and evaluated by our security professionals. With the benefit of hindsight and new information, we are now asking hard questions regarding the judgments that were made at that time and assessing whether different judgments may have led to different outcomes.

We believe that the intruders initially obtained an HVAC vendor's credentials to access the outermost portion of our network. We are still investigating how the intruders were able to move through the system using higher-level credentials to ultimately place malware on Target's point-of-sale registers. The malware appears to have been designed to capture payment card data from the magnetic strip of credit and debit cards prior to encryption within our system.

On the evening of December 12, we were notified by the Justice Department of suspicious activity involving payment cards used at Target stores. We immediately started our internal investigation.

On December 13, we met with the Justice Department and Secret Service. On December 14, we engaged an outside team of experts to lead a thorough forensic investigation.

On December 15, we confirmed that criminals had infiltrated our system, installed malware on our point-of-sale network and potentially stolen guest payment card data. That same day, we removed the malware from virtually all registers in our U.S. stores.

Over the next two days, we began notifying the payment processors and card networks, preparing to publicly notify our guests, and equipping call centers and stores with the necessary information and resources to address our guests' concerns.

Our actions leading up to our public announcement on December 19—and since—have been guided by the principle of serving our guests. We moved quickly to share accurate and actionable information with the public. When we announced the intrusion on December 19, we used multiple forms of communication, including a mass-scale public announcement, e-mail, prominent notices on our website, and social media.

Additionally, when we subsequently confirmed the theft of certain personal data, we used various channels of communication to notify our guests on January 10.

The breach affected two types of data: payment card data, which affected approximately 40 million guests, and certain personal data, which affected up to 70 million guests. The theft of the payment card data affected guests who shopped at our U.S. stores from November 27 through December 18. The theft of personal data included name, mailing address, phone number or e-mail address, and in many cases, it was partial in nature.

It is difficult to develop an accurate assessment of overlap between these two types of data, due in part to the partial nature of the information related to the file of 70 million individuals. Our analysis indicates there is an overlap of at least 12 million guests in the two populations, and likely more.

III. Protecting Our Guests

From the outset, our response to the breach has been focused on supporting our guests and taking action to further protect them against constantly evolving cyber threats. We are taking a hard look at security across the network. While we don't know everything yet, we have initiated the following steps to further protect our perimeter and better secure our data:

Segmentation. We are increasing the segmentation and separation of key portions of our network by enhancing the protections provided by the firewalls we have in place to limit unauthorized traffic. This is about making it more difficult to move across our network.

Whitelisting. We continue to strengthen our anti-virus tools, and accelerated the installation of a whitelisting solution on our registers. Whitelisting protects guests by detecting malicious applications and stopping them from running on our registers and gives us another tool to prevent malware from taking root and spreading in our environment. This is about limiting what can run on our network.

Authentication. We are strengthening our network perimeter by expanding two-factor authentication for entry into the system. This is about double locking the door.

Beyond these technology responses, we need to ensure the right people, with the right experience, are in the right place. That's why we are also taking a hard look at our organization, with the intention of bolstering our information security structure and practices.

- Earlier this month, Target became the first retailer to join the Financial Services Information Sharing and Analysis Center (FS–ISAC), an initiative developed by the financial services industry to help facilitate the detection, prevention, and response to cyber attacks and fraud activity. Target was eligible to join the organization because of its financial operations. During my testimony to Congress in February, I stressed Target's commitment to more coordinated information sharing with law enforcement and others fighting cyber threats, in order to help make our company, partners and guests more secure. Joining the FS–ISAC underscores Target's position that the retail and financial industries have a shared responsibility to collaborate and strengthen protection for American consumers.
- We are accelerating our $100 million investment in the adoption of chip technology because we believe it is critical to enhancing consumer protections. We have already installed approximately 10,000 chip-enabled payment devices in

Target stores and expect to complete the installation in all Target stores by this September, six months ahead of schedule. We also expect to begin to issue chip-enabled Target REDcards and accept all chip-enabled cards by early 2015. As a founding member and steering committee member of the EMV Migration Forum, we will continue to lead the adoption of these technologies across the payment ecosystem.

- We continue to reissue new Target credit or debit cards immediately to any guest who requests one.
- We continue to offer one year of free credit monitoring and identity theft protection to anyone who has ever shopped at our U.S. Target stores. This protection includes a free credit report, daily credit monitoring, identity theft insurance and unlimited access to personalized assistance from a fraud resolution agent.
- We have informed our guests that they have zero liability for fraudulent charges on their cards arising from this incident. To ensure our guests are protected, we continue to encourage them to monitor their accounts and promptly alert either Target or their issuing bank, as appropriate, of any suspicious activity.

Moving Forward

For many years, Target has invested significant capital and resources in security technology, personnel and processes. Prior to the data breach, we had in place multiple layers of protection, including firewalls, malware detection software, intrusion detection and prevention capabilities, and data loss prevention tools. We performed internal and external validation and benchmarking assessments. And, in September 2013, our systems were certified compliant with the Payment Card Industry Data Security Standards, meaning that we met approximately 300 independent requirements of the assessment. Yet the reality is that our systems were breached.

To prevent this from happening again, none of us can go it alone. All businesses—and their customers—are facing frequent and increasingly sophisticated attacks by cybercriminals. Protecting American consumers is a shared responsibility and requires a collective and coordinated response. Target remains committed to being part of the solution.

V. Conclusion

I want to once again say to the Members of this Committee and our guests how sorry we are that this happened. We are determined to get things right. Thank you.

The CHAIRMAN. Thank you, sir.

Now Ms. Ellen Richey, who is Chief Enterprise Risk Officer for a small corporation called Visa.

[Laughter.]

STATEMENT OF ELLEN RICHEY, CHIEF ENTERPRISE RISK OFFICER AND CHIEF LEGAL OFFICER, VISA, INC.

Ms. RICHEY. Thank you, Chairman Rockefeller, Ranking Member Thune, and members of the Committee. I appreciate the invitation to testify today.

Everyone in our payment system—merchants, financial institutions, networks, and cardholders—is affected when data compromises occur, because they jeopardize the trust that we have worked to build for more than 50 years. We continue to work to maintain that trust every day by placing security at the forefront of everything we do.

The payments industry has adopted a layered approached to data security. First, we protect consumers from financial harm through zero-liability policies that ensure they aren't held responsible for fraudulent charges on their accounts. And then we work behind the scenes to protect their personal information and prevent fraud before it can happen. As a result, fraud rates in the Visa system have declined by more than two-thirds in the last 2 decades to just 6 cents for every $100 transacted.

As recent compromises show, however, our work is never done. A critical first step in data security is to limit the amount of data that needs to be protected. For example, years ago we campaigned successfully to eliminate the storage of sensitive card data in large merchant environments. This made it more difficult for criminals to steal large volumes of data.

But, as we all know, more sophisticated criminals today are stealing data in transit. Therefore, strong data security remains fundamental to our program to protect the payment system. The Payment Card Industry data security standards establish a baseline which, when fully and consistently implemented, has proven effective in protecting our stakeholders from cyber attack.

Visa understands, however, that it is difficult for any organization to maintain complete security all of the time. With that in mind, we are working with others in the industry toward a paradigm shift that would in the future reduce or even eliminate vulnerable payment data from the merchant environment. If the data available in the environment could no longer be reused to commit fraud, criminals would have no reason to attack. We call this devaluing the data.

That is why we are joining with others in the industry to create a roadmap for the future of payment security with a focus on three data-devaluation technologies: EMV chip, tokenization, and point-to-point encryption.

The EMV chip is a microprocessor that can be embedded in payment cards. Chip cards are nearly impossible to counterfeit, and, as such, they eliminate one of the most important incentives for criminals to steal payment data today: the profit opportunity from counterfeit cards.

But EMV is not a silver bullet. In countries where it is widely used, fraud has simply moved to the online channel. So to address that threat, we have proposed a new standard for digital payments known as "tokenization," which replaces the accountholder's 16-digit account number with a digital token during the transaction process. Tokenization removes the sensitive data from the online merchant environment because it is the token and not the card number that goes to the merchant.

The third element in the roadmap is point-to-point encryption, a technology which is available today and protects account data from the moment it enters a point-of-sale terminal to the completion of the transaction process.

Securing data today and devaluing it tomorrow are the most critical components of our security strategy, but the layered approach assumes that no single strategy will ever be 100 percent effective. Therefore, we also invest in fraud prevention and analytical tools, some of the most advanced in the world, that identify and prevent billions of dollars of fraud each year. And we also invest in breach response, continuously improving our ability to identify breaches, respond to them quickly, and protect consumers when they occur.

As a result, the vast majority of accounts exposed in large data breaches do not experience fraud. In fact, just 2 to 5 percent of the accounts exposed incur fraud resulting from a breach.

As the Committee considers its policy responses, Visa believes there are three areas where government help could be most effec-

tive. First, the government can help create a safe environment to share cyber-threat information. Second, the government can continue to work with the international community to improve coordination among law enforcement agencies and to eliminate the havens from which cyber criminals launch their attacks on our financial system. Third, the government can establish a uniform breach-notification standard to replace the myriad state laws currently in place.

And, finally, in closing, let me note that we know cyber criminals will always be with us. They will continue to target any environment that contains valuable information. The payments industry has fought back, investing in sophisticated solutions that protect the system and the consumers who rely on it.

But as the criminals improve their technologies, we have to improve ours as well. The key is to work together to defeat our common enemy. And Visa is fully committed to working with all the participants in the payments industry toward this objective.

Thank you again for the opportunity to testify today.

[The prepared statement of Ms. Richey follows:]

PREPARED STATEMENT OF ELLEN RICHEY, CHIEF ENTERPRISE RISK OFFICER AND CHIEF LEGAL OFFICER, VISA INC.

Chairman Rockefeller, Ranking Member Thune and Members of the Committee, my name is Ellen Richey and I am Chief Enterprise Risk Officer and Chief Legal Officer at Visa Inc. Thank you for the invitation to appear before the Commerce Committee to discuss payment system security and Visa's ongoing efforts to protect cardholder data from cyber attacks and data breaches.

For more than 50 years, Visa has enabled people, businesses and governments to make and receive payments across the globe. As a global payments technology company, we connect financial institutions, merchants and governments around the world with credit, debit and prepaid products. Visa works behind the scenes to enable billions of daily transactions, powered by our core processing network—VisaNet. We make digital commerce more convenient, reliable and secure. It's important to note that Visa does not issue credit or debit cards or set the rates and fees on those products—our financial partners do.

Fighting fraud and protecting cardholders is a top priority for Visa—and securing electronic payments is fundamental to Visa's success. We invest heavily in advanced fraud-fighting technologies and develop and deploy innovative programs that protect cardholders and merchants.

Recent breaches have highlighted that organized and enterprising cyber criminals will seek to infiltrate any vulnerability to access consumers' personally identifiable information, payment card data or other information they view as valuable. When successful, these criminals steal more than money or information; they steal customers' peace of mind. Everyone in the payments system—merchants, financial institutions, networks, and customers—is affected by these breaches because they jeopardize the trust we've worked to establish over the last 50 years. At Visa, nothing is more important than trust in the payment system. Trust is the cornerstone of electronic payment systems, and consumers have long trusted us to safely and efficiently move their money. We value their trust and work to maintain it every day, by placing security foremost in everything we do.

It's also important to emphasize that when fraud does occur, Visa cardholders are protected through Visa's Zero Liability policy, which protects debit and credit cardholders from being held liable for fraudulent purchases.

Visa believes that protecting consumer data is the shared responsibility of all parties, including payment networks, financial institutions and merchants. No business or industry is exempt from protecting customer data or guarding against cyber attacks. Criminals are constantly adapting their techniques to gain access to systems that store or transmit data. To meet this challenge, security is a 24/7 job for all businesses that touch customer data.

The electronic payments industry secures payment card data through a layered approach. It takes a combination of technology, processes and people to guard account information and prevent fraud. As a result of the industry's security invest-

ments, we've seen fraud rates in the Visa payment system decline by more than two-thirds over the past two decades and fraud rates remain low and stable at less than six hundredths of a percent—that's 6 cents for every hundred dollars transacted. Our collective success in maintaining the trust and confidence of consumers comes from the ability to work together, share information and coordinate our defenses. However, as recent compromises show, our work is never done.

Protecting Sensitive Data

The first principle of protecting sensitive data is to limit the amount of data you have to protect. To promote this objective, Visa is constantly working to eliminate the storage of vulnerable payment data in the merchant environment. "Prohibited" data includes full magnetic stripe information, the CVV2 or "Card Verification Value 2," and PIN. Since 2006, Visa has promoted a "drop the data" campaign around the world to encourage merchants to discontinue storage of prohibited data and reduce cardholder data storage overall. As of March 2013, all major merchants (Level 1 and Level 2 as defined by PCI DSS) have confirmed they do not store prohibited data.

Eliminating data storage reduces the damage a hacker can cause by decreasing the amount of sensitive data in the environment. However, today's cyber criminals can also steal data in transit—while passing into, out of, or through the system—even if the data is never stored. Therefore, strong data security remains a critical element of our program to protect and secure the payment system.

The key to an effective data security program—as with any successful operation—is a solid foundation. For the electronic payments industry, the Payment Card Industry Data Security Standards (PCI DSS) provides that foundation. PCI DSS has proven to be an effective set of minimum security standards when fully and consistently implemented across all systems handling cardholder data. No standard can provide an absolute guarantee of security in a changing world, and PCI DSS is not an exhaustive list of all the security practices that an organization should consider. However, compliance with the standard is a valuable component of a comprehensive security program and greatly reduces the risk of data compromise. In fact, we have yet to see a payment data compromise in which the breached entity was fully in compliance with PCI DSS at the time of the breach.

The implementation of technical security tools is only one component of an effective security regime. In addition, companies must put in place business processes that ensure their tools are used and maintained properly, their procedures are executed correctly, and the inevitable human errors are detected and corrected quickly. This requires a rigorous program of internal control, monitoring, corporate governance, communication, and training that touches every part of the business environment.

It can take a considerable effort to ensure, for example, that everyone in the company follows basic security protocols such as removing default passwords, using strong ones in their place, prohibiting the use of unapproved removable USB devices, and limiting access to systems containing sensitive data. Employees often find these controls tedious and inconvenient. But sadly, a lapse in any of these areas can open the door to a criminal intrusion that threatens the entire enterprise. We often see data compromises that could have been avoided by following baseline security procedures.

Going beyond the basics, we believe that advanced cyber training is critically important for large enterprises. For instance, Visa cyber defense analysts have undergone training with leading organizations including Lockheed Martin, RSA Advanced Cyber Defense and the Department of Homeland Security's Industrial Control Systems Cyber Emergency Readiness Team.

Visa views the recent release of the NIST Cyber Security Framework for Improving Critical Infrastructure as a positive development in strengthening U.S. cyber defenses. We support a flexible, standards-based approach that recognizes and builds upon existing private and public regulatory structures, and we're encouraged that the final framework issued by the Administration embraces existing security best practices.

Finally, it is important to recognize that cyber security is not a one-time exercise. Companies must continually assess and evolve their policies and procedures and educate their employees on how to best protect against cyber threats. Cyber hygiene is something Visa, and all companies, must work at every day.

Devaluing Data

While effective security is critical, we understand that it is difficult for any organization to be completely secure all the time. With that in mind, Visa is working with others in the industry toward a paradigm shift that would in the future re-

duce—or even eliminate—vulnerable payment data from the merchant environment, by moving from a data protection to a data devaluation approach. If the data available in the merchant environment could no longer be reused to commit fraud, then criminals would have no reason to steal it, and merchants would no longer be targeted by criminals seeking to commit payment fraud.

This approach to the future of payment security relies on three technologies: EMV chip, tokenization and point-to-point encryption.

The EMV chip is a microprocessor that can be embedded in plastic payment cards or in other form factors such as mobile phones. Sometimes referred to as a smart card or chip card, EMV enables more secure processing by generating a one-time-use code for each transaction. Since EMV chip cards are nearly impossible to counterfeit, they eliminate one of the most important incentives for criminals to steal payment data today—their ability to use the data to create counterfeit cards. As such, EMV chip makes payment data a less attractive target for criminals.

To encourage adoption of EMV chip in the United States, in August 2011, Visa announced a roadmap that included processor requirements and liability shifts. Visa's EMV roadmap is not a mandate. Instead, it provides marketplace incentives to encourage adoption by Visa financial institutions and merchants—elements that have proven to be effective in moving other markets to deploy EMV chip technology.

As part of Visa's incentive program, the party that has not implemented EMV technology bears the loss from any resulting counterfeit fraud. This shift will become effective October 1, 2015 for point-of-sale environments, and October 1, 2017 for Automated Fuel Dispensers and ATMs.

Last fall, we reached an important milestone in the migration process when the vast majority of U.S. Visa acquirer/processor endpoints certified their ability to support merchant acceptance of EMV chip transactions. Acquirers representing 95 percent of Visa's payment volume in the United States have been certified to support EMV chip processing.

Based on years of experience working with merchants as well as issuing banks, Visa has taken care to ensure that our roadmap supports a variety of cardholder verification methods, including signature, PIN and no cardholder verification for low value, low risk transactions. In order to accomplish the transition to EMV in the most cost-effective and expeditious way, we want to provide customers, merchants and financial institutions with options that minimize the disruption to the current payments environment.

Many have asked why the United States is taking longer than other markets to adopt EMV chip technology. The speed and efficiency of our telecommunications infrastructure, coupled with back-office tools such as the real-time authorization and advanced fraud analytics have helped stakeholders to effectively manage fraud levels here. In other markets, including the European Union, one reason EMV was adopted was because the existing telecommunications infrastructure presented challenges for using the kind of real-time network authorizations that occur on virtually all transactions in the U.S. As a result, an alternative technology was needed to facilitate off-line security checks between the card and terminal; thus the emergence of a microchip.

As the U.S. is adopting EMV chip, we are also now seeing international markets adopt real-time authentication tools similar to those used in the U.S. While each market went down different paths over a decade ago, we are now seeing fraud and security strategies converge as all markets recognize the need to deploy multiple technologies to fight fraud and to protect personal data.

As we make the transition to EMV in the United States, it is critical that all participants in the payments system work together. The payments ecosystem in the U.S. is larger and more complex than any other in the world, with thousands of financial institutions and millions of businesses accepting electronic payments. Visa has been mindful to allow enough time for this migration to occur without disadvantaging smaller merchants and financial institutions or unduly disrupting the consumer experience as the migration process occurs.

While EMV is the traditional first step to devaluing payment data, it is not a silver bullet. When EMV has been adopted in other countries we have seen that cyber thieves continued to steal data in order to commit fraud in the eCommerce channel. To address this growing threat, in 2013, Visa, MasterCard and American Express proposed a new standard for digital payments that will allow a traditional account number to be replaced with a payment "token" in eCommerce or mCommerce.

Tokenization uses a unique digital token that is tied to and replaces the accountholder's 16-digit account number in a payment transaction. Tokenization can enhance transaction efficiency, improve cardholder privacy and data security, and may enable new types or methods of payment. Tokenization shows particular promise in stopping online fraud, because it is the token—not the card number—that

goes to the merchant, and because the token can be issued with limits on the times and places it can be used. Tokenization, like EMV chip, can be used to introduce a dynamic element into the transaction, thus devaluing the data and making it less lucrative for criminals to steal in the first place. When fully deployed, tokenization in combination with EMV could eliminate the need for merchants, digital wallet operators or others to secure account numbers.

The final element in a comprehensive data devaluation strategy is point-to-point encryption, which can be implemented to secure data as it is transmitted from one point to another throughout the transaction processing environment. To gain full protection from EMV and tokenization approaches, multiple stakeholders must make changes to their systems that can take several years to complete. In the meantime, encryption technologies are available that can be deployed to protect data from the moment it enters a point-of-sale terminal to the completion of the transaction process. When properly implemented, encryption makes stolen data unusable by criminals and thus reduces the incentive to steal it.

Preventing Fraud

Securing data and ultimately devaluing it are two core elements of Visa's approach to securing the payment system and protecting consumers. The third is fraud prevention. Our fraud analytics are among the most advanced in the industry and have helped to identify and prevent billions of dollars of fraud. One such prevention tool is Visa Advanced Authorization, which provides an instantaneous rating of a transaction's potential for fraud to the financial institution that issued the card, including whether it was part of a reported data security compromise. This rating occurs as part of the transaction authorization and enables the issuer to make a more informed decision about whether to accept or decline the transaction.

These technologies allow financial institutions to better serve and protect their customers. I am sure many of you here have received a call from your bank or credit union to inquire about a possible suspicious transaction. These types of services provide additional layers of security to help protect consumers.

Visa has also invested in tools for consumers to help prevent fraud. For instance, Visa offers a service called Verified by Visa that adds an extra layer of security, making it harder for someone else to use your Visa card to shop online in the rare event your Visa card or account number is lost or stolen. Each time your Visa credit or debit card is presented to make an online purchase at a participating merchant, Verified by Visa helps to make sure it is you who is attempting to make that purchase and not someone else.

In addition, Visa has developed an alerts service that instantly notifies cardholders of transaction activity on their mobile phones via SMS text or e-mail. Many banks offer this service, or similar ones they have developed themselves. An alert is triggered whenever a transaction meets a cardholder's preset parameters, and can be sent within seconds of a transaction occurring. Alerts generally contain important transaction details such as the amount, time, date, the type of purchase, and may also include the merchant name and location and the currency conversion exchange rate for international transactions. These instant notifications are useful to consumers for monitoring their own transactions. More importantly, however, they assure consumers that they will receive instant notice of any fraudulent activity on their accounts, providing them with additional peace of mind.

Breach Response

The fourth and final element of security and fraud prevention is how we respond when a breach has occurred. Visa is continually working with clients to improve our ability to identify payment data breaches and protect consumers affected by them. We may learn of a breach through issuer reports, self-reporting by a compromised merchant, our own monitoring efforts, or through law enforcement.

One commonly used method for detecting compromise activity is known as the "Common Point of Purchase" or "CPP." Card issuing banks and payment networks use advanced analytical tools to search millions of transactions in order to identify those unique locations that show a pattern of genuine transactions followed by confirmed fraudulent activity on the same card. Identifying points of compromise at the early stages of stolen card account usage helps to minimize the financial consequences of compromise events and enables corrective and mitigation actions as early as possible.

When data breaches expose sensitive cardholder information, Visa's first priority is to protect cardholders from fraud. After learning of data compromise events, Visa immediately begins working with the compromised entity, law enforcement and affected client financial institutions to ensure the compromise is remediated and to prevent card-related fraud. Visa notifies all potentially affected card issuing institu-

tions and provides them with the necessary information so that they can monitor the accounts, reissue cards, and, if necessary, advise customers to check closely all charges on their statements.

The banks that issue Visa cards have the direct responsibility and relationship with cardholders; they work diligently to ensure that cardholders are not responsible for any fraudulent charges. But it is also important to note that the vast majority of the accounts exposed in large data breaches do not experience fraud. In fact, thanks to network, issuer and merchant fraud detection, prevention and monitoring solutions, only about 2 to 5 percent of compromised accounts incur incidents of fraud resulting from the compromise.

Public Policy Considerations

As the Committee considers appropriate actions in response to recent events, Visa believes there are several areas where government can help defend against cyber criminals.

First, as the payments and other industries reinforce their safeguards, the government can help create a safe environment to share cyber threat information. Visa currently works closely with a number of different groups to gather threat information, including the Financial Services Information Sharing and Analysis Center. Improvements in cyber threat information sharing with appropriate liability protections can further bolster collective efforts on global cyber security.

Second, a number of cyber criminals are launching attacks from overseas. We encourage the government to continue to work with the international community to improve coordination and cooperation among law enforcement agencies. Cyberspace is not limited by geographic borders, and we know that the most sophisticated attackers are often physically located overseas. Therefore, any effort to strengthen law enforcement cooperation across national or jurisdictional boundaries would be beneficial. In addition, governments should agree that it is unacceptable for any country to provide a safe haven for cyber criminals.

In addition, the development of a uniform Federal data breach-notification standard would be a valuable tool to replace the myriad of state laws currently in place. Such a standard could guide when and by what means consumers and law enforcement agencies should be notified—as well as by whom—when consumer harm may result from a compromise of account information.

Lastly, we would caution against legislating technology standards or mandating a specific security or payment technology, to avoid hindering the rapid rate of new payment innovations that are coming to market, especially mobile wallet solutions that will leverage a range of new tools to authenticate payments and enhance security.

In closing, the reality is that cyber criminals will continue to target U.S. companies, the payment system or any database that contains valuable information. But the good news is that there are sophisticated tools to protect the system. Visa is committed to working with all participants in the payments industry to implement the full range of technologies that will fight fraud and further protect consumers' information as the marketplace and threats evolve. Of course, technology cannot completely eliminate human error or internal threats, so it remains critical for businesses to adopt strong policies that are effectively implemented by their employees. Cyber criminals are a common foe and we all must work together to protect personal consumer information from cyber attacks and data breaches.

Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.

The CHAIRMAN. Thank you very much, very much indeed.

Now Mr. Peter Beshar, who is Executive Vice President and General Counsel, Marsh & McLennan Companies.

STATEMENT OF PETER J. BESHAR, EXECUTIVE VICE PRESIDENT AND GENERAL COUNSEL, MARSH & MCLENNAN COMPANIES

Mr. BESHAR. Chairman Rockefeller, Ranking Member Thune, members of the Committee, my name is Peter Beshar. And as a former David Rockefeller fellow, it gives me particular pleasure, Mr. Chairman, to be before this committee.

I would like to focus my remarks this morning——

The CHAIRMAN. You did it for free?

Mr. BESHAR. I am sorry?

The CHAIRMAN. My uncle did this for free?

[Laughter.]

Mr. BESHAR. Something like that, Mr. Chairman.

The CHAIRMAN. That is very unusual.

Please.

Mr. BESHAR. Thank you.

So I would like to focus my remarks this afternoon on a single and narrow topic of cyber insurance: What is it? Who is buying it? And what role might it play as part of a comprehensive risk-mitigation framework?

As the world's leading insurance broker, our company has a unique perspective on the cyber insurance marketplace. Marsh assists clients in preparing risk-mitigation strategies, including as to cyber insurance, and has issued its first cyber policy as far back as 1999 called "NetSecure."

So there are three basic types of cyber insurance.

The first and most fundamental is coverage that protects out-of-pocket expenses that the University of Maryland or another institution might suffer—expenses like credit monitoring or setting up call centers or notifying affected individuals.

The second type of insurance is something analogous to business interruption insurance so that if your system is really disabled for a period of days or longer, you are able to recover the actual harm that you have suffered in the form of lost profits.

And the third type of insurance is for damage that might be suffered by parties outside of your company, so customers or consumers or clients, and that is called third-party insurance.

To give the Committee some insight into the dynamics in the cyber insurance market, we just conducted a survey of our cyber clients to give you a sense of who is buying it, what the take-up rights are, and what the price of this insurance actually is.

So there are a couple of charts that were in my written testimony. I think you have some of them in front of you.

The CHAIRMAN. They are in each of our packets.

Mr. BESHAR. Great. Thank you, Mr. Chairman.

So there are a couple of important headlines.

The first is that interest in cybersecurity is increasing rapidly. Indeed, the number of Marsh clients who purchased stand-alone cyber insurance increased by more than 20 percent just in the past year.

The highest take-up rates are in industries like financial services; health care, particularly because of the HIPAA statute and the importance of protecting healthcare data; and also, interestingly, in the education space, where there have been marked increases. So that is a breakdown by industry.

In terms of size of companies, larger companies perceive a greater risk to cyber threat than smaller companies do. And so we analyzed the take-up rates, and if you are a company with revenues of more than $1 billion, your take-up rates are almost double what they are if you are a smaller company.

And, last, Mr. Chairman, on pricing, here the news is actually quite positive. Throughout the past year, even as the perception of the risk and potential severity associated with cyber attacks in-

creased, pricing has remained relatively stable throughout the year. This is partly a product of a number of new entrants, new underwriters coming into the marketplace.

So that is the actual insurance. The process of simply applying for the insurance is itself constructive because, similar to the NIST framework, the process of applying forces you to go through a gap analysis to try to benchmark yourself against industry standards and what are considered the best practices and see what you can do to position yourself as a better risk for the underwriting community.

So, just in closing, Mr. Chairman, as this committee is all too aware, this is a race without a finish line. Our adversaries will continue to adopt new methods of attack and different strategies. And it is extraordinarily important that, in combating this threat, government, the private sector, and also the nonprofit world partner together to try to respond effectively.

Thank you.

[The prepared statement of Mr. Beshar follows:]

PREPARED STATEMENT OF PETER J. BESHAR, EXECUTIVE VICE PRESIDENT AND GENERAL COUNSEL, MARSH & MCLENNAN COMPANIES

Introduction

Good afternoon Chairman Rockefeller, Ranking Member Thune, and members of the Committee. I am Peter Beshar, the Executive Vice President and General Counsel of Marsh & McLennan Companies. I commend you for convening this hearing and am grateful for the opportunity to participate.

Marsh & McLennan Companies operates through four market-leading brands—Marsh, Guy Carpenter, Mercer, and Oliver Wyman. Our 55,000 employees provide advice and solutions to clients across an array of industries in the areas of risk, strategy and human capital. In particular, Marsh and Guy Carpenter assist companies in identifying and then mitigating key risks to their business—including cyber security.

I wanted to offer a couple of initial observations and then focus my remarks on a single topic—cyber insurance.

First, hyperconnectivity has been a boon for enhancing our productivity. We are able to connect the world and execute tasks with a speed that was inconceivable even a decade ago. With that hyperconnectivity, however, comes the risk of a significant disruption through a cyber attack.

Second, the government has led the way in identifying the significance of this risk and then pushing industry and the non-profit sector to bolster their defenses. A case in point was the release last month of the Administration's Cyber Security Framework. This is an important tool to help enterprises assess their preparedness and then enhance their resilience against a cyber attack.

Moreover, this Committee has been at the vanguard of the effort to raise awareness of the threat posed by a cyber security attack. In particular, this Committee's interactions with the SEC have served to help companies, and investors, better understand the potential disruption that can occur from a significant attack.

In the area of cyber security, offense is a lot easier than defense. There is no silver bullet or panacea that will eliminate this risk. Rather, it will take a collaborative effort between government and business and among professionals in different disciplines—IT, HR, Legal and Compliance—to assess vulnerabilities and link arms to confront this risk head on.

This afternoon, I would like to discuss the role that cyber insurance can play as one component of a comprehensive risk mitigation strategy.

To begin, what is cyber insurance? Who is buying it? What role can it play to mitigate this risk?

As the largest insurance broker in the world, Marsh has a unique perspective on the cyber insurance market.

The concept of cyber insurance was first introduced the 1980s, when insurers began providing coverage for computer failures at banks and other Fortune 500 companies. Marsh launched its first cyber insurance product, NetSecure, in 1999.

Broadly stated, there are three core types of cyber insurance.

The first, and most basic, provides protection for out-of-pocket expenses that a company incurs in the wake of a data breach. These expenses include notifying affected individuals, setting up call centers and providing credit monitoring.

The second form of coverage protects companies if their computer network is effectively shut down for days or longer. With this broader business interruption coverage, a company can recover the actual harm it suffers in the form of lost profits.

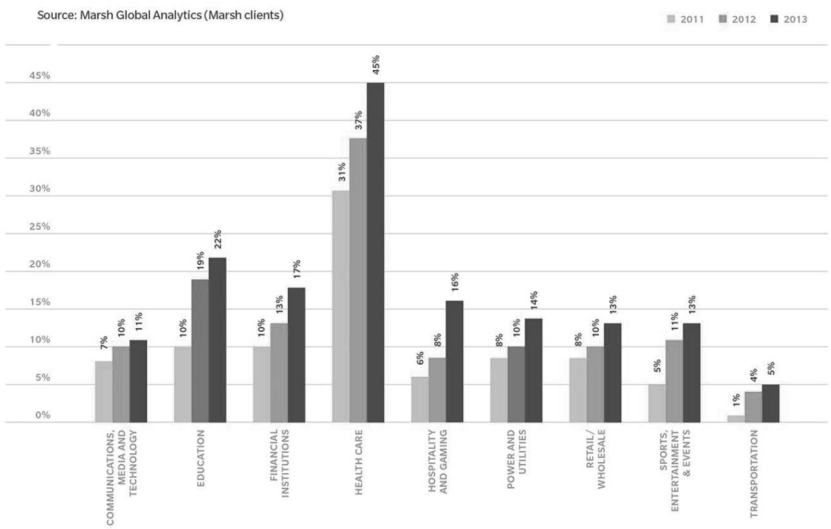
The third type of coverage is for harm caused to an insured's clients, customers and consumers as a result of a significant breach. This is called third-party coverage.

To give the Committee insight into this market, Marsh conducted a comprehensive survey of the type of companies that are currently purchasing cyber coverage—broken down by industry and size of company.

There are a number of important headlines. Most importantly, interest in cyber insurance is expanding rapidly. Indeed, the number of Marsh clients purchasing stand-alone cyber insurance increased more than 20 percent in just the past year.

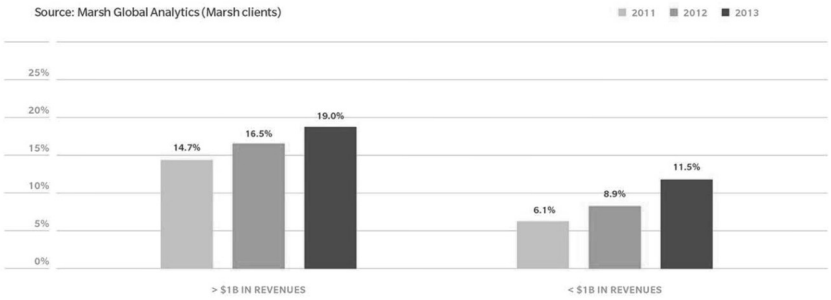
As reflected below, the highest take up rates for cyber insurance are in the following three industries: (1) health care; (2) education; and (3) financial services. These industries handle a large volume of sensitive personal information, including health care data, social security numbers and credit card information. As a result of statutes like HIPAA, the take up rates in health care are markedly higher—approaching 50 percent—than any other industry.

Figure 1: Take Up Rates by Industry



Marsh also analyzed how the size of a business impacts its decision whether to purchase cyber insurance. As a general matter, larger companies perceive a greater threat to their operations than smaller companies. As a result, the take up rates for companies with revenues over $1 billion are almost twice as high as the rate for companies with revenues below $1 billion.

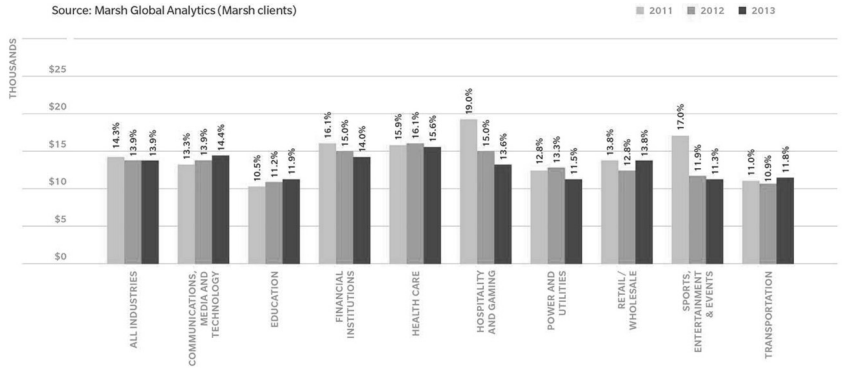
Figure 2: Take Up Rates by Company Size



Third, Marsh analyzed trends in the cost of cyber insurance. Here, the news is quite positive. Throughout 2013, cyber insurance rates remained stable—even as the perception and potential severity of the risk increased. This is partly because a number of new underwriters are interested in providing cyber coverage.

As reflected in the analysis below, the average price per million dollars of coverage for a cyber policy actually dropped in 2013 in a number of sectors, including financial institutions, utilities, sports and entertainment, while increasing for other sectors, including communications and transportation.

Figure 3: Insurance Coverage Price Per $1 Million Across Industry Sectors



Furthermore, the process of applying for cyber insurance—analogous to the process of conducting a gap analysis under the Administration's Cyber Security Framework—is itself a constructive exercise for raising awareness and identifying potential vulnerabilities. At Marsh, we utilize a proprietary Information Security and Privacy Self-Assessment, which is based on international information security management standards known as ISO 27001.

Using the assessment, Marsh brokers perform a high-level review of information security management protocols with respect to access control, physical security, incident response and business continuity planning. The assessment focuses on the strength of a company's governance procedures regarding cyber practices to understand how insurance carriers will view the company's risk profile.

Importantly, a number of cyber coverages also provide access to experts who are available to monitor the client's information security and assist the client to restore operations in the event of a network attack. These services include technical advice from on-call consultants, vulnerability detection to examine network devices and servers, and assistance developing incident response plans.

Conclusion

As the SEC indicated in its cyber security guidance, cyber insurance is one element, among many, of a comprehensive risk mitigation strategy.

This is a race without a finish line. As we strengthen our defenses, adversaries will adjust and develop new methods of attack. Our success in combatting this dynamic and evolving threat will depend on continued collaboration between government, industry and the non-profit sector.

I look forward to answering any questions you might have.

The CHAIRMAN. Thank you very much. It was eloquent and helpful.

Mr. David Wagner, President, Entrust, Incorporated.

Welcome.

STATEMENT OF DAVID WAGNER, PRESIDENT, ENTRUST, INC.

Mr. WAGNER. Good afternoon, Chairman Rockefeller, Ranking Member Thune, Committee members. Entrust is pleased to be here to help facilitate and to continue the dialogue for a better understanding of cybersecurity issues.

Just over 2 years ago, Entrust testified on the similar topic of cybersecurity, and since that time the situation has worsened. Nation-states and criminals are continuing to use cyber to advance their interests.

The December point-of-sale breaches are another example of this escalation. Although Entrust has no direct relationship with any of the victims of the December point-of-sale attacks, we can provide general insight into the attacks.

As we have heard earlier in these testimonies, criminals are using old-fashioned con tricks and cyber tools to get past moat-style defenses. Social engineering and malware are the silent equivalent of crowbars, penetrating into corporate networks. And once past the perimeter defenses, the criminal uses a stolen identity and virtually becomes someone on the network, making them difficult to distinguish from normal network behavior.

In the case of the retail breaches, once the criminals assumed the right identity, they were able to push malicious code to the point-of-sale terminals, they were able to collect customer credit card data from the magnetic stripes, and then they stored and exfiltrated that data overseas.

You can see from the attack scenarios that they are sophisticated. They are sophisticated, but they are not rocket science. They use stolen identities to access the victim company's network and then use the victim company's IT tools to complete their crime.

A determined cyber attacker can overcome even strong moat defenses. We need strategies to strengthen the defenses inside the perimeter. Good information security governance is vital, and industry regulations like PCI and frameworks like SANS 20, COBIT, and ISO are available to help build effective security architectures.

So you might be asking, with all of this knowledge, guidance, and standards, how did the breaches occur? Why weren't accounts using authentication techniques stronger than username and password? Why wasn't the network segmented to protect sensitive data? Why weren't alerts responded to and network monitoring equipment capturing the unauthorized traffic patterns?

Nothing in the breaches was new. We know that good security governance requires investment in people, process, and technology applied consistently over time. But have we created a culture where executives and board members are aware and understand

the information security risk at their enterprise? Have we created regulations that evolve and change with technology? If we haven't, then no regulation or no security tool will solve our problem.

When a retailer is breached, financial institutions bear the cost of the stolen data, banks and credit unions bear the cost of card reissuance, and consumers suffer the pain of changing cards and cleaning up accounts. Risk assessments at the organizations where sensitive data reside must consider the full systemic value of their data.

Cyber crime poses a greater threat to the security of nations, corporations, and individuals than ever before. The challenge is balancing—balancing the importance of protecting data with the benefits of emerging technology. As policymakers, you are charged with facilitating commerce and putting in place a structure for finding this balance.

Entrust recommends actions in three areas.

First, Federal breach notification law needs to be passed. Federal harmonization will allow enterprises and consumers alike to know what is expected of them on a national level. It will also put the Federal Government in a role where it belongs.

Second, the Federal Government needs to continue to foster best practices and sharing of information across the public and private sectors. Collaboration fueled by real-world learning is critical to creating a strong, unified front so criminal groups can't simply migrate to the next weakest target.

Third, we must change the cybersecurity culture. Enterprises large and small, public and private, need to embrace information-security governance as a core responsibility.

Evolving our approach and our cyber defense posture needs to be a Federal priority, and we need to move forward now. Without changes to the security posture of our most important industries and infrastructure, cyber crimes will continue to grow in frequency and potency. The best path forward rests upon a public-private ecosystem that is built upon good security governance, secure identities, and constant self-assessment of vulnerabilities.

Whether we drive adoption through incentives or directives, we need to proceed now. I urge you, your colleagues, and the administration not to let 2014 expire without adoption of measures that will better protect our economy and our security posture.

Thank you for your time this afternoon and for your attention to this important matter of cybersecurity.

[The prepared statement of Mr. Wagner follows:]

PREPARED STATEMENT OF DAVID WAGNER, PRESIDENT, ENTRUST, INC.

I am David Wagner, President of Entrust, a leader in identity-based security software systems and solutions. On behalf of Entrust, we appreciate the opportunity to testify today.

At Entrust, a wholly owned subsidiary of Datacard Group, we secure and protect digital identities and information. We serve more than 5,000 organizations, spanning 85 countries, by safeguarding enterprises, governments, financial institutions, websites and citizens—including your constituents.

For its part, Datacard is the world leader in secure identity and card personalization solutions. Most payment cards in circulation today are issued using Datacard systems. As a combined company, and as a result of the ways in which we serve our customers, we possess a unique perspective on secure identity and trusted transactions and the increasing threat of cyberattacks on networks and systems.

Just more than two years ago, we testified before a U.S. House of Representatives Energy and Commerce Committee subcommittee on this same subject of cybersecurity. We said then that cybercrime poses a greater threat to the security of nations, corporations and individuals than ever before. We noted that the threat had moved from one of hacking for honor to one of hacking for harm and profit via overt criminal activity.

Today, it's no secret. The situation has worsened. Incidents involving the loss of personal information have increased an average of 40 percent in each of the two years since we last testified.[1] Practically every day, new headlines appear about a data breach at a financial institution, a retailer, a university, a hospital, a government agency—and the list continues.

In February, cybersecurity firm Hold Security said it uncovered stolen credentials from some 360 million accounts available for sale on cyber black markets. It also reported the criminals are selling some 1.25 billion e-mail addresses.[2] The breaches impact consumer confidence and have economic consequences.

- In the U.S. alone, the direct and indirect impact of identity theft totaled $24.7 Billion (USD).[3]
- According to the Bureau of Justice Statistics, 7 percent of Americans aged 16 and older fell victim to identity theft in 2012. Of these, 22 percent fell victim more than once.[3]
- The median loss for those victims to identity theft was $2,183, with a mean of $300.[3]
- In a report from the Federal Trade Commission (FTC), which consists of formal complaints registered with law enforcement, the FBI, Canadian counterparts, the FTC, and several other organizations, identity theft remained the largest single consumer compliant category in 2013.[4]

It also appears that the number of larger breaches is increasing. Unfortunately, and a point we will elaborate on later, there is no national breach law and the means of assessing an aggregated view of this data remain somewhat elusive.

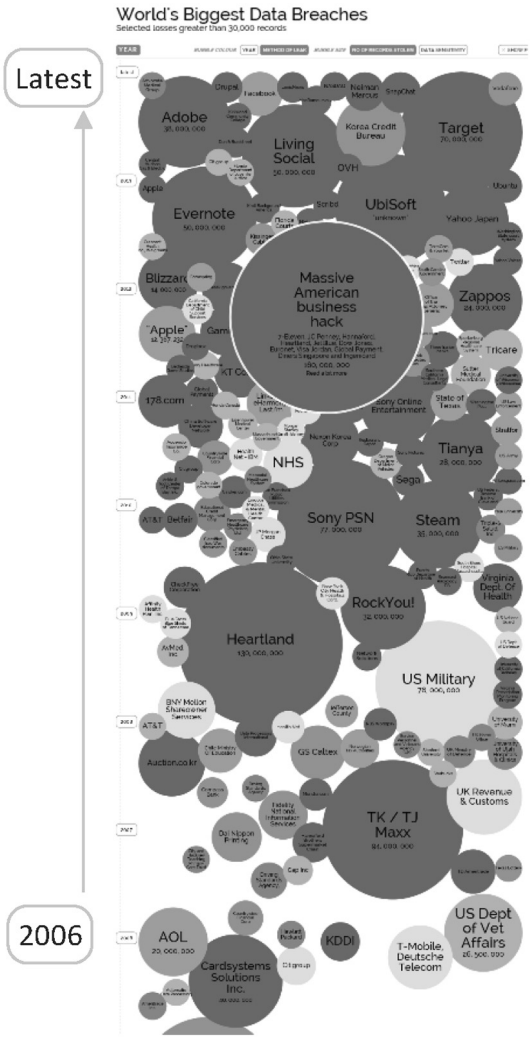
---

[1] "Incidents Over Time: 2011 versus 2012 and 2013." Open Security Foundation n.pag. Data Loss Statistics. Web. 24 Mar 2014. *<http://datalossdb.org/statistics>*.

[2] Finkle, Jim. "360 million newly stolen credentials on black market: cybersecurity firm." Reuters [Boston] 25 02 2014, n. pag. Web. 24 Mar. 2014. *<http://www.reuters.com/article/2014/02/25/us-cybercrime-databreach-idUSBREA1O20S20140225>*.

[3] Harrell, Erika, and Lynn Langton. United States. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. 2013. Web. *<http://www.bjs.gov/content/pub/pdf/vit12.pdf>*.

[4] United States. Federal Trade Commission. Consumer Sentinel Network Data Book for January-December 2013. 2014. Web. *<http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf>*.



However, one view of the data behind the breaches is shown in the adjacent figure, which is an aggregation of data from several well-known breach reporting sites.[5]

What this data suggests is that the overall volume and numbers of large attacks continue to increase. Additionally, the majority of attacks are dedicated efforts to extract information (versus accidental losses). In total, it appears that both the number of records exposed and the number of incidents have nearly doubled since 2011 and the majority of these incidents were in the U.S.[6]

[5] Quick, Miriam, Miriam Hollowood, Christian Miles, and Dan Hampson. "World's Biggest Data Breaches: Selected losses greater than 30,000 records." Information Is Beautiful. N.p., 31 Dec 2013. Web. 24 Mar 2014. *<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>*.

[6] "Data Breach QuickView: An Executive's Guide to 2013 Data Breach Trends." Risk Based Security & Open Security Foundation, n.d. Web. 24 Mar 2014. *<https://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf>*.

We are witnessing massive growth in the volume of transactions, amount of data and number of devices connected online. This attracts criminals and provides vectors for attacks. It is at the center of the rising tide of cyber issues and the increasing impact of related breaches.

The challenge is to make sure that success in protecting the growing volume of data doesn't unnecessarily hinder users from receiving the benefits of emerging technology or burden those charged with securing the systems. As policymakers, you are charged with facilitating commerce and ensuring an optimal structure for finding this balance.

The Focus: Identity and Malware

Before recommending actions to enhance our cyber posture, I'd like to provide a bit more background on how the attacks are occurring.

Although Entrust has no direct relationship with any of the victims of the December 2013 point-of-sale (POS) attacks, we can provide general insight to the attacks from public information and from our understanding of how cyberattacks are normally perpetrated.

In many of the retail breaches, and not unlike attacks witnessed in other industries, criminals are using a combination of social engineering and technical tools, such as malicious software or "malware," to steal credit card numbers and personal information.

The traditional approach to network security continues to put significant focus on developing a perimeter around the corporate network. Whether or not these defenses can be breached directly, we can ascertain that they aren't the weakest link in the defense by assessing the successful attacks. Instead of trying to breach perimeter defenses directly, criminals are focusing on obtaining an identity that provides access directly inside the network.

The logic could work something like this: criminals know that many organizations still treat the internal network as being protected by the perimeter (*i.e.,* castle walls and moat analogy). As a result, less attention gets paid to internal systems and where monitoring occurs, it tends to get less attention than the external environment.

As a criminal, if you can get inside, your objectives become much easier. So, what is the easiest way to accomplish this goal? A direct attack is possible against the perimeter, but this is where we're focusing our security investment and attention.

Back to the castle analogy, the walls are formidable, and the moat is deep. However, organizations are people; people working on the trusted "inside" of the network, people just trying to get their jobs done (we will come back to this later). And we generally trust these people. They become the vector for many of the attacks.

If a criminal can get one of their identities, or more specifically credentials, they have bypassed the perimeter, the walls and the moat. This can be done through social engineering an unsuspecting individual with legitimate access to the network (*e.g.,* an employee or contractor), by exploiting flaws in a technical implementation, or via direct access through a knowing accomplice on the network.

Using stolen credentials, the criminal has virtually become "someone" on the network and appears as a legitimate user, making them difficult to see and detect. From here, the attacker can move more easily within the network, using the systems available to the legitimate user and bringing in their own more malicious tools.

How Hackers Do It

A cyberattack is typically not a single event. Regardless of the attack goal, there are a series of objectives that need to be completed along the way. As described above, each step is made significantly easier if the attacker possess the identity of a legitimate person or device on the target network.

Disciplined cyberattackers do not need to "hack" or "break" a computer system in order to take advantage of it maliciously. Attackers will use the system as a whole, by taking full advantage of the way that PCs and networks are engineered. PCs and their operating systems are designed to be highly connected and interoperable in order to provide excellent user experiences for their legitimate users.

This, unfortunately, also provides rich functionality for an attacker. Computer networks are naturally trusting by their nature, and cyberattackers take full advantage of that. It is very difficult to tell the difference between malicious and legitimate behavior on a PC or on a computer network. This is because the cyber attacker has stolen a legitimate identity. The attacker is not a masked, highly visible criminal. The attacker has your identity and is imitating you.

Employees inside a corporate network can be tricked into opening e-mails that contain a malicious payload. The original Greek 'Trojan Horse' is a good analogy,

but instead of a wooden horse, the gift may be an e-mail that looks like a legitimate request for assistance from your boss.

Anyone can be tricked into opening that e-mail or browsing to a Web link. The e-mail or Web link will contain the malicious payload that will infect the employee's PC, which will serve as a beachhead from which the attacker will perform subsequent steps in the attack.

By infecting the first PC, the attacker has assumed the identity of the employee on that PC. If the employee happens to be an administrator, which is all too often the case, the attacker will also have the rights of an administrator and allow the attacker to move even more quickly to their target.

The initial infection will be invisible to the employee. Attackers are using techniques that defeat end-point protections and continually adapt to monitoring. Unfortunately, most defenses at the PC and network level are based on catching attacks where the patterns of attacker behavior have been seen before. But attackers are capable of adjusting their tools and behavior just enough to slip through these defenses.

From the beachhead of the initial PC infection, the cyberattacker will use the first stolen identity to gather information on the target network and begin to move towards the ultimate target. The fog of war is quickly cleared for the attacker as they map out the network.

If you have ever browsed for a printer on an enterprise network, your own computer has performed network reconnaissance indistinguishable from the activity a malicious attacker needs to do to map out your network. This means that the attacker's movements in your network are exceedingly difficult to distinguish from a normal user, unless you have very tight controls over identity, and the rights that those identities have.

A human resources employee should normally never need to view computer resources that store highly valuable intellectual property. A third-party partner or vendor who has been given access rights to a corporate network should not have access to anything beyond the limited systems needed to complete their tasks.

Preventing Data Breaches

You can see from the attack scenario that the criminals must be knowledgeable of the systems involved and typical responses from the compromised organization. They are knowledgeable, but they aren't overly sophisticated. They merely use stolen identities to access and use the normal IT tools of the victim in conjunction with malware.

Although the most advanced and persistent attackers can breach even strong defenses, good security governance and strong security policies, processes and implementation can thwart most attacks or at least limit their impact.

In addition to industry standards such as the Payment Card Industry Data Security Standard, best practices for information security are covered in a number of security frameworks such as SANS 20, ISO 27002, COBIT and recent publications from NIST.

The SANS Top 20 Critical Security Controls is an example of the focus areas provided in the frameworks. The controls discussed by SANS are a subset of a larger body of work provided in NIST SP 800–53, with the top 20 controls as follows:

Top 20 Critical Security Controls—Version 5

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defenses
6. Application Software Security
7. Wireless Access Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Audit Logs

15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Protection
18. Incident Response and Management
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

Examples of the rationale behind some of this guidance are provided below:

> The principle of "least privileges" should be considered a vital part of policy, leading to a minimal usage of administrative credentials. Employees and third parties are often given too many rights on a corporate network, which increases risk. If an attacker is able to steal an administrative identity, this brings huge risk. Therefore, administrative identities should be used minimally and secured strongly.
>
> It is difficult or impossible to defend a computer network without an inventory of resources. This includes desktop computers, back-office servers, Wi-Fi and wired access points. This is required in order to create secure network architecture.
>
> A trained security staff equipped with tools is needed to operationalize that defensive posture.
>
> For example, an important tool to thwart identity-stealing is strong second-factor authentication. Most people think of authentication as being only username and password. Username and password is a single-factor authentication. In other words, the attacker only has to steal one secret (the username and password) in one place in order to steal the identity and be able to log in to a computer system.
>
> Second-factor authentication requires a user to use two secrets. Strong forms of second-factor authentication exist that take advantage of mobile devices. Strong second-factor authentication provides a very high level of identity protection, not only for employees on a corporate network, but also for third-party users of the network such as partners and vendors.
>
> Strong second-factor authentication also makes it more difficult to inadvertently 'share' a credential with a co-worker. Imagine a scenario where an 'insider' wishes to sabotage a network for malicious purposes. If an insider simply stood over the shoulder of an administrative co-worker and learned the username/password, they could simply log in as their co-worker and perform malicious activity with the co-worker's identity. With strong second-factor authentication, this is not possible.
>
> Complementing the above, network segmentation is a concept where important resources are only made minimally accessible to computer systems that have a need to reach them.
>
> Focusing on the December 2013 attacks, whitelisting the software programs able to run on the POS terminal make it more difficult to install the malware. Whitelisting is a technique that allows only a specific set of software to be installed on a computer. If malware is installed on a computer, it will not match the "whitelisted" set of software and be rejected.

In addition, carefully monitoring network traffic with intrusion detection and intrusion prevention systems (IDS/IPS) could allow security analysts to detect the unauthorized network traffic patterns used by the attackers.

Although attackers are knowledgeable and persistent, there are ways to reduce the likelihood of a successful attack and mitigate damages. It is commonly understood that security in layers and defense in depth help combat attacks.

However, what is appropriate for any given organization is typically defined through an assessment of risk. Inputs to this process come from the core values of the business and require top-level engagement to be accomplished successfully.

Challenges and Recommendations

One of the questions we should be asking is, "with all of the knowledge, guidance and standards, how did the breach happen?"

One avenue to explore is the pace at which we bring lessons learned from the experts on the frontline of cyber into practice. Nothing in the breaches was new. We don't have a gap in understanding the attacks currently being executed.

Any security practitioner will tell you that good information security requires investment in people, process and technology applied consistently over time. But have we established a cybersecurity system and culture that inherently evolves at the

same rate as the threats? Is the bureaucratic process seen in government and industry groups inherently too slow to adapt? If so, there is no silver bullet in technology will help.

Another problem with many cybercrimes is that the loss has an asymmetric impact on its victims. For example, although a retailer is breached, the bank bears the cost of the stolen card data, financial institutions bear the cost of card reissuance, and consumers suffer the pain of changing cards and cleaning up accounts.

A major focus of the guidance and regulation that exists today is based on the organization conducting a risk assessment where one of the first steps is to assign value to the data. But if the impact of a breach is only partially born by the organization conducting the assessment, then the amount of protection given to that asset may not completely capture its systematic value.

Over the past decade we have significantly advanced our understanding of the threat landscape and best practices. What the most recent events are showing us is that there are opportunities to improve the translation of understanding the threats into mechanisms that turn this understanding into action. Evolving our approach and defense posture needs to be a Federal priority and we need to move forward now.

We should start with harmonizing breach notification laws so that enterprises and consumers alike know what is expected of them. The first state-level breach notification law was enacted in California in 2002; today, 46 states have similar laws.[7] However, we are still without a common Federal approach. Federal harmonization of breach notification laws is a good place to start.

Second, the Federal government needs to continue to foster the adoption of best practices across both the public and private sectors. Investments in Federal programs like HSPD–12 and the Transportation Workers Identity Modernization program are advancing the security infrastructure and generating significant lessons learned. NIST is also playing a key role in generating recommendations and guidance based on cross-sections of best practices and lessons learned from many industries. So, there is a good baseline to work from.

Finally, we must change the cybersecurity culture. Enterprises—large and small, public and private—need to embrace information security governance as a core responsibility. Industries where data has been viewed as a critical asset of the organization have found ways to integrate this into their DNA with many good examples existing in finance and the defense and intelligence communities.

However, in these cases, the value of the data is obvious. Losses are not asymmetrical. We may want to look closer at how industries where handling data, especially personally identifiable information (PII), is a byproduct and not an objective of the organization. Healthcare, retail and critical infrastructure are all very good examples.

In either case, we believe the focus should be on 1) how to accelerate the cycle from learning to implementation and 2) ensuring that the asymmetric nature of data is taken into account in cyberstrategy. Whether you want to drive adoption via incentives or directives is a public policy matter, but however we proceed, we need to proceed now.

Conclusion

Simply as a result of more transactions, data and devices going online, and without changes to the security posture of our most important industries and infrastructure, cybercrimes will continue to increase in frequency and potency. The asymmetric impacts will afflict those entrusted with sensitive data and the consumers, citizens and employees who put their faith in these systems.

Given the current situation, you must not let the perfect become the enemy of the good. The recommendations put forward would increase visibility into the threat environment and costs borne by individuals, organizations and the system as a whole. This insight needs to quickly filter into a more accurate assessment of risk and a system that is quicker to adapt.

Finally, the recent breaches have brought more attention to the cyber challenges we face today. We must take advantage of this focus, turn a negative into a positive, and move forward with policy that helps organizations embrace information security governance as a core responsibility. I urge you, your colleagues and the Administration to not let 2014 conclude without adoption of some measures that will better protect our economy and security.

---

[7] "State Security Breach Notification Laws." National Conference of State Legislatures. N.p., 21 Jan 2014. Web. 24 Mar 2014. <*http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx*>.

The CHAIRMAN. Thank you very, very much.

Because of an unusual circumstance, and with the permission of my distinguished ranking member, the first question from our side will come from Senator McCaskill.

STATEMENT OF HON. CLAIRE MCCASKILL,
U.S. SENATOR FROM MISSOURI

Senator MCCASKILL. Thank you. I adore you.

[Laughter.]

Senator MCCASKILL. I wanted it on the record. Both of you, I adore both of you.

[Laughter.]

Senator WICKER. Fails for lack of a second.

[Laughter.]

Senator MCCASKILL. I believe that ultimately the market is more effective at controlling behavior than the government. So let me start with a question that I don't think has fully been answered.

Mr. Mulligan or Ms. Richey or can any of you shed light on exactly how much fraud has resulted from this breach?

Mr. MULLIGAN. Are you speaking specifically to our breach?

Senator MCCASKILL. Yes, to the Target breach.

Mr. MULLIGAN. I will start, and certainly feel free—I can only speak to, about 15 percent of the cards that were taken were Target-branded product cards. The other 85 percent are third parties that we don't have visibility to.

But when I can tell you, what we have seen, two of the card products—one is a branded debit card, the other is a proprietary card, a card that only be used at Target—we have not seen any incremental fraud on those two particular cards.

We also have a Visa product that can be used broadly, just like anywhere else. There, on our $5.5 billion portfolio, we have seen about $2 million of incremental fraud or about a 0.1 percent increase.

Senator MCCASKILL. OK. Tiny amount, then, on your 15 percent.

Mr. MULLIGAN. On ours, yes.

Senator MCCASKILL. Ms. Richey, do you have any figures for us in terms of——

Ms. RICHEY. Yes. I would say, I mentioned in my testimony that 2 to 5 percent of accounts might be expected to experience incremental fraud.

We are actually seeing much lower numbers from the Target breach. I do believe that the rapid notification that Target provided, as well as the strong response from our member financial institutions, is responsible for limiting the fraud.

Senator MCCASKILL. OK. So what is the total, do you think, dollar-wise?

Ms. RICHEY. I don't have those dollars available right now.

Senator MCCASKILL. Does anybody?

Ms. RICHEY. We can get those for you. Of course, you have to realize we are still in relatively early stages. But we could provide those for you.

Senator MCCASKILL. Well, what I am trying to figure out here is how much fraud there was and who is holding the bag on the fraud. Because I think people don't understand that this—I mean,

I don't think people understand that Visa doesn't necessarily hold the bag on any of it, that most of this debit card fraud ends up with a local bank, that a lot of the costs associated with this breach, in fact the majority of them, fall to credit unions and local banks as opposed to Target.

Of the $61 million that you have said it cost your company, Mr. Mulligan, how much of that was marketing to try to reassure your customers that you were—and you are the good guys, by the way. I am not trying to say you are not the good guys. But how much of that $61 million was marketing as opposed to actual loss that you suffered?

Mr. MULLIGAN. For the $61 million that we recorded in the fourth quarter—any marketing expenses that we undertook would have been recorded in the normal course of our business. The $61 million was related to response costs, credit monitoring, activities such as that.

Senator MCCASKILL. Well, the credit monitoring that you are offering to your customers, that, in fact, is marketing.

Mr. MULLIGAN. We viewed that as a way to respond and help our guests for what is, we know, a difficult time for them, to provide for them not only credit monitoring but identity theft protection and identity theft insurance.

Senator MCCASKILL. I think it is terrific you are doing it, and I think it was smart for you to do it, and I think it was a wise corporate decision. But it was an optional activity you engaged in in order to try to repair the damage that had occurred as a result of the breach.

Mr. MULLIGAN. Yes, we were——

Senator MCCASKILL. Correct?

Mr. MULLIGAN.—focused on our guests, absolutely.

Senator MCCASKILL. OK.

And the estimate to the banks and credit unions is about $200 million. And those are costs that are not optional to them, correct? That is them having to reissue the cards and bearing the cost of doing that.

Mr. MULLIGAN. So the payment card industry has collectively determined that, importantly, consumers don't bear any of the fraud related to this type of activity.

There are commercial arrangements that underpin that. Those commercial arrangements provide both for the revenues that companies like Target pay in. They also provide for the remediation in situations like this.

Senator MCCASKILL. The point I am trying to make here is that I think it is confusing to the consuming public where this loss falls and where the costs are absorbed.

I know that there is $10 billion in more revenue to retailers as a result of the government getting involved in interchange fees, because interchange fees were $19 billion before the Durbin amendment and now they are $10 billion—less than $10 billion. So there was $10 billion extra that flowed to retailers as a result of those prices coming down. And I am not saying that was a good or bad thing.

I guess what I am trying to get at here is that I think it is very important that the risk be borne by those who must engage in the

activity to protect. Because if the risk goes somewhere else, it lessens the incentive to protect.

Now, I am not going to argue that you all have had a terrible thing happen to your company and that you are working hard to recover from it and you have been damaged. But there are many instances where people think there has been a breach—I think most Americans thought you guys were covering all the costs of this. When you said, "We are going to make sure that no customer loses a dime," I don't think that they realize that most of the dimes were being paid by somebody else in the first place.

So I think a clarification of where the risk falls is important for us if we are going to do anything as a government, because it is going to be much better to align those risks with the right incentives in the free market.

Ms. Richey?

Ms. RICHEY. I was just going to say that if there is any lack of clarity about who is bearing the loss here in the Committee, the financial institutions would make their customers whole in the first instance, as we know, with the zero-liability policies.

And then the payment networks, both Visa and MasterCard, do have a program to shift the cost back to a merchant if the merchant is shown to have been out of compliance with our industry standards.

Senator MCCASKILL. OK.

Ms. RICHEY. However, that program covers only a portion of their costs. And the reason for that is, just as you said, to balance the incentives so that each party is incented to reduce the risk and protect the consumer.

Senator MCCASKILL. I would love to get into the weeds on that, if you would help us with that information, Ms. Richey.

Ms. RICHEY. You mean right now?

Senator MCCASKILL. No. I mean later.

[Laughter.]

Senator MCCASKILL. No, no, no. I am done. I am done.

[Laughter.]

Senator MCCASKILL. No, no, I mean later. I mean, I really want to understand how these risks are being shifted in the marketplace.

Ms. RICHEY. OK.

Senator MCCASKILL. Thank you.

STATEMENT OF HON. MARK PRYOR,
U.S. SENATOR FROM ARKANSAS

Senator PRYOR [presiding]. Thank you.

What I am going to do is I am going to recognize Senator Thune and then, just for the Committee's information, we will recess for votes.

And we have four votes scheduled, I believe? Five votes scheduled.

So we will work that out, but I just wanted the Committee to know we will go to Senator Thune, then we will take as short a recess as we can, come back and conclude the hearing.

Senator THUNE. Thank you, Mr. Chairman.

Mr. Mulligan, we are still learning all the details of the Target breach, but we know that it affected two types of data. One was the payment card data of approximately 40 million Target shoppers and other personal data of up to 70 million customers.

The question is, what steps have you taken to provide your customers the assurance that their personal information is going to be protected going forward?

Mr. MULLIGAN. Senator, we have taken several steps. Immediately upon identifying the malware, we removed it from our system. We closed the portal that created the access point in the first place. We have narrowed the scope of who has access to our systems.

We also began an investigation and hired a third-party advisor who brought in a forensic investigator to do an end-to-end review, not just a forensic analysis but a review of our entire data security technology processes and controls. From that, we will have additional learnings, and we have already taken steps that we have learned from there.

We have enhanced our data segmentation. We have hardened our perimeter by increasing the use of two-factor authentication. And we have increased malware detection with something called "whitelisting." We accelerated the investment in that. And that essentially allows only the programs we want to run on our point-of-sale terminals to run.

We have also accelerated the investment in chip and PIN technology. A $100 million investment will complete the installation of guest payment devices this year and roll out the cards in early next year.

So we have taken many steps, and we will continue to have learnings from our end-to-end review and expect to continue to make changes.

Senator THUNE. Good.

Ms. Ramirez, you state in your testimony that, and I quote, "Although most states have breach notification laws in place, having a strong and consistent national requirement would simplify compliance by businesses while ensuring that all consumers are protected," end quote.

I agree with that statement, and I am wondering maybe if you can elaborate on the advantages of a consistent national requirement for breach notification.

Ms. RAMIREZ. We see a need for legislation for various reasons, and I think that is one. I think it is critical that there be comprehensive Federal legislation in this area. And we think that if that legislation and the standards that are set are sufficiently strong, that in that instance the Federal standards should preempt state breach notification laws.

Senator THUNE. OK.

And several of you, I think, have testified to the advantages of having a single Federal standard. And I am just wondering maybe if you would like to underscore the value of Federal preemption of what is a patchwork right now of state laws.

Ms. RAMIREZ. I am sorry, if I may add one more point that I want to make sure is also clear, in terms of our position at the FTC. It is also critical that the states be permitted to enforce in

this area, that there be concurrent jurisdiction on the part of the FTC as well as the states.

Senator THUNE. Right. OK.

Anybody else want to comment on the value of having a national——

Mr. WAGNER. Just a couple quick comments.

You know, we have talked about transparency here on the panel today, and transparency is absolutely critical. So having a common breach standard would make it easier to aggregate the data to know what is going on from a national perspective.

And then we also know from these crimes that they often—probably most often have a multi-state impact and very often an international impact. And having the Federal Government involved in breach notification seems to make a lot of sense to centralize that.

Senator THUNE. Anybody else?

Ms. RICHEY. I would just say that a single standard would ease the way for getting the notification out faster and spending less time and money on lawyers and more on informing consumers.

Senator THUNE. Dr. Loh, you are here today because the University of Maryland experienced a security attack, which exposed the names and Social Security numbers and dates of birth of more than, as you note in your testimony, 300,000 members of your community.

In your testimony today, you state that the University of Maryland experienced a second breach on March 15 but that this time that breach resulted only in one senior university official having their data breached.

And so the question is, why is that? Was that official the only target of that breach, or was it because of steps taken after the first breach?

Mr. LOH. They actually had unlawful access to far more information than was breached the first time, but we don't call it a breach because, except for that one individual, it was not made public, it was not circulated. And, again, I want to thank the FBI for their very expeditious and effective intervention that resulted in the successful mitigation within 36 hours.

The reason we are not saying anything more is because the investigation is still proceeding. But it is the case that no other information was made available. The fact that that one senior university official's name, ID, everything was put on the Web and on a public website, on Reddit, was simply because, well, the intruder wanted to show how clever he or she was and wanted the world to know.

Senator THUNE. I just have one last question, Mr. Chairman, and that has to do—again, I want to come back to Ms. Ramirez.

You testified today that your role at the FTC is to protect consumers and ensure companies take reasonable and appropriate measures to protect consumer information and that, to do that, the FTC uses both its unfairness and deception authority, deception authority being relatively clear-cut. And, in that case, if a company acts deceptively, it makes materially misleading statements or omissions, for instance regarding the security measures it has taken.

But a good number of the FTC's actions in data security have come under its unfairness authority, which some have argued provides less guidance to companies regarding which practices cross the line. Because most of these cases are the result of consent decrees, it doesn't seem like there is a record, or it doesn't produce a record of precedential value.

So the question is, short of regulations, should the FTC make public the rationale that they use to determine what is unfair so that companies have better guidance?

Ms. RAMIREZ. Senator, I have to disagree with the critiques that have been made of the FTC in this arena. I think that we have provided good guidance.

The approach that we take when we exercise, frankly, both our deception authority and our unfairness authority in this area is one of reasonableness. As a law enforcer, what we do is really driven by the specific facts of a given case. And the documents that are part and parcel of our consent decrees demonstrate and explain the bases for our allegations and also what we believe are remedies and actions that a company should undertake.

So, in our view, we have provided guidance. And the actions that we have taken really go to very basic and fundamental failures on the part of companies that we think are unreasonable and, therefore, that would be a violation of Section 5.

So I do take issue with that. We provide a great deal of guidance, also, to businesses as part of our outreach and educational efforts. And I believe that companies can discern the approach that we take.

It is a process-based approach, where we urge companies to do a very thorough risk assessment based on the type of information that they collect and that they use and that they then, in turn, develop a program that would be able to address any risks to which that information might be exposed.

We also think it is absolutely critical to have one person, at least, who would be in charge of any data security program.

Senator THUNE. Is that guidance made public?

Ms. RAMIREZ. Absolutely.

Senator THUNE. OK.

All right, Mr. Chairman, I see we are out of time and we have to run and vote, so I yield back.

Senator PRYOR. Thank you.

And that is what we will do. We are going to recess for a little while; I don't have a time certain. My guess is it will be 40 minutes or so, but I don't know exactly, depending on how many actual votes we have on the floor. There is a little bit of conflicting information about it, whether we have four or five votes.

But, nonetheless, what we will do is we will recess. And probably, just for everybody's benefit, we will probably try to start as we are doing our last vote on the floor, because members can vote and then come back here. So we are trying to do that.

So, with that, what we will do is we will take the recess now, and we will reconvene subject to the call of the chair. Thank you. [Recess.]

The CHAIRMAN [presiding]. You know, it is nice, we are actually just piling through judges. And that has been an enormous problem

in our system. And we did something called the nuclear option, which means if you can get past cloture, then all you need is 51 votes. That is what everybody—we have five judges, which may not be of any interest to you.

[Laughter.]

The CHAIRMAN. OK. Mr. Mulligan—where is my Mr. Mulligan? There you are.

Have you all been nice to Mr. Mulligan?

[Laughter.]

The CHAIRMAN. OK.

My staff, as you know, have prepared a report analyzing the data breach at your company. And we do a lot of reports.

One that doesn't have anything to do with you or the question—and I shouldn't even be saying it—but I am interested, so I am going to say it—and I am Chairman, so I can say what I want.

[Laughter.]

The CHAIRMAN. A lot of moving companies, if you want to move, you sign a contract, they put your stuff in the moving van, and then they take it about 2 miles and then park in an alley and call you up and say, "The price has just tripled." And, you know, you say, well, that doesn't happen in America. The point is it does. And it is very disturbing. It is very disturbing.

So that is why we focus a lot on these kinds of things. It is not that we are nasty.

Richard, you are not nasty, are you? Senator Blumenthal? You are not nasty. You are smart, you——

Senator BLUMENTHAL. Ask my wife, Mr. Chairman.

[Laughter.]

Senator BLUMENTHAL. Never.

The CHAIRMAN. That is right.

My granddaughter and his——

Senator BLUMENTHAL. Wife.

The CHAIRMAN.—wife are together at school.

Senator BLUMENTHAL. Your granddaughter and my wife——

The CHAIRMAN. I didn't mean that——

Senator BLUMENTHAL. Your granddaughter and my daughter were together in school.

The CHAIRMAN. Were, yes, that is right.

Senator BLUMENTHAL. Yep.

The CHAIRMAN. At different levels.

Senator BLUMENTHAL. Yes.

The CHAIRMAN. Right.

[Laughter.]

The CHAIRMAN. So, anyway, Mr. Mulligan, we have prepared this report, and I want to know if you have read the report.

Mr. MULLIGAN. I have. I had a chance to review it last night.

The CHAIRMAN. You did last night.

The report walks through the many steps the attackers had to go through in order to hack your company. And then it explains how Target could have prevented the breach if you had stopped the attackers from completing even just one of the steps.

Let me give you a few examples. You could have prevented the breach if one of your vendors, a small Pennsylvania company called—is it "Fazio" or "Fazio"?

Mr. MULLIGAN. My understanding is it is "Fazio."

The CHAIRMAN.—Fazio Mechanical Service had better security practices.

Will you acknowledge that poor vendor security was a factor in this attack?

Mr. MULLIGAN. Yes.

The CHAIRMAN. And once the attackers had gotten into your network, you did not stop them from gaining access to your company's highly sensitive consumer data. Will you acknowledge that Target failed to properly monitor your computer network for the intruders?

Mr. MULLIGAN. Senator, it is my understanding that we did have proper segmentation in place. As recent as 2 months prior to the attack, we were found to be PCI-compliant, and that includes network segmentation.

But your question is an excellent one. How they migrated from the outermost portion of our network to our point-of-sale data is an excellent question, and I don't have the answer to that.

The CHAIRMAN. OK. And who is "they"?

Mr. MULLIGAN. How the intruder, excuse me.

The CHAIRMAN. OK.

Chairwoman Ramirez, I congratulate the Federal Trade Commission for its recent announcement of its 50th data security case.

The FTC has been successful in pursuing data security cases using the authority under Section 5 of the FTC Act. As you know, Senator Feinstein, Pryor, Nelson, and I have introduced data security legislation, as Senator Pryor has done in previous years, all to no avail so far—legislation the FTC has consistently called for.

Can you talk about why you see the need for such legislation? Why isn't your existing authority under the FTC Act enough?

Ms. RAMIREZ. Chairman, thank you for your question. And, again, I want to thank you for your leadership in this area.

The FTC has undertaken very critically important work in this arena. But I think that our experience and what we see happening in the marketplace really does show that companies are continuing to under-invest when it comes to data security.

And that is why we believe that more needs to be done in this area and why we think that Congress absolutely needs to take action to have Federal comprehensive legislation that addresses the issues of data security.

And, in particular, we want to highlight things that we think are critically important relative to enforcement authority on the part of the FTC. And that is that we feel that it is critical that the FTC have civil penalty authority so that there can be appropriate deterrence. We also feel that it is important that any legislation give us APA rulemaking authority so that the agency can have the flexibility to implement any legislation and to adapt to changing technology in this arena.

And then, in addition, we feel that it is also important for the FTC to have jurisdiction over nonprofits. Currently, we do not have jurisdiction over nonprofits, and we do see that universities and other nonprofits are falling victim to intrusions and that it is important for the nonprofit sector also to have reasonable security measures in place so that Americans' information can be protected.

The CHAIRMAN. But they will precisely at that point tell you that self-regulation works.

Ms. RAMIREZ. We believe that self-regulation is an important element of all of this. Data security is a complicated issue, and in order to really address it effectively, we need to do it in a multi-pronged way.

So we believe that self-regulation that is robust and where you have backup enforcement by the FTC, for instance, that that would be a good and important complement to the civil law enforcement that we undertake.

The CHAIRMAN. But, in essence——

Ms. RAMIREZ. But it wouldn't—in my mind, it is not enough.

The CHAIRMAN. You are saying it is not enough.

Ms. RAMIREZ. That is correct.

The CHAIRMAN. Yes. But whether it is cybersecurity, whether it is this, whether it is almost anything else, self-regulation always solves the problem.

We had, as you know, recently a chemical spill in Charleston in West Virginia. Nine counties just couldn't drink water, including my house, and it was not a pleasant experience. And I found out rather quickly that there is no regulation, they are under no Federal regulation, no state regulation—they can do exactly as they please.

And so one of the people who was really trapped by this, who is my, sort of, chief of staff for my West Virginia operations, has two young children. And I talked to her this morning, and she said—and she had just been on a trip to India, in fact, to look at water, new ways of doing water—that two more leaks had been discovered on that river, just causing one to be blindingly angry and infuriated at ourselves for allowing that to happen.

I was a Governor for eight years; I never did anything about it. Every time I drove into Charleston, which I did hundreds and hundreds and hundreds of times, I always came directly toward those tanks that held all this toxic stuff which leaked, and I said, that doesn't look very good to me, it looks kind of crummy.

It is sort of like the pictures in Washington State before everything went wrong. Everything looked fine, but if you knew that there was a lot of mud there, your mind would lead you to other kinds of conclusions. But your mind doesn't choose to dwell on things which aren't of the moment.

Anyway, so I am encouraging increasing hostility towards giving the FTC—I am hearing this from others—authority to address consumer protection issues like data breaches. That is a common complaint from some. And it reaches ears easily because people like to hear about the Federal Government not being able to do its work, or failing to do its work.

Unlike years past, when this committee routinely gave the FTC the tools it needs to do the job, I am now constantly hearing about the dangers of an overzealous FTC, overregulating and overburdening American businesses, a lot—hearing it a lot, and in this committee.

My data breach bill, which is S. 1976, gives your agency basic rulemaking authority to set data security standards, just as Congress did in the Gramm-Leach-Bliley and the children's online pri-

vacy laws. I don't think that is a controversial idea, but some people do.

Chairwoman Ramirez, can you explain, please, to these skeptics, through me, how the FTC goes about setting these rules so that, one, I can be satisfied that you are not out to ruin industry for the pure pleasure of doing it but you are trying to do your job; how the Commission has a careful and deliberative process that does not lend itself to the type of regulatory chaos that some fear? And then can you explain how these rules will help protect consumers from data breaches?

Ms. RAMIREZ. I would be happy to.

Let me say that, first of all, the call for legislation in this area is a bipartisan call. The Commission unanimously supports the enactment of Federal legislation in this area and supports specifically the pieces of legislation that I have outlined.

Let me also say that, in response to the critics of the FTC, anyone who looks closely at the work that we undertake can see that we do our work in a very balanced way and that we absolutely want to be—our job is to protect American consumers fundamentally, but we absolutely do listen to the concerns of industry.

And I think when you look at the body of casework that we have in this area, the 50 data security cases that you mentioned, I think people will see exactly what the basis for these are and, in fact, that the actions that we took were justified.

In response to your specific question about how we employ APA rulemaking authority, in my initial remarks I referenced the CAN–SPAM Act, which is one example of a situation where we were given APA rulemaking authority. Any rule that the agency would promulgate would go through a notice-and-comment period, so stakeholders would have an opportunity to give input. Any rule that we ultimately would impose would be based on the evidentiary record that would be developed over the course of the rulemaking process.

And the reason that we ask for that is that it is critical that the FTC have flexibility in this arena to implement any legislation. And two main issues, I think, are the ones that I want to highlight.

One is that we have to recognize that technology is just moving very rapidly. So, a decade ago, no one would have predicted that facial recognition technology would be so readily available, for example, or that geolocation information would be so easily obtainable today. So it is critically important that there be flexibility that is embedded in any legislation to allow the FTC to adapt any rule to emerging and evolving technology.

By the same token, it can also be to the benefit of businesses to grant the FTC that flexibility, because we may be able to lift certain requirements that may no longer be necessary over time. And that certainly happened in connection with our implementation of the CAN–SPAM Act.

So, in my view, it really would be to the advantage of everyone—consumers as well as the business community—to grant us that flexibility.

The CHAIRMAN. I thank you.

I am well over my time, and it is time for Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much, Mr. Chairman. Thank you for holding this important hearing and for working on some important legislation.

I think we all know that this is no longer one singular problem, as we have heard from our witnesses today. In fact, *The Washington Post* printed an article yesterday showing that the Federal Government notified 3,000 U.S. companies of a breach in just the last year.

And I think it calls attention to the fact that we need to move on cybersecurity legislation, that we need to move on some of the notification bills and the work that Senator Rockefeller is doing, Senator Leahy is doing. I am on both committees, so I have been immersed in this.

As Mr. Mulligan knows, we had another hearing, and Chairwoman Ramirez, in the Judiciary Committee. And one of the things we focused on a lot there that I continue to believe is important is, one, going after the people that did this and working with the Justice Department on that. That has to be a top priority. But, number two, how we prevent this going forward.

And one of the things that I found pretty shocking was that in America we have 25 percent of credit card transactions in the world but we have 50 percent of the world's fraud. And, as we know, some of the other countries have moved to the chip and PIN technology. I know that Target tried some of this technology—maybe you can talk about that—a few years back, but it wasn't adopted by other companies.

And so I think I would start with that. What do you think we need to do to stop this from happening, in terms of adopting some of the technology? And how long do you think it is going to take, when we already have parts of the world that are already adopting this? It is currently the standard in Europe.

So maybe we could hear from you, Ms. Richey, first.

Ms. RICHEY. We do believe that it is necessary for the United States to join most of the rest of the countries of the world in adopting the chip technology to control fraud in the face-to-face environment.

We have set out a roadmap for EMV chip adoption, and we announced that in August of——

Senator KLOBUCHAR. Great.

Ms. RICHEY.—2011, with the idea that it would take probably around 4 to 7 years to get to a critical mass of chip adoption, based on our experience in other countries.

I am encouraged by the level of enthusiasm toward the chip project that we are seeing in the wake of these recent events. And I am hopeful that by our liability-shift date in 2015, October 2015, that we will see substantial adoption in both the merchant and the issuing bank side.

Senator KLOBUCHAR. And do you think it would be better to have the PIN rather than signatures? Would that be safer?

Ms. RICHEY. "Safe" is an interesting word in this context.

Senator KLOBUCHAR. OK. Would that lead to less fraud?

Ms. RICHEY. It might initially lead to less fraud. PIN does reduce lost and stolen fraud. So PIN does nothing to prevent the criminal from counterfeiting a card, unfortunately. And about 70 percent of the fraud that occurs in physical locations, brick-and-mortar stores, is counterfeit, not lost and stolen.

So we believe the bigger problem is counterfeit. It is also easier for the criminal to accomplish because they can do it by stealing data, not by having to take possession of, you know, thousands or millions of physical plastic cards.

So we believe that the best thing for the industry to do is to focus on chip and that trying to change the environment between PIN, signature, and no cardholder verification, which are our current methodologies, would just slow things down and increase the cost.

So, therefore, we are saying the issuer could have the choice, based on their own risk profile, whether to issue with chip and PIN or chip and signature, and similarly in the merchant environment, where today about two-thirds of the merchants don't currently deploy PIN.

Senator KLOBUCHAR. Right.

And I think we know, I mentioned—Mr. Mulligan, maybe you want to address this—that Target had tried to go with the chip technology. And what happened?

Mr. MULLIGAN. We did. A little more than 10 years ago, we introduced what we call guest payment devices to read chip cards. And we introduced our Target Visa card, actually, with chips enabled in it 10 years ago.

The real benefit for consumers comes with wide adoption, though, when those cards are widely used and they are widely read throughout the economy. And we have seen that in other geographies. After we went about 3 years by ourselves, we determined that it didn't make much sense for us to continue, given that there was no real benefit to consumers broadly.

We have continued to support, in our case, chip and PIN, but we agree that moving to at least chip-enabled technology is a positive step forward.

Senator KLOBUCHAR. Are you speeding up your adoption of that now?

Mr. MULLIGAN. We are. We have accelerated that. It is a $100 million investment for us. And we will have the guest payment devices in September, and we will issue cards, chip-enabled cards, and read them early next year.

Senator KLOBUCHAR. And, Mr. Wagner, as a subsidiary of Datacard, which is also a Minnesota company, how does your company view the transition to chip cards? And how have Entrust and Datacard been involved in making recommendations to the finance and payment networks on implementing new cards and new security methods?

Mr. WAGNER. Well, Datacard is, in fact, the world leader in producing equipment to encode financial transaction cards, both magnetic stripe and of course EMV other places in the world. And so we are a big supporter of the EMV technology.

You know, one of the things, when you combine security, you know, it is clear that the chip and PIN is a more secure way to do it, but there is obviously balance and usability that needs to be

considered. But when you consider from a security perspective, the chip and PIN is a more secure way to go about it. But either is better than the current mag-stripe environment.

Senator KLOBUCHAR. And, Mr. Chair, if I could just ask one more question——

The CHAIRMAN. Of course.

Senator KLOBUCHAR.—of Chair Ramirez?

Many of the large data breaches and the hacking operations are perpetrated by people outside the U.S. And there is no shortage of crimes that they could be charged with, but it can be very hard to bring them into our courts because they operate largely overseas.

In the case of the Target breach, I understand that *Business Weekly* has identified a Ukrainian operation that could be responsible. Again, the investigation is under way; this is just what we read in *Business Weekly*.

But can you discuss how you work with law enforcement on investigations? I know I asked this of the Justice Department in a Judiciary hearing, but what steps do you think we could be taking to make it easier to get these international hackers into a courtroom to stop them?

Ms. RAMIREZ. As to your specific question, I do have to defer to the criminal law enforcement authorities to get into the details of that. But I will say that the FTC works very closely, in terms of our own work, in parallel with our criminal law partners in these areas.

We, of course, are focused on the front end, how retailers and other businesses are protecting consumer information. But, again, we work in parallel with and I think our efforts are complementary to the efforts of criminal law enforcers who are seeking to locate and punish perpetrators.

Let me also add that we do a tremendous amount of work on the international front, working with civil law enforcement agencies around the world to address these issues. That is a significant part of our own engagement. And we use authority that has been given to us by Congress under the SAFE WEB Act to be able to pursue civil law enforcement where needed. And so we do want to partner with other law enforcers, because we have to these days.

Senator KLOBUCHAR. And so do you think we should be doing more, as we negotiate trade agreements, as we work with these other countries as part of security agreements, in terms of trying to come up with some international standards?

Because it seems to me that more and more of these cases are outside of our borders, in terms of who is perpetrating them.

Ms. RAMIREZ. Absolutely. I think increasingly we need to be working with international partners around the world, and we absolutely have to focus on that set of issues, as well.

Senator KLOBUCHAR. Thank you very much.

The CHAIRMAN. Thank you.

Senator Pryor?

Senator PRYOR. Thank you, Mr. Chairman.

And let me follow up on that, if I can, Chairwoman Ramirez. With the FTC working with other agencies, other Federal and state and other law enforcement agencies generally, plus the international community, is there a formal process there? I mean, do

you have these formal relationships where you sit down every day or every week or every month with these folks? Or is it more on a case-by-case, ad-hoc basis?

Ms. RAMIREZ. We do work regularly with sister agencies here domestically. It does operate on a case-by-case basis.

We do also have specifically a Criminal Liaison Unit, because as part of our overall enforcement work we do partner with U.S. attorney's offices. We also do close work with main Justice and then also with the FBI, Secret Service. But specifically on these issues, it tends to be in conjunction with specific investigations.

On the more global level, we do work through multilateral organizations as well as through specific bilateral relationships that we have with counterpart law enforcers around the globe who also have consumer protection authority. And then we do also engage, where necessary, where appropriate, with criminal authorities around the world, as well.

Senator PRYOR. You know, one reason I ask is my experience with law enforcement is that sometimes they will form what are sometimes called task forces, you know, where they will have multi-agency or multi-jurisdiction.

I didn't know if FTC serves in, like, a task force-type setting where you have regular meetings, where people are focused on this, trying to find solutions, trying to head some of this off before it starts. Are you all involved in anything like that?

Ms. RAMIREZ. It really is on more a case-by-case basis. Again, our focus is on the civil law enforcement side and on the front end. But we absolutely will cooperate very closely where it is necessary, and we do stay in close contact with domestic criminal law enforcers.

Senator PRYOR. OK, let me go down to the other end of the table there.

Mr. Wagner, I know in both the Rockefeller bill and also the Toomey bill, they use the word "reasonable" policies—"reasonable" is the key word—policies to ensure consumers' private data is protected.

And, you know, obviously, "reasonable" is a little elastic, a little situational. And that may be the best word to use, but could you please speak to that and kind of talk about what principles are contained within the, kind of, concept of "reasonable"?

Mr. WAGNER. Well, the key principles that we would espouse are those of information security governance, understanding the risks that the enterprise has around information security at a high level, at a corporate, at a board level, understanding which information assets have value, and making sure that that is not just an assessment of the value to your organization but, as we are seeing, the effect can be ecosystem-wide, and so making sure that those, you know, asymmetric values get considered at the risk officer level, at the corporate level, so it can be dealt with.

Senator PRYOR. Does anybody else on the panel want to comment on "reasonable" and, you know, what that means in the context of what you do?

Ms. RICHEY. Well, there are a whole set of well-known security standards applicable either on an industrywide basis or broadly across all industries. And I believe that many of them have very

specific things that need to be done but that at the same time they are flexible.

So there is a whole custom and practice of the trade that you would want to look at based on the risks that you have identified as to whether the measures that you took were in accordance with those standards.

Senator PRYOR. And is that a good starting point here?

Ms. RICHEY. I believe so, yes.

Senator PRYOR. Yes.

Did you have something?

Mr. LOH. Yes. The word "reasonable" was what caught my attention in Section 2 of the bill, "requiring reasonable measures and procedures for information security."

Even though it has only been about 5 weeks since our major data breach, I have already asked for the estimates of the cost to have, quote, "reasonable" defenses and reasonable" perimeter defenses, penetration testing, and protection of sensitive information.

It can range from a few million dollars to as high as $30 million to $50 million. They have quoted me figures from other studies that say that, at least in academic settings, it is approximately $100 per every identity stolen. So if we had 310,000 stolen, the cost, as a rough estimate, is 310,000 times $100.

And the question I think that Mr. Mulligan raised, which I thought was an excellent question: Who shares in the responsibility for protection?

It would bankrupt most universities to spend $20 million, $30 million in cybersecurity protection, especially when there is no 100 percent guarantee anyway. Is this something that should be shared more widely between private business, universities, and the Federal Government?

To take one example, Social Security numbers. Why don't we devalue Social Security numbers? Why not require financial institutions not to use Social Security numbers so that there is no longer the incentive to steal Social Security numbers?

If one doesn't do that, one shifts all of those costs to, at least in this case, higher education institutions. And so it is a balancing between risks and costs. And all I can tell you is that the costs can be staggering. And even then, all of the experts that we have retained are telling us there is no 100 percent guarantee.

Ms. RAMIREZ. I wanted to add a few words from the perspective of the Federal Trade Commission on this issue.

We do believe that the reasonableness is the right approach. Given the different types of companies that we have jurisdiction over across many industries, we think that it is critical to have flexibility and, again, to have a very fact-specific approach. At the same time, we certainly understand the challenges that Dr. Loh has identified.

And going back to your question about certain things that the Federal Government can do, one area where we have been participating in a task force has been in connection with identity theft. And as part of that task force that was set up under the Bush administration, a number of different Federal agencies have made recommendations about how to deal with issues such as Social Security numbers to minimize the risks of ID theft.

So I do think that while this is a complicated question, there are many places where the government can play an important role. And, to me, data security legislation is one step in that effort, but I think there are other things that need to be examined, including the way personal information is being utilized.

Senator PRYOR. Thank you, Mr. Chairman.

Thank you.

The CHAIRMAN. Thank you, Senator Pryor.

Philosophically and realistically, that was an interesting discussion because—and it gets back to something that I talk about as often as I can. Unless this country is willing to get serious about infrastructure, from which I mean cybersecurity to 200,000 pound water tankers crossing 75,000 max pound bridges all over West Virginia so that they can build a fracking platform—if we don't have the infrastructure, which is research, which is NIH, which is the Cancer Institute, which is Alzheimer's, which is everything, plus the hard stuff, the roads—I mean, you know, we have a lot of pipelines in West Virginia. Nobody knows where they are. They carry gas, but somebody goes in to build a house and breaks through five layers of pipelines that nobody knew were there.

At some point, the sense of forgiveness runs dry, that if we are going to be a serious country, continue to be a serious country, we have to do infrastructure. We have no choice.

If you said, Senator Rockefeller, are you for raising the gas tax, I would say yes. I believe in user fees; I always have. If you have an objective that you want—you want to build roads and bridges—then you do that thing which is necessary to make it happen.

If you choose not to—you are ideologically pure—you probably win your next election, and your state declines and fritters away. Or people, young people, make the conclusion, as they have, or some of them already, on our water spill, the toxic water spill, for which there was no state regulation whatsoever—of which I was partly responsible, because I was Governor for 8 years. And I told you, I kept looking at these tanks and wondering what they were doing there but did nothing about it.

If you don't take responsibility for your future, you have no future. And that gets to the very bottom of what divides this Congress. It is not Republicans and Democrats. Roy Blunt and I have been friends for years. I got him to do something which he didn't want to do, for which he has forgiven me for getting him to do it because he finds it not that undoable. Plus, he likes me and I like him. OK? So things work.

But you have to be willing to raise taxes to pay for things where we are eons behind. STEM, modern bridge structures—I mean, the list is endless: NSF, NIH, NIST. You want a good way to find out where a good standard is? You go to NIST. That is where the cybersecurity people want to go. They will do it fairly. They will do it, but it will cost.

And so to Dr. Loh, who runs a university, which does not have endless amounts of money, I am full of sympathy. But I can't walk away, as a Senator, from being part of the solution to his problem. And that is what we are doing here; we are walking away year after year from being part of the solution to the problem.

If you want good infrastructure, you have to pay for it. If you are going to pay for it, you have to raise taxes. Then the question is, how do you raise taxes? Then you get into the 1 percent versus the—and then that becomes a lot of talk. But the point is you either get the infrastructure or you don't. And if you don't, your future is dim.

It was very interesting when the President called, accurately, Russia an important regional power. Mr. Putin must have been unhappy at that, but it was accurate because of the size of his economy and because of what he has not done and they have not done over the years. In projecting power, projecting toughness and all the rest of it, they have not built things up. My son-in-law lives there; he knows. You can't escape that.

So that is my little editorial. But, to me, it is the way we improve this country. The way we help Dr. Loh, the way we help everybody, is that we are in this together, that we have to share responsibility, that we don't point fingers. We are all to blame.

We are in the habit of being comfortable. We are in the habit of thinking that the world is as it was 30 years ago. Now, that is a stupid and trivial thing to say, but it is just totally true. It is totally true. So I am trying to make life tougher on us.

I am not running for re-election, so it is easy for me to talk like that. But if I were running for re-election, I would talk like that. Or else I don't belong in this job; I shouldn't run for the job.

So that is just my thought. Now, I have gone over my time. And Senator Markey has been here, and he doesn't like it if I go for over a minute and a half. But I am just going to ask my question and hope for Roy and Ed's forbearance.

Mr. Mulligan, this is for you. According to press reports, attackers gained access to the Target network through the Pennsylvania vendor, which we have discussed already. Does Target require any particular level of security of its third-party vendors?

Mr. MULLIGAN. We do assess the inherent risks of our third-party vendors and rate them on a risk scale and determine which of those we need to review, which of those we don't, Senator. We have a process for doing so.

The CHAIRMAN. I am not sure what the answer is.

Mr. MULLIGAN. We do. We do. We have standards, Senator. And we have an audit process to ensure they are meeting them.

The CHAIRMAN. A lot of people have audit practices. Not all of them are enforced. That is a high bar question, I admit.

Mr. MULLIGAN. We have a process where we routinely review the inherent risk. And those with high risk we evaluate periodically. Those with a medium risk we evaluate less often. And those we deem low-risk we don't evaluate, Senator. We——

The CHAIRMAN. OK.

Do any third-party vendors have access to Target's point-of-sale systems? And if so, what security standards apply to them?

Mr. MULLIGAN. Anyone who has access to our point-of-sale networks, the same security standards would apply: two factor authentication, as is required by PCI. And beyond that, anyone, whether our own team members or if we have, say, technology contractors working on them, they would apply similarly.

The CHAIRMAN. See, Senator Markey, we have the rhetoric of attention and auditing but not necessarily the fact of. One can still get away with rhetoric in this country. One can get on the evening news with brilliantly sculpted rhetoric. It doesn't mean you are doing anything.

I just threw that your direction. You are not a media hound, so I am not accusing you of being that kind of person. I mean, I would if I knew my audience better, because I would have fun doing it and you would have fun squashing me.

At the same time of the breach, who at Target was ultimately responsible for the company's data security?

Mr. MULLIGAN. Senator, we have multiple teams that work in data security. At the time of the breach, various elements reported it to several different executives.

The CHAIRMAN. Now, you see, that worries me. That worries me. You had a former CIO, Beth Jacob, and I want to make sure she doesn't get run over by a bus in this discussion.

It is true that Target data security responsibilities have been divided up, as you indicate, among a variety of staff and not under a chief information security officer. But what I am obviously getting at is, at some point, the CEO and the Board of Directors have to accept responsibility for what is happening.

That is why I mentioned this morning with data breaches—that you should have to report it to the SEC. And there was no law. I just called up Mary Schapiro, who was there at the time; she said, sure, I will do it.

And I did the same thing with coal mines. We have a lot of coal mine disasters in West Virginia. So any time somebody is killed or there is a coal mine disaster, it has to be reported, because that is helpful to investors and shareholders about their decisions.

But I believe in responsibility. I think it has to come down to a point, a source point. And I think that has to be a Board of Directors and the CEO. And then you can scatter the responsibility however you want.

I have talked too long, and now I have to figure out who got here first.

I think, Roy, did you get here first?

Senator BLUNT. I was here first.

The CHAIRMAN. Roy was here first.

So, Senator Blunt, I am sorry. Senator Blunt.

STATEMENT OF HON. ROY BLUNT,
U.S. SENATOR FROM MISSOURI

Senator BLUNT. I thank the Chairman.

And the Chairman and I are good friends, and the thing he talked me into doing was co-chairing with him an effort to be sure we understood what all the alternatives are out there at a staff level on health care. And whether I wanted to know it or not, I needed to know it. And, once again, he figured out something that was better for me than I probably thought it would be.

But thank you all for being here. It has been a long afternoon, people coming and going. I may very well ask a question that has already been asked, but as a rule here, even if everything has been said, if everybody hasn't said it yet, it is still OK to repeat it.

[Laughter.]

I just sort of—you know, whenever we set this hearing, I think there were 46 different requirements to comply. There may be more than that by the time we get to the end of the hearing, but there were at least that many.

And my first question is simply a "yes" or "no" question. Do you believe that a uniform national standard for data breach notification would benefit consumers? And just "yes" or "no" is all I would like to have there.

Ms. RAMIREZ. I will start. Yes.

Senator BLUNT. Dr. Loh? A uniform standard of notification?

Mr. LOH. Yes.

Mr. MULLIGAN. Yes.

Ms. RICHEY. Yes.

Mr. BESHAR. Yes.

Mr. WAGNER. And yes.

Senator BLUNT. Well, that is what I think too. And hopefully we can figure out how to do that. And I think the Attorney General recently called for that uniform standard, as well, and it is something that hopefully this Congress can accomplish. [Editor's note: Senator Blunt requested that the Attorney General's statement in this regard be placed in the record. See pp. 76–77, herein.]

One of the questions the Chairman asked—and maybe it was your answer, Mr. Mulligan. At the time of the breach, was there more than—weren't there multiple breaches of data in what happened in Target in the last part of last year?

Mr. MULLIGAN. We had breach of our systems, Senator, and two types of data were removed.

Early in December, or mid-December, on December 19, we indicated that approximately 40 million credit card account numbers had been removed from our systems.

And then, once verified, we also, on January 10, provided notice that certain personal information, including name, address, e-mail, and phone number, in various combinations, had also been removed in the same breach.

Senator BLUNT. So if I understand this right, in the same breach, does that mean you had all the information for all 40 million people? Or did you have some of them you had individual information and others you just had card information that didn't identify it to an individual?

Mr. MULLIGAN. That is correct. And the overlap between the two, while one would think it would be a relatively simple process, it was not. We know that there was at least 12 million of the records that overlapped and likely more than that.

Senator BLUNT. So where you had the breach of information but you didn't know who that related to, is there any way you could have—who could you have notified there if you wanted to notify an individual customer that their card information had been shared in ways you wouldn't have wanted and stolen, in effect, from you?

Mr. MULLIGAN. Given the nature of our breach, Senator, we felt that the best way to notify customers was very broad public disclosure. We did so on December 19 through the media, through our website, through social media. We did so again on January 10 related to the personal data.

In both cases, we augmented that public disclosure by e-mailing. In the first case we e-mailed about 17 million of our guests and in the second case about 47 million guests.

Senator BLUNT. How did you know who those 47 million were?

Mr. MULLIGAN. We had their e-mail addresses.

Senator BLUNT. And that was for everybody in that particular file, or everybody that had shopped within a window of time, or how did you know that?

Mr. MULLIGAN. For the 70 million records, those are the individuals we had accurate e-mail addresses for.

Senator BLUNT. For the 47 million e-mails out of the 70 million.

Mr. MULLIGAN. Correct.

Senator BLUNT. I see.

And, Ms. Richey, I think—what did the Chairman say? Does Visa—no. A level of security for—it was asked about the company. I thought of a question then. Does your company require any level of security for the merchants who use Visa? And are you changing what that level of security is?

Ms. RICHEY. Yes, we do require a level of security. It is the level embodied in the PCI data security standards.

And we also require for large merchants that they provide us a validation by an independent security assessor once each year that they are in compliance. For the smaller merchants, we require a self-assessment questionnaire that is administered by the merchant bank that has set them up to accept payments.

So that is what we have in place today. The PCI Council actually administers that standard, and they review it periodically and promote improvements to it.

Senator BLUNT. And have you given notice of a new level of standard that you want merchants to have by sometime in 2015?

Ms. RICHEY. So there are two different things going on here. One is the security standard, how they secure the data in their environment.

Senator BLUNT. Right.

Ms. RICHEY. And the other is to devalue the data in their environment so that they would no longer have valuable data and no longer be targeted by thieves.

So the standard for October 2015 is for these EMV chip cards, where the card actually sends a one-time-use signal so that even if you steal all the data relative to the card it can't be reused to commit fraud.

So the standard for 2015 is to implement the EMV standard by placing EMV terminals in the stores and outfitting them with the proper technology on the back end, failing which the merchant would be liable for the fraud if a chip card, an EMV chip card, is used in that terminal. So that is that standard.

Senator BLUNT. OK.

My last question for you and then anybody else who wants to answer it is, do you believe there is any benefit in Congress in the law trying to specify exactly what the card standard should be? If we said in law you would have to have a chip in the card or you would have to have a chip and a PIN number in the card, is that, in your view, a good thing or an unhelpful thing?

Ms. RICHEY. Generally speaking, I would say that our success across the world has been through this liability-shift mechanism. It allows the flexibility in the different merchant environments for them to move in that direction.

Senator BLUNT. So "liability shift" means if they don't secure things as you required, they would have a higher level of liability as a merchant.

Ms. RICHEY. Right. And that allows them to set the pace of their transition according to their environment and the risk in their environment. So we believe that should be effective. We have seen it over and over again across the world.

I hesitate—naturally, we would like to get out of the business of having to administer this ourselves, but when we have seen the few governments that have tried to mandate technologies in other parts of the world, they tend to have unintended consequences and actually make it more difficult to move forward with new types of technology that can leapfrog current technology. So that would be my hesitation on that.

Senator BLUNT. Anybody disagree with that?

My sense has been that the thieves, the hackers would always be more nimble than the Congress. And we prove that on a regular basis, our lack of nimbleness. And if you are too specific in law, all you do is create a roadmap as to what you have to do if you want to break the code.

But what were you going to say, Ms. Ramirez?

Ms. RAMIREZ. I was going to agree with what Ms. Richey has testified to. We believe that a flexible approach is the right way to go here.

Senator BLUNT. Thank you, Chairman.

The CHAIRMAN. Thank you very much.

Ah, you have made it back.

STATEMENT OF HON. RICHARD BLUMENTHAL, U.S. SENATOR FROM CONNECTICUT

Senator BLUMENTHAL. I have made it back, Mr. Chairman. I have a reprieve on my presiding because I felt this committee hearing was so important. And thank you for——

The CHAIRMAN. So then I have the pleasure of putting you in front of Senator Markey and watching him fume.

[Laughter.]

The CHAIRMAN. Senator Blumenthal was here and is recognized.

Senator BLUMENTHAL. I was here before and——

The CHAIRMAN. Yes.

Senator BLUMENTHAL. Thank you, Mr. Chairman. Thank you. And thank you for your leadership in convening this hearing.

Thank you to the panel. You know, I feel that this afternoon is, in a certain way, a missed opportunity for all of us because we have been bouncing in and out due to the votes and our schedules and so forth. But this panel's contribution I think has been very, very useful and I think could be even more useful. And I am going to be submitting some additional questions for the record that perhaps you can address.

And speaking of missed opportunities, the report done by the majority staff of this committee I think performs an extraordinary

service and provides an excellent backdrop and summary and analysis of what happened here. And it uses the term "opportunities"—missed opportunities" is the way I would interpret them—that, very unfortunately, were failed here.

And it brings home to me one of the truths that I think maybe Senator Blunt was alluding to: The best technology in the world is useless unless there is good management.

And here, to be quite blunt, there were multiple warnings from the company's anti-intrusion software. They were missed by management, maybe because of lack of training, perhaps simply a sense of confidence or complacence. And the automated warnings, the specific kinds of signals that should have been an indication not only of intrusion but the need for action were missed. And that has created enormous costs.

So one of the lessons of this incident for me is that better management has to come with better technology. Do any of you disagree?

I take it by your silence you are agreeing.

The other area that has not been explored so far is the notification here. And the breach occurring on 11/12, November 12, happened well before there was notification to consumers, December 19 I think it was.

And the question that arises, I think, in the minds of a lot of consumers, and justifiably, is: Was there timely enough, quick enough, fast enough notification here? And what can be done to improve that pace in the future?

So let me ask Mr. Mulligan first and then perhaps the others about what you think about the timeliness of notification.

Mr. MULLIGAN. Senator, first, we identified the malware on our system on the morning of December 15. From that moment forward, we were very focused on public notification.

Senator BLUMENTHAL. But should you have discovered it earlier?

Mr. MULLIGAN. That is a reasonable question, Senator, and one—you know, the report, as you indicated, is very well done. It is asking a lot of hard questions, questions we are asking——

Senator BLUMENTHAL. And, in my view, let me just state very simply, there should have been earlier discovery. Whether you could have prevented the intrusion and stopped it earlier, that may be a subject of debate, but certainly it should have been discovered and notified earlier.

Mr. MULLIGAN. We are certainly going back to understand that, Senator.

As the alerts were surfaced, our team assessed them. They assess hundreds of alerts every day and make judgments based upon those. Given the circumstances we were in, we identified the malware on the morning of December 15 and provided public notice 4 days later.

We were very focused, your point is exactly right, on speed and doing so quickly. And we balanced that with ensuring that we could provide accurate information to our guests and respond to their questions, given the volume, that we knew were coming in both our call centers and our stores.

Senator BLUMENTHAL. Chairwoman Ramirez?

Ms. RAMIREZ. Thank you.

From our perspective, reasonably prompt notice is, of course, quite critical, but we also understand that it is very important for companies who have been victims of a breach incident to be able to assess exactly what transpired. And I think, as Mr. Mulligan has noted, it is critical that consumers receive accurate information, as well.

So we understand that that can take time. From our perspective, ultimately, notice should happen reasonably promptly. In our view, at the very outside, it should be about 60 days. Of course, it is critical that consumers have an opportunity to be able to take steps to protect themselves if their information has been exposed.

Senator BLUMENTHAL. I want to thank all of you for your answers. My time has expired, and I am going to yield to Senator Markey before he truly starts fuming, with good reason.

And I want to follow up on this question of notification. Because anybody can be a victim of hacking or intrusion, but no one should in any way delay notification to consumers once it has happened. And even when there is something less than complete certainty, a warning to consumers can save literally hundreds of millions, if not billions of dollars.

And the ultimate cost, often, is borne by those consumers in identity theft. So Senator McCaskill earlier was talking about, you know, who is bearing the cost in terms of the suffering and the pain resulting from identity theft? Consumers bear it, even if they get money, even if they are told by a monitoring—or even if they get insurance.

So I want to thank you all for your cooperation. I know that Target has cooperated with my office and with this committee, and I want to thank you for the contribution that you made here today and before now.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Blumenthal. And thank you; I don't know how you pulled it off, but you got a leave of absence. And I have been here 29 years, and you are the first person who has ever gotten that. So you clearly care, and so we are grateful for your coming back.

But now we are treated to the one and only, great Mr. Edward Markey.

[Laughter.]

STATEMENT OF HON. EDWARD MARKEY,
U.S. SENATOR FROM MASSACHUSETTS

Senator MARKEY. Thank you, Mr. Chairman.

Dr. Loh, the University of Maryland decided to provide 5 years of credit protection to those impacted by the data breach at your school. How did you determine that 5 years was an appropriate time period?

Mr. LOH. Well, as you know, we announced it within 24 hours, notified everybody within about 4 or 5 days. And very quickly, the way most students communicate is by social media——

Senator MARKEY. But why the 5-year period to offer protection?

Mr. LOH. And so, what they were complaining about was that we initially offered one year, and they said one year is not adequate.

Senator MARKEY. And what was your conclusion?

Mr. LOH. And my conclusion is I think they are right. It is going to cost more money, but it is the right thing to do. And then——

Senator MARKEY. And why is it the right thing to do?

Mr. LOH. I am sorry?

Senator MARKEY. Why is it the right thing to do?

Mr. LOH. Why is it the right thing to do? Because, after all, it did happen. It is our responsibility to provide the maximum protection possible of our sensitive data. We did not do it. I think we have very strong defenses, yet even so they were penetrated in a very sophisticated way. But that is no defense.

Senator MARKEY. OK. So——

Mr. LOH. And so we decided to up it from 1 year to 5 years.

Senator MARKEY. OK. Great.

So, Mr. Mulligan, Target has offered victimized consumers just one year of credit monitoring service. My concern is the same as Dr. Loh's and the students at the University of Maryland that 1 year is too brief a period a time, given the compromise of this information.

So why did you choose one year and not have a longer period of time, even though, as Dr. Loh said, it costs more money, but it is consistent with the risk that the consumer now runs?

Mr. MULLIGAN. We certainly evaluated this. Not having experience, we reached out to other entities that had had similar experiences. Our understanding at the time we made the offer was that one year was appropriate, would provide appropriate coverage.

We are certainly not dogmatic about that. We have not received the same feedback from our guests. We have issued millions of access codes to our coverage and have not received that feedback. But certainly if we did, we would reconsider that.

And I think, importantly, part of our coverage is that you have access to a fraud specialist ongoing beyond that one year. That goes on forever.

Senator MARKEY. Yes, I mean, my concern is, of course, this information has been compromised and it is sitting out there, and 1 year is just an arbitrary period of time to select to say that it can't be used in a way that comes back to haunt the individuals whose information has been compromised. And I just think that a more lengthy period of time makes more sense. I think the University of Maryland reached the correct decision.

I also understand the credit monitoring Target is offering tracks only one credit report, Experian, and not the credit files maintained by TransUnion and Equifax.

Why do you believe that one bureau monitoring is good enough? Wouldn't free monitoring all of three reports provide consumers with better protection following the breach?

Mr. MULLIGAN. Here again, we reached out to several other entities who had similar situations. We understood Experian is a well-established company. They had a product that we felt would work very well for our consumers, our guests, because it offered, in addition, identity theft protection, identity theft insurance, and, additionally, the ongoing access to the fraud specialist, which we thought was particularly important. So we went with their particular product.

Senator MARKEY. Yes. Again, I would suggest to you that you look perhaps to a broader group of companies here that would be helpful.

Credit monitoring may also provide consumers with a false sense of security because these services monitor only attempts to open new lines of credit; they do not watch for day-to-day unauthorized charges on your credit card.

So tell us what Target is doing to help consumers with that problem.

Mr. MULLIGAN. That is an excellent question. And as we have communicated to our guests, we have talked consistently about the need to monitor your existing accounts.

And, again, we understand that this has impacted them. We have tried to provide resources, tools, communication. We have provided one spot on our website which has all the information we have provided to them. We have provided e-mails and additional information to our REDcard holders, all with a focus to keep them informed about the information we have.

Senator MARKEY. Thank you.

And let me move to you, Mr. Wagner, if I could. What steps are you taking today to ensure that better ways of ensuring data security keep up with new payment technologies?

Mr. WAGNER. Well, as Visa has testified, the EMV technology is a major improvement for payment security, so that is something that Datacard is interested in supporting.

From an Entrust perspective, you know, our commitment is to help our customers have the identity technologies that they need to, you know, provide a strong layer of security in their defense mechanisms.

And one of the things that is really key to understand is that the malware has changed the way it operates in the last several years. And this idea of being someone on the network, being able to overtake a network administrator's credential and move freely inside the corporate network as if you have a ticket to Disneyland is a very different security risk than we were dealing with, you know, 4 and 5 years ago.

So trying to educate the industry, get governance processes in place that help companies understand their risk, and provide tools to mitigate those risks are what Entrust is trying to do.

Senator MARKEY. You know, and I guess what I would suggest is this, OK? That it doesn't make any sense for the Congress to mandate specific technologies. What it does make sense to do, however, is to say to industries that you have to keep up with the changes, and if you don't keep up with the changes, that you are liable. So to say that any of this is a surprise is just to say that you are not keeping up with what is going on.

And so the Chairman here could call a hearing of the five or six smartest young geeks in America, and they could explain it to this committee right now. But the truth is that the five or six smartest geeks in each one of your companies should be having that meeting right now with the CEOs, just saying, these are the changes and these are the recommendations that we make in order to provide the extra protection, because the law requires us to keep up. OK?

And so, to just keep saying we are surprised at the changes means that you haven't kept up. But it doesn't mean that younger people in your own organizations have kept up. And so, in and of itself, it is no excuse, OK? It just isn't.

And the Congress shouldn't require a specific technology, but it should require a standard. You know? If you don't have a radio on your boat in 1900, you are not derelict. You don't have one on your boat in 1920, now you have a problem. It evolved, you know? There are two-way radios now. If you don't have one, you can't say, "Oh, my God, I didn't have one when I bought the boat," huh? That is not an excuse, OK? You had to have noted that a guy named Marconi came along, you know, in the interim and that, you know, young people have these devices now and you might have learned that there was a storm coming, huh? And you just can't exempt yourself from the liability.

So that is kind of the challenge here. And that is why Senator Blumenthal and I have introduced legislation to give the Federal Trade Commission much greater authority, so that they can require these security measures to be put in place and that consumers receive immediate notification, as well, of any breach that occurs.

And I think it is important for us to act this year, because this has been occurring over and over and over. And T.J. Maxx is in my congressional district, my old congressional district, and they had a similar breach in 2007. So it is not as though this doesn't keep happening over and over again. It is that we keep treating it as though it is a huge surprise that it is going to happen.

And I just think we need to put in place the highest possible standards. That is why Senator Blumenthal and I introduced the legislation to help to accomplish that goal, and that is why Chairman Rockefeller is having these hearings, because we ultimately have to deal with the issue.

I thank you, Mr. Chairman.

The CHAIRMAN. That was very good questioning. I would like to be a part of the bill.

Senator MARKEY. Your staff was the first group of human beings on the planet to receive a copy of the bill.

The CHAIRMAN. Good.

But, see, you raise a very important point, and that is that we measure everything based upon what it was. And that absolves us of the responsibility of saying what it might become. And the only important question, whether you are talking about national security, anything, appropriate security, is what it might become. And that is why we are constantly surprised.

You know, the painful memory of the Boston Marathon, I am not sure what the teaching of that was. Because that was kind of a traditional act. Did we have something that we should have known, that there had been an advance in technology or in technique or in dispersion or whatever that we missed?

But regardless of what the answer to that is, you are basically right. NIST's job is not to say exactly what it should be for this month, the next month, the next month. It should be the highest possible, practicable—the highest possible—standard. And that will reach many people who will object.

Senator MARKEY. May I just say that it is a good example, where the Russians had given information about these suspects.

The CHAIRMAN. And that is correct.

Senator MARKEY. So the technology had worked, in fact, in gathering the information, but the human judgment then, in terms of what to do——

The CHAIRMAN. Yes.

Senator MARKEY.—with the information, you know?

So here, the technology is something that now is available to deal with the threats. And it is there and available, and younger people, of course, are familiar with it. But it just becomes, in most instances, do you want to spend the money?

The CHAIRMAN. Yes.

Senator MARKEY. Do you want to spend the money to keep up with this technological arms race that you necessarily have to because it is concomitant with the electronic era that each of these companies are embracing?

And so you can't think of that as a loss that you now have to suffer because you have to build in the security. You have to think of it as a necessary investment that you have to make.

The CHAIRMAN. Yes, and we are not accustomed to that——

Senator MARKEY. We are not.

The CHAIRMAN.—pattern of thought. But you are suggesting that we need to be.

Senator MARKEY. Exactly.

The CHAIRMAN. And that is what NIST is there for.

You missed my speech on spending money on infrastructure, and I will not pain you with repeating it. But you already agree with it.

[Laughter.]

The CHAIRMAN. Look——

Senator MARKEY. Does that mean we are passing a transportation bill out of this committee this year?

The CHAIRMAN. No. No, don't tease me with that.

[Laughter.]

The CHAIRMAN. This has been a very interesting and a very frustrating hearing for a couple of reasons. One is that it is a very complicated subject. I mean, we have the FTC, the President of the University of Maryland, this vast institution my former Chief of Staff, Kerry Ates, got her degree from, magna cum laude. And you all have great experience, and you bring great experiences to this.

But we are under the stricture of the sense that time is running out on us. And are we going to have the time to energize people? As Senator Markey has indicated, young people are already knowledgeable. The question is, will they be energized to go into these fields? Will they be energized to go work at the University of Maryland and help you? Or at your firm, Mr. Mulligan, to help you?

And I think it also makes the point that I made earlier, that at some point there is more reason there for it to have a point of responsibility. Ultimately, whether you are a senator or whether you are a President of a company or President of a university or playing first for the Boston Red Sox, it is not just holding on to your job, but it is how you do it, how people assess it with a hard eye, that makes the difference.

Accountability is everything. We have tended to forget that in this country because somehow America always muddles through. America is not now muddling through, and it is not a pretty sight.

You have been fantastic. You have been alert, you have been helpful. You have put up with our absences. We had nine votes. That is not a lot of fun for us, but we got nine judges, did we not? And that is a wonderful thing for America.

So I want to profoundly thank you, each one of you, for being here and for being here this long.

Mr. Beshar, I am feeling guilty about you. You haven't talked enough.

[Laughter.]

The CHAIRMAN. Would you like to talk for 2 or 3 minutes?

[Laughter.]

Mr. BESHAR. I will decline your very kind invitation.

The CHAIRMAN. Why? It is the perfect opportunity. Nobody is going to get up and leave while you are talking.

[Laughter.]

The CHAIRMAN. Say something that is on your heart that you want to say.

Mr. BESHAR. I will say very briefly, Senator, that I think the Government has really been out front of the bulk of industry and the nonprofit sector in identifying the significance of cybersecurity and in prodding business and the nonprofit sector to try to accelerate the pace of the commitment that they are showing.

And you have done it in this committee. The FBI, the DHS, the White House—there are various government agencies that have really advanced the ball. And I think it is incumbent upon the bulk of business and the nonprofit sector to try to follow the lead that has been set.

The CHAIRMAN. Yes. We have to get our act together, no question. And we are all part of it—part of the future, part of the wrongs of the present, part of the forgetfulness of the past, or taking too much comfort in the past.

I have nothing wise to say, so I will end this hearing. I don't tend to bang a gavel because I think that is kind of showmanship, so I just end it by saying it is at an end. So you are free.

[Laughter.]

The CHAIRMAN. But you have our great gratitude.

[Whereupon, at 5:17 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF THE ELECTRONIC TRANSACTIONS ASSOCIATION

Chairman Rockefeller, Ranking Member Thune and Members of the Committee, the Electronic Transactions Association (ETA) appreciates the opportunity to submit this statement for the record for the Committee's hearing, "Protecting Personal Consumer Information from Cyber Attacks and Data Breaches."

ETA is an international trade association representing companies that offer electronic transaction processing products and services. The purpose of ETA is to help the merchant acquiring industry by providing leadership through education, advocacy, and the exchange of information. ETA's membership spans the breadth of the payments industry, from financial institutions and transaction processors to independent sales organizations and equipment suppliers to merchants. More than 500 companies worldwide are members of ETA.

As the trade association for the payments industry, ETA recognizes the critical importance of data security. With more than 70 percent of consumer spending now done electronically, consumers depend on the security and reliability of payment systems. Consumers prefer electronic payments due to their convenience, efficiency, and low cost, but data theft and cybercrime, if not properly combatted, could cause some consumers to forgo these benefits out of concern about the security of their personal financial information. And if consumers do not have confidence in electronic commerce, then neither will the entrepreneurs and investors who spur financial innovation. Accordingly, the continued development of online commerce and other technology-based sources of economic growth rest on effective data security.

ETA is committed to ensuring that payment systems are fully secure and that customer information is protected. While recent high-profile data breaches remind us of the gravity of the threat posed by cybercriminals, existing data security systems have proven remarkably effective overall. Last year, U.S. payment systems processed more than $5 trillion in payments, and only a small fraction of those payments (less than one tenth of one percent) were fraudulent and consumers had no liability for such fraud. Nevertheless, data security will only be effective if it continues to stay ahead of the always evolving techniques and technologies of criminal enterprises.

Because ETA members are on the front lines of fighting data theft, our members have dedicated significant resources annually to developing secure payment systems. ETA's members have worked with their merchant customers to employ advanced technologies to prevent data theft and the fraudulent use of personal information. Due to these efforts, for example, fraud accounts for less than 6 cents of every $100 of credit and debit card transactions. Even in the relatively small number of cases where fraud does occur, consumers are usually not responsible for those amounts as financial institutions have adopted zero customer liability policies for fraudulent activity.

To further reduce the threat of fraud, ETA members that provide credit and debit cards are also beginning the phase-in of chip smart card technology beginning in 2015. This technology will replace magnetic stripe technology on credit and debit cards with cards containing embedded computer chips, which prevent criminals from producing counterfeit credit and debit cards. The adoption of EMV is a costly undertaking since it requires "point of sale" (POS) terminals to be updated to handle the new cards, but the investment is expected to yield a significant reduction in the incidents of card fraud and ensure the integrity of payment systems. Our industry is also working hard to deploy other technology solutions to fraud, like tokenization and end-to-end encryption, which hold real promise for thwarting criminal activity against merchants.

ETA recognizes that protecting the personal financial information of consumers is a responsibility shared among payments processors, retailers, and banks. Accordingly, we recently joined with 14 leading retail and financial services trade groups in a partnership aimed at ensuring that our shared infrastructure is secure. This partnership seeks to enhance information sharing to prevent cyber attacks, promote

new technologies to stay ahead of increasingly sophisticated threats, and collaborate on comprehensive solutions to threats growing to card-not-present transactions and the mobile environment. ETA believes that such industry collaboration offers the best means for the development of industry standards and innovative solutions to strengthen data security.

With respect to how government can best promote data security, ETA believes that the Federal government has an important role to play in creating a legal and regulatory environment conducive to technological innovation and the efficient and effective protection of consumer information. As Congress considers possible legislative measures to address data security, therefore, ETA would like to offer several recommendations.

1. *Congress should adopt national data breach standards.* ETA believes that a uniform national standard for data breach notification will help make sure consumers are notified when a security breach puts at risk their personally identifiable information, while minimizing the compliance risks to businesses. Today, payment processors must comply with an ever-changing array of 46 different state laws on data breach. These ambiguous laws unnecessarily increase the cost of data security and confuse consumers with inconsistent rights and responsibilities. A better approach is for a Federal standard that preempts state laws with a clear notification trigger and that provides a reasonable time for notifying consumers following a breach. In addition, Federal data breach legislation should avoid applying duplicative and inconsistent requirements by providing a safe harbor for entities subject to the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act, while not subjecting additional entities to these statutes.
2. *Congress should not legislate technology standards.* Since the advent of electronic payments, payments technologies have rapidly evolved to better protect consumer information and further improve the efficiency of electronic payments. While cybercrime has become increasingly complex, payments systems have continued to make the investments in new technology required to keep ahead of criminal efforts. Because future cybercrimes are impossible to predict, payments systems need to have the flexibility to quickly respond to new threats. Thus, Congress should avoid mandating any particular technology standards. Any standard Congress would adopt is likely to be quickly rendered obsolete by new criminal tactics and, therefore, could have the unintended consequence of restricting the ability of payment systems to protect customer information and the integrity of electronic commerce.
3. *A layered approach to data security is the best strategy.* There is no one solution that will prevent every attempt by criminals to steal data. Accordingly, in the same way that banks do not rely solely on vaults to thwart bank robberies, but also utilize in-house security guards, video cameras, and secure facilities, payments systems need to deploy a layered approach to data security. The utilization of multiple defenses—from chip and tokenization to firewalls and encryption—is the best strategy for minimizing data theft. Therefore, ETA recommends that Congress not mandate a particular method of data security.

We want to thank you for the opportunity to present this statement for the record on this important topic. If you have any questions about this statement or the issues discussed, please contact Jason Oxman, President of ETA.

DEPARTMENT OF JUSTICE

For Immediate Release—Monday, February 24, 2014

ATTORNEY GENERAL HOLDER URGES CONGRESS TO CREATE NATIONAL STANDARD FOR REPORTING CYBERATTACKS

WASHINGTON—In a video message released today, Attorney General Eric Holder called on Congress to create a strong, national standard for quickly alerting consumers whose information may be compromised by cyberattacks. This legislation would strengthen the Justice Department's ability to combat crime, ensure individual privacy, and prevent identity theft, while also helping to bring cybercriminals to justice.

The complete text of the Attorney General's weekly address is available below:

"Late last year, Target—the second-largest discount retailer in the United States—suffered a massive data breach that may have compromised the personal

information of as many as 70 million people, in addition to credit and debit card information of up to 40 million customers. The Department of Justice is currently investigating this breach, in close coordination with the U.S. Secret Service. And we are moving aggressively to respond to hacking, cyberattacks, and other crimes that harm American consumers—and expose personal or financial information to those who would take advantage of their fellow citizens.

"As we've seen—especially in recent years—these crimes are becoming all too common. And they have the potential to impact millions of Americans every year. Just days after the Target breach was made public, another major retailer—Neiman Marcus—reported that it also suffered a suspected cyberattack during the holiday season. And although Justice Department officials are working closely with the FBI and prosecutors across the country to bring cyber criminals to justice, it's time for leaders in Washington to provide the tools we need to do even more: by requiring businesses to notify American consumers and law enforcement in the wake of significant data breaches.

"Today, I'm calling on Congress to create a strong, national standard for quickly alerting consumers whose information may be compromised. This would empower the American people to protect themselves if they are at risk of identity theft. It would enable law enforcement to better investigate these crimes—and hold compromised entities accountable when they fail to keep sensitive information safe. And it would provide reasonable exemptions for harmless breaches, to avoid placing unnecessary burdens on businesses that do act responsibly.

"This legislation would strengthen the Justice Department's ability to combat crime and ensure individual privacy—while bringing cybercriminals to justice. My colleagues and I are eager to work with Members of Congress to refine and pass this important proposal. And we will never stop working to protect the American people—using every tool and resource we can bring to bear."

The full video is available at *http://www.justice.gov/agwa.php*

PREPARED STATEMENT OF THE AMERICAN BANKERS ASSOCIATION

Chairman Rockefeller, Ranking Member Thune, and members of the Committee, ABA appreciates the opportunity to submit for the record comments regarding the recent Target and other data security breaches. The ABA represents banks of all sizes and charters and is the voice for the Nation's $14 trillion banking industry and its two million employees.

The subject of today's hearing, "*Protecting Personal Consumer Information from Cyber Attacks and Data Breaches,*" is an important one. Notwithstanding these recent breaches, our payment system remains strong and functional. No security breach seems to stop the $3 trillion that Americans spend safely and securely each year with their credit and debit cards. And with good reason: Customers can use these cards confidently because their banks protect them from losses by investing in technology to detect and prevent fraud, reissuing cards and absorbing fraud costs.

At the same time, these breaches have reignited the long-running debate over consumer data security policy. ABA and the thousands of community, mid-size, regional, and large banks we represent recognize the paramount importance of a safe and secure payments system to our Nation and its citizens. We thank the Committee for holding this hearing and welcome the ongoing discussion. From ABA's perspective, Congress should examine the specific circumstances of the Target breach and the broader data security issues involved, and we stand ready as a resource to assist in your efforts.

In our statement for the record we will focus on four main points:

- *Protecting consumers is the banking industry's first priority.* As the stewards of the direct customer relationship, the banking industry's overarching priority in breaches like that of Target's is to protect consumers and make them whole from any loss due to fraud. Despite what others maintain, it is the banking industry that reimburses consumers for any losses, only later seeking reimbursement from the preached party.
- *A National data breach standard is essential.* Consumers' electronic payments are not confined by borders between states. As such, a national standard for data security and breach notification is of paramount importance.
- *All players in the payments systems, including retailers, must significantly improve their internal security systems as the criminal threat continues to evolve.*
- *Protecting the Payments System is a Shared Responsibility.* Banks, retailers, processors, and all of the participants in the payments system must share the responsibility of keeping the system secure, reliable, and functioning in order

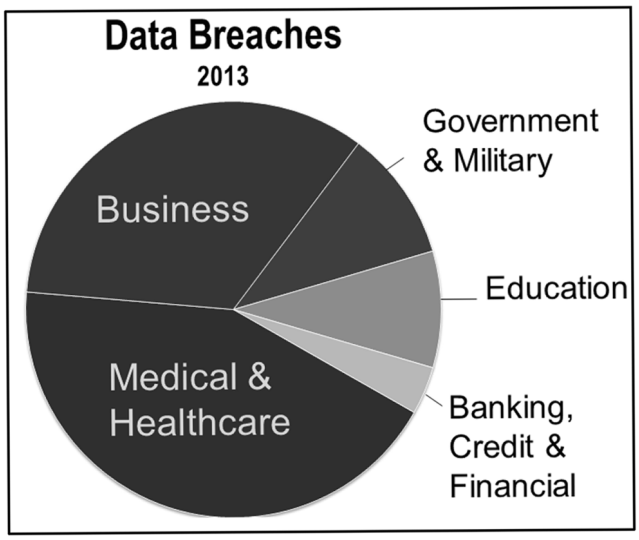
to preserve consumer trust. That responsibility should not fall predominantly on the financial services sector.

Before addressing each of these points in detail, it is important to understand the data security vulnerabilities in our system. The numbers are telling and point to the need for shared responsibility to fight off the continual attacks on data.

I. Data Security: Where are the Vulnerabilities?

It is a sobering fact that, since January 2005, a total of over 4,200 breaches exposing almost 600 million records have occurred nationwide. (Source: Identity Theft Resource Center) There were over 600 reported data breaches during 2013 alone, an increase of 30 percent over 2012 and the third highest number of breaches over the last nine years. The two sectors reporting the highest number of breaches were the healthcare sector at 43 percent of reported breaches and the business sector, including merchants, which accounted for nearly 34 percent of reported breaches.

Moreover, the business sector, because of the Target breach, accounted for almost 82 percent of 2013's breached records. The Banking, Credit and Financial sector accounted for only 4 percent of all breaches and less than 2 percent of all breached records.[1] However, in spite of the small percentage of actual data breaches, the Banking, Credit and Financial sector bears a disproportionate share of breach recovery and fraud expenses. This is a consistent trend since 2005, where over this nine year period our sector accounted for approximately 8 percent of all reported breaches. The business sector accounted for approximately 36 percent and health care sector approximately 23 percent of all breaches over the same time period.



Source: Identity Theft Resource Center

These numbers point to the central challenge associated with breaches of financial account data or personally identifiable information: while the preponderance of data breaches occur at entities far removed from the banking sector, it is the bank's customer potentially at the end of the line who must be protected.

II. Protecting Consumers is Our First Priority

While the facts of the Target breach remain fluid, the company has acknowledged that the breach occurred within its internal systems, affecting nearly 40 million credit and debit card accounts while also revealing the personally identifiable information (*e.g.,* name, address, e-mail, telephone number) of potentially 70 million people. *On average, the Target breach has affected 10 percent of every bank's credit and debit card customer base.*

[1] *2013 Data Breach Category Summary,* Identity Theft Resource Center, January 1, 2014, Available at: *http://www.idtheftcenter.org/images/breach/2013/BreachStatsReportSummary 2013.pdf*

Paying for Fraud

When a retailer like Target speaks of its customers having "zero liability" from fraudulent transactions, it is because our Nation's banks are making customers whole, not the retailer that suffered the breach. Banks are required to swiftly research and reimburse customers for unauthorized transactions, and normally exceed legal requirements by making customers whole within days of the customer alerting the bank of the fraud, if not immediately.[2]

After the bank has reimbursed a customer for the fraudulent transaction, it can then attempt to "charge-back" the retailer where the transaction occurred. Unfortunately, the majority of these attempts are unsuccessful, with the bank ultimately shouldering the vast majority of fraud loss and other costs associated with the breach. Overall, for 2009, 62 percent of reported debit card fraud losses were borne by banks, while 38 percent were borne by merchants.[3]

It is an unfortunate truth that, in the end (and often well after the breach has occurred and the banks have made customers whole) banks generally receive *pennies for each dollar* of fraud losses and other costs that were incurred by banks in protecting their customers. This minuscule level of reimbursement, when taken in concert with the fact that banks bear over 60 percent of reported fraud losses yet have accounted for less than 8 percent of reported breaches since 2005 is clearly inequitable. We believe banks should be fully reimbursed for the costs they bear for breaches that occur elsewhere.

Reissuing and Ongoing Monitoring

Each bank makes its own decision as to when and whether to reissue cards, which on average costs banks about $5 per card, but could be more. In the case of the Target breach, the decision of whether to reissue cards was made even more difficult considering the inconvenience this can cause during the holiday season: breach or no breach, many consumers would not have wanted their cards shut down leading up to Christmas. Those cards that have not been reissued are being closely monitored for fraudulent transactions. In some instances, banks gave customers an option of keeping their cards open through the holidays until they could reissue all cards in January or, if they were concerned, to shut their card down and be reissued a new card immediately.

The Target compromise was also unique in terms of the high awareness of the "Target" name, the sheer number of people affected, and the media coverage of the event. In addition to proactively communicating with customers about the breach, bank call centers and branches have handled millions of calls and in-person inquiries regarding the card compromise. Many smaller and community banks have increased staffing to meet consumer demand. At the end of the day, consumers expect answers and to be protected by their bank, which is why they call us, not Target or whoever actually suffered the breach.

We also remain vigilant to the potential for fraud to occur in the future as a result of the Target breach. Standard fraud mitigation methods banks use on an ongoing basis include monitoring transactions, reissuing cards, and blocking certain merchant or types of transactions, for instance, based on the location of the merchant or a transaction unusual for the customer. Most of us are familiar with that call from a card issuer rightfully questioning a transaction and having a card cancelled as a result. In many cases, however, the lifespan of compromised consumer data extends well beyond the weeks immediately following the breach itself. Just because the headlines fade away does not mean that banks can afford to relax their ongoing fraud protection and screening efforts. In addition there are ongoing customer support issues as customer's setup new card numbers for recurring transactions related to health club memberships and online stores such as iTunes.

III. A National Data Breach Standard is Essential

In many instances, the identity of the entity that suffered the breach is either not known or, oftentimes, intentionally not revealed as there is no requirement to do

---

[2] With traditional card payments, the rights and obligations of all parties are well-defined by Federal statute when an unauthorized transaction occurs. For example, Regulation E describes consumers' rights and card issuers' obligations when a debit card is used, while Regulation Z does so for credit card transactions. The payment networks also have well-established rules for merchants and issuers. For instance, while Regulation Z limits a customer's liability for unauthorized transactions on a lost or stolen credit card to $50, the card networks require issuers to provide their cardholders with zero liability.

[3] *2009 Interchange Revenue, Covered Issuer Cost, and Covered Issuer and Merchant Fraud Loss Related to Debit Card Transactions,* June 2011, Board of the Governors of the Federal Reserve System,, available at: *http://www.federalreserve.gov/paymentsystems/files/debitfees_costs.pdf*

so. Often, a retailer or other entity would rather pass the burden on to the affected consumers' banks rather than taking the reputational hit themselves. In such cases, the bank is put in the position of notifying their customers that their credit or debit card data is at risk without being able to divulge where the breach occurred. Many banks have expressed great frustration regarding this process, with their customers—absent better information—blaming the bank for the breach itself and inconvenience they are now suffering.

Like the well-defined Federal regulations surrounding consumer protections for unauthorized credit or debit transactions, data breach notification for state and nationally-chartered banks is governed by the Gramm-Leach-Bliley Act and guidance from the from the Federal Financial Institutions Examination Council (FFIEC), requiring every bank to have a customer response program. Retail establishments have no comparable Federal requirements. In addition, not only are retailers, healthcare organizations, and others who suffer the majority of breaches not subject to Federal regulatory requirements in this space, no entity oversees them in any substantive way. Instead they are held to a wide variety of state data breach laws that aren't always consistent. Banks too must also abide by many of these state laws, creating a patchwork of breach notification and customer response standards that are confusing to consumers as well as to companies.

Currently, 46 states, three U.S. territories, and the District of Columbia have enacted laws governing data security in some fashion, such as standards for data breach notification and for the safeguarding of consumer information. Although some of these laws are similar, many have inconsistent and conflicting standards, forcing businesses to comply with multiple regulations and leaving many consumers without proper recourse and protections.

Establishing a national data security and notification law that brings others up to bank standards, requiring any business that maintains sensitive personal and financial information to implement, maintain, and enforce reasonable policies and procedures to protect the confidentiality and security of sensitive information from unauthorized use, would provide better protection for consumers nationwide.

Our existing national payments system serves hundreds of millions of consumers, retailers, banks, and the economy well. It only stands to reason that such a system functions most effectively when it is governed by a consistent national data breach policy.

IV. All Players in the Payments System Must Improve Their Internal Systems as the Criminal Threat Continues to Evolve

While some details of the Target breach are still unknown, what is clear is that criminal elements responsible for such attacks are growing increasingly sophisticated in their efforts to breach the payments system. This disturbing evolution, as demonstrated by the Target breach, will require enhanced attention, resources, and diligence on the part of all payments system participants.

The increased sophistication and prevalence of breaches caused by criminal attacks—as opposed to negligence or unintentional system breaches is also borne out in a recent study by the Ponemon Institute. Evaluating annual breach trends, the Institute found that 2012 was the first year in which malicious or criminal attacks were the most frequently encountered root cause of data breaches by organizations in the study, at 41 percent.[4]

Emerging details of the Target breach are allowing us to see a troubling picture of the direction the criminal evolution is taking, and what it means for at-risk consumer data. For example:

- While Target's last public statement on the issue stated that the PINs that were compromised as part of the breach were encrypted, the company originally stated that PINs were not compromised at all. If the PINs were unencrypted, this would be particularly troubling, as that would make bank customer accounts vulnerable to ATM cash withdrawals as well as unauthorized purchases. We call on law enforcement and those in the forensics process to be as transparent as possible in outlining what are the precise threats to our customers.
- Even if the PINs that were breached were in fact encrypted, there is still the potential that they could be decrypted, placing our customers at just as much risk as if unencrypted PINs had been captured.

---

[4] *2013 Cost of Data Breach Study: United States,* May 2013, Ponemon Institute, available 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__markewire__linkedin__2013Jun__worldwide__CostofaDataBreach*

- Banks also do not know the extent to which their customers' bank account numbers, which are linked to Target's RedCard, were compromised as a result of the breach. If this information was compromised, customers could be vulnerable to unauthorized Automated Clearing House (ACH) transactions directly from their accounts.
- More generally, banks have also encountered significant customer confusion as to the nature of Target's RedCard and the bank's ability to help. Many believe the bank can cancel the card and reissue it even though the card was issued by Target. This confusion points to a broader problem with the emergence of many non-traditional payments providers: customers have a hard time understanding which payment entity is responsible for what, and often just assume the bank is the responsible party.

These threats to bank customer accounts point to the security vulnerabilities associated with non-traditional payments companies, such as Target, having direct linkages to the payments system without information security regulatory requirements comparable to that of financial institutions.

V. Protecting the Payments System is a Shared Responsibility

While much has recently been made about the on-going disagreements between the retail community and the banking industry over who is responsible for protecting the payments system, in reality our Nation's payments system is made up of a wide variety of players: banks, card networks, retailers, processors, and even new entrants, such as Square, Google, and PayPal. Protecting this system is a shared responsibility of all parties involved and we need to work together and invest the necessary resources to combat increasingly sophisticated threats to breach the payments system.

We must work together to combat the ever-present threat of criminal activity at our collective doorstops. Inter-industry squabbles, like those over interchange, have had a substantial impact on bank resources available to combat fraud. Policymakers must examine that impact closely to ensure that the necessary resources are not diverted from addressing the real concern at hand—the security of our Nation's payment system and the need to protect consumers. *All* participants must invest the necessary resources to combat this threat.

In the wake of this breach, there has been significant discussion over how to enhance payment card security, focusing on the implementation of chip-based security technology known as EMV.[5] This technology makes it much harder for criminals to create duplicate cards or make sense of encrypted data that they steal.

We encourage the implementation of chip technology, both on the card and at the point-of-sale. In fact, the rollout of this technology in the U.S. is well underway, with the next set of deadlines for banks and retailers coming in late 2015. It takes time for full implementation of chip technology in the U.S., as our country supports the largest economy in the world, with over 300 million customers, 8 million retailers, and 14,000 financial institutions.

Even though EMV is an important step in the right direction, there is no panacea for the ever-changing threats that exist today. For instance, EMV technology would not have prevented the potential harm of the Target breach to the 70 million customers that had their name, address, e-mail, and/or telephone number compromised. Moreover, EMV technology will help to address potential fraud at the point-of-sale, but it does not address on-line security, nor is it a perfect solution even at the point-of-sale as criminal efforts evolve. Because it is impossible to anticipate what new challenges will come years from now, we must therefore be cautious not to embrace any "one" solution as the answer to all concerns.

VI. The Path Forward

Any system is only as strong as its weakest link. The same certainly holds true in our rapidly-changing consumer payments marketplace. The innovations that are driving the industry forward and presenting consumers with exciting new methods of making purchases is also rapidly expanding beyond the bounds of our existing regulatory and consumer protection regimes. And, as has historically been the case, the criminals are often one step ahead as the marketplace searches for consensus. That said, there are several positive steps policymakers can take to facilitate a higher level of security for consumers going forward. For example:

[5] EMV stands for Europay, Mastercard, and Visa, the developers of a global standard for interoperation of integrated circuit, or "chip" cards and chip card compatible point-of-sale terminals and automated teller machines.

Raise all participants in the payments system to comparable levels of security. Security within the payments system is currently uneven. In addition to adhering to the Payment Card Industry Data Security Standards, banks and other financial institutions are also subject to significantly higher information security requirements than others that facilitate electronic payments and house bank customer payment data.[6] More must be done to buttress and enforce the current regulatory requirements that merchants face.

Establish a national data security breach and notification standard. A national data breach standard, replacing the current patchwork of state laws and establishing one set of national requirements, would provide better and more consistent protection for consumers nationwide.

Make those responsible for data breaches responsible for their costs. Banks bear the majority of costs associated with the fraud caused by breaches even though our industry is responsible for only a small percentage of the breaches that have occurred since 2005. When any entity—be it a bank, merchant, college or hospital—is responsible for a breach that compromises customer payment data or personally identifiable information, that entity should be responsible for the range of costs associated with that breach to the extent it was not adhering to the necessary security requirements.

Increase the speed and transparency with which the results of forensic investigations are shared with the financial community. When a breach occurs, there is much banks and others do not know and are not told for extended periods of time regarding the vulnerability of certain aspects of their customers' data. Similar to the robust manner in which banks and law enforcement currently share other cybersecurity threat data, we must examine ways to share the topline threat data from merchant and other breaches that does not impede the overall investigation. For example, banks and payment networks currently share an increasing amount of cybersecurity threat and fraud information through groups such as the Financial Services Information Sharing and Analysis Center and other groups within ABA. Our efforts would be greatly enhanced if that information sharing capacity expanded to include the merchant community. We would welcome such expansion and look forward to working collectively with merchants to combat our common adversaries.

Banks are committed to doing our share, but cannot be the sole bearer of that responsibility. Policymakers, card networks, and all industry participants have a vital role to play in addressing the regulatory gaps that exist in our payments system, and we stand ready to assist in that effort. Thank you for giving ABA the opportunity to provide this statement. We look forward to continuing to work with Congress to enhance the security of our Nation's payment system, and maintain the trust and confidence hundreds of millions of Americans place in it every day.

PREPARED STATEMENT OF THE NATIONAL RETAIL FEDERATION

Chairman Rockefeller, Ranking Member Thune, members of the Committee, on behalf of the National Retail Federation (NRF) we want to thank you for giving us this opportunity to provide you with these comments on data security and protecting American's financial information. NRF is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the Nation's largest private sector employer, supporting one in four U.S. jobs—42 million working Americans. Contributing $2.5 trillion to annual GDP, retail is a daily barometer for the Nation's economy.

Collectively, retailers spend billions of dollars safeguarding consumers' data and fighting fraud. Data security is something that our members strive to improve every day. Virtually all of the data breaches we've seen in the United States during the past couple of months—from those at retailers that have been prominent in the news to those at banks and card network companies that have received less attention—have been perpetrated by criminals that are breaking the law. All of these companies are victims of these crimes and we should keep that in mind as we explore this topic and public policy initiatives relating to it.

This issue is one that we urge the Committee to examine in a holistic fashion: we need to reduce fraud. That is, we should not be satisfied with deciding what to

[6] For instance, banks are subject to the information security requirements contained within the Gramm-Leach-Bliley Act, the FFIEC Red Flag Rules regarding identity theft, and are continually examined against these requirements.

do after a data breach occurs—who to notify and how to assign liability. Instead, it's important to look at why such breaches occur and what the perpetrators get out of them so that we can find ways to reduce and prevent not only the breaches themselves, but the fraudulent activity that is often the goal of these events. If breaches become less profitable to criminals then they will dedicate fewer resources to committing them and our goals will become more achievable.

With that in mind, these comments are designed to provide some background on data breaches and on fraud, explain how these events interact with our payments system, discuss some of the technological advancements that could improve the current situation, raise some ways to achieve those improvements, and then discuss the aftermath of data breaches and some ways to approach things when problems do occur.

Data Breaches in the United States

Unfortunately, data breaches are a fact of life in the United States. In its 2013 data breach investigations report, Verizon analyzed more than 47,000 security incidents and 621 confirmed data breaches that took place during the prior year. Virtually every part of the economy was hit in some way: 37 percent of breaches happened at financial institutions; 24 percent happened at retail; 20 percent happened at manufacturing, transportation and utility companies; and 20 percent happened at information and professional services firms.

It may be surprising to some given recent media coverage that more data breaches occur at financial institutions than at retailers. And, it should be noted, even these figures obscure the fact that there are far more merchants that are potential targets of criminals in this area. There are hundreds of times as many merchants accepting card payments in the United States than there are financial institutions issuing and processing those payments. So, proportionally, and not surprisingly, the thieves focus far more often on banks which have our most sensitive financial information—including not just card account numbers but bank account numbers, social security numbers and other identifying data that can be used to steal identities beyond completing some fraudulent transactions.

Source: 2013 Data Breach Investigations Report, Verizon

Nearly one-fifth of all of these breaches were perpetrated by state-affiliated actors connected to China. Three in four breaches were driven by financial motives. Two-thirds of the breaches took months or more to discover and 69 percent of all breaches were discovered by someone outside the affected organization.[1]

These figures are sobering. There are far too many breaches. And, breaches are often difficult to detect and carried out in many cases by criminals with real resources behind them. Financially focused crime seems to most often come from organized groups in Eastern Europe rather than state-affiliated actors in China, but the resources are there in both cases. The pressure on our financial system due to the overriding goal of many criminals intent on financial fraud is acute. We need to recognize that this is a continuous battle against determined fraudsters and be guided by that reality.

[1] 2013 Data Breach Investigations Report, Verizon.

Background on Fraud

Fraud numbers raise similar concerns. Just a year ago, Forbes found that Mexico and the United States were at the top of the charts worldwide in credit and debit card fraud.[2] And fraud losses in the United States have been going up in recent years while some other countries have had success reducing their fraud rates. The United States in 2012 accounted for nearly 30 percent of credit and debit card charges but 47 percent of all fraud losses.[3] Credit and debit card fraud losses totaled $11.27 billion in 2012.[4] And retailers spend $6.47 billion trying to prevent card fraud each year.[5]

Fraud is particularly devastating for retailers in the United States. LexisNexis and Javelin Strategy & Research have published an annual report on the "True Cost of Fraud" each year for the last several years. The 2009 report found, for example, that retailers suffer fraud losses that are 10 times higher than financial institutions and 20 times the cost incurred by consumers. This study covered more than just card fraud and looked at fraudulent refunds/returns, bounced checks, and stolen merchandise as well. Of the total, however, more than half of what merchants lost came from unauthorized transactions and card chargebacks.[6] The founder and President of Javelin Strategy, James Van Dyke, said at the time, "We weren't completely surprised that merchants are paying more than half of the share of the cost of unauthorized transactions as compared to financial institutions. But we were very surprised that it was 90–10."[7] Similarly, Consumer Reports wrote in June 2011, "The Mercator report estimates U.S. card issuers' total losses from credit-and debit-card fraud at $2.4 billion. That figure does not include losses that are borne by merchants, which probably run into tens of billions of dollars a year."[8]

Online fraud is a significant problem. It has jumped 36 percent from 2012 to 2013.[9] In fact, estimates are that online and other fraud in which there is no physical card present accounts for 90 percent of all card fraud in the United States.[10] And, not surprisingly, fraud correlates closely with data breaches among consumers. More than 22 percent of breach victims suffered fraud while less than 3 percent of consumers who didn't have their data breached experienced fraud.[11]

---

[2] "Countries with the most card fraud: U.S. and Mexico," *Forbes* by Halah Touryalai, Oct. 22, 2012.

[3] "U.S. credit cards, chipless and magnetized, lure global fraudsters," by Howard Schneider, Hayley Tsukayama and Amrita Jayakumar, *Washington Post,* January 21, 2014.

[4] "Credit Card and Debit Card Fraud Statistics," CardHub 2013, available at *http://www.cardhub.com/edu/credit-debit-card-fraud-statistics/*.

[5] *Id.*

[6] A fraud chargeback is when the card-issuing bank and card network take the money for a transaction away from the retailer so that the retailer pays for the fraud.

[7] "Retailers are bearing the brunt: New report suggests what they can do to fight back," by M.V. Greene, NRF Stores, Jan. 2010.

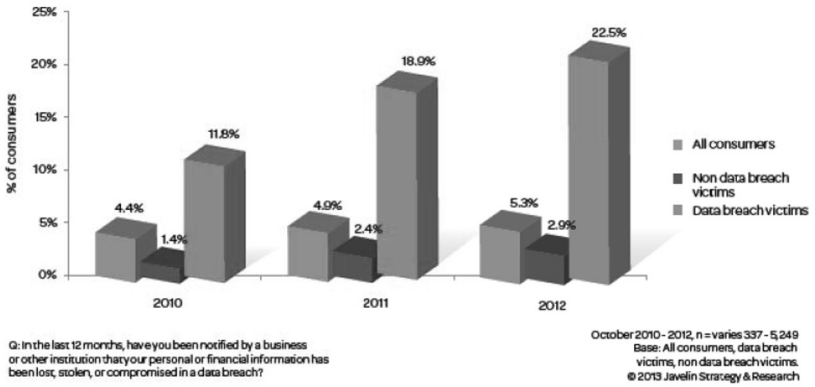
[8] "House of Cards: Why your accounts are vulnerable to thieves," *Consumer Reports,* June 2011.

[9] 2013 True Cost of Fraud, LexisNexis at 6.

[10] "What you should know about the Target case," by Penny Crosman, *American Banker,* Jan. 23, 2014.

[11] 2013 True Cost of Fraud, LexisNexis at 20.

Figure 11. Fraud Incidence Rate Among All Consumers, Data Breach Victims, And Non Data Breach Victims (2010 -2012)



Source: 2013 True Cost of Fraud, LexisNexis

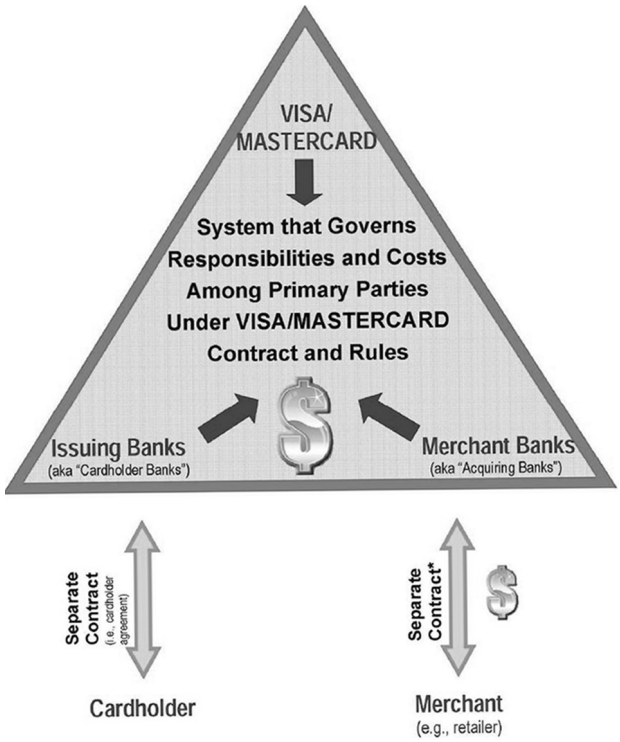
These numbers provide insights as to how to get to the right solutions of better safeguarding consumer and cardholder data and the need to improve authentication of transactions to protect against fraud. But before delving into those areas, some background on our payments system could be helpful.

The Payments System

Payments data is sought in breaches more often than any other type of data.[12] Now, every party in the payment system, financial institutions, networks, processors, retailers and consumers, has a role to play in reducing fraud. However, although all parties have a responsibility, some of those parties are integral to the system's design and promulgation while others, such as retailers and consumers, must work with the system as it is delivered to them.

As the following chart shows, while the banks are intimately connected to Visa and MasterCard, merchants and consumers have virtually no role in designing the payment system. Rather, they are bound to it by separate agreements issued by financial intermediaries.

[12] 2013 Data Breach Investigations Report, Verizon at 445, figure 35.



Typically contract between merchant bank and its retailers requires retailers to reimburse merchant bank for any costs, penalties, or fees imposed by the system on the merchant bank (including chargebacks—*i.e.,* disputed charges—and costs of data breaches)

Thus consumers are obligated to keep their cards safe and secure in their wallets and avoid misuse, but must necessarily turn their card data over to others in order to effectuate a transaction. Retailers are likewise obligated to collect and protect the card data they receive, but are obligated to deliver it to processors in order to complete a transaction, resolve a dispute or process a refund. In contrast, those inside the triangle have much more systemic control.

For example, retailers are essentially at the mercy of the dominant credit card companies when it comes to protecting payment card data. The credit card networks—Visa, MasterCard, American Express, Discover and JCB—are responsible for an organization known as the PCI (which stands for Payment Card Industry) data security council. PCI establishes data security standards (PCI–DSS) for payment cards. While well intentioned in concept, these standards have not worked quite as well in practice. They have been inconsistently applied, and their avowed purpose has been significantly altered.

PCI has in critical respects over time pushed card security costs onto merchants even when other decisions might have more effectively reduced fraud—or done so at lower cost. For example, retailers have long been required by PCI to encrypt the payment card information that they have. While that is appropriate, PCI has not required financial institutions to be able to accept that data in encrypted form. That means the data often has to be de-encrypted at some point in the process in order for transactions to be processed.

Similarly, merchants are expected to annually demonstrate PCI compliance to the card networks, often at considerable expense, in order to benefit from a promise that the merchants would be relieved of certain fraud inherent in the payment system, which PCI is supposed to prevent. However, certification by the networks as PCI Compliant apparently has not been able to adequately contain the growing fraud and retailers report that the "promise" increasingly has been abrogated or ignored. Unfortunately, as card security expert Avivah Litan of Gartner Research wrote re-

cently, "The PCI (Payment Card Industry) security standard has largely been a failure when you consider its initial purpose and history." [13]

PCI has not addressed many obvious deficiencies in cards themselves. There has been much attention to the fact that the United States is one of the last places on earth to put card information onto magnetic stripes on the backs of cards that can easily be read and can easily be counterfeited (in part because that data is static and unchanging). We need to move past magstripe technology.

But, before we even get to that question, we need to recognize that sensitive card data is right on the front of the card, embossed with prominent characters. Simply seeing the front of a card is enough for some fraudsters and there have been fraud schemes devised to trick consumers into merely showing someone their cards. While having the embossed card number on the front of the card might have made sense in the days of knuckle-buster machines and carbon copies, those days are long passed.

In fact, cards include the cardholder's name, card number, expiration date, signature and card verification value (CVV) code. Everything a fraudster needs is right there on the card. The bottom line is that cards are poorly designed and fraud-prone products that the system has allowed to continue to proliferate.

PCI has also failed to require that the identity of the cardholder is actually verified or authenticated at the time of the transaction. Signatures don't do this. Not only is it easy to fake a signature, but merchants are not allowed by the major card networks to reject a transaction based on a deficient signature. So, the card networks clearly know a signature is a useless gesture which proves nothing more than that someone was there purporting to be the cardholder.

The use of personal identification numbers (PINs) has actually proven to be an effective way to authenticate the identity of the cardholder. PIN numbers are personal to each cardholder and do not appear on the cards themselves. While they are certainly not perfect, their use is effective at reducing fraud. On debit transactions, for example, PIN transactions have one-sixth the amount of fraud losses that signature transactions have.[14] But PINs are not required on credit card transactions. Why? From a fraud prevention perspective, there is no good answer except that the card networks which set the issuance standards have failed to protect people in a very basic way.

As noted by LexisNexis, merchant fraud costs are much higher than banks' fraud costs. When credit or debit card fraud occurs, Visa and MasterCard have pages of rules providing ways that banks may be able to charge back the transaction to the retailer (which is commonly referred to as a "chargeback"). That is, the bank will not pay the retailer the money for the fraudulent transaction even though the retailer provided the consumer with the goods in question. When this happens, and it happens a lot, the merchant loses the goods *and* the money on the sale. According to the Federal Reserve, this occurs more than 40 percent of the time when there is fraud on a signature debit transaction,[15] and our members tell us that the percentage is even higher on credit transactions. In fact, for online transactions, which as noted account for 90 percent of fraud, merchants pay for the vast majority of fraudulent transactions.[16]

Retailers have spent billions of dollars on card security measures and upgrades to comply with PCI card security requirements, but it hasn't made them immune to data breaches and fraud. The card networks have made those decisions for merchants and the increases in fraud demonstrate that their decisions have not been as effective as they should have been.

Improved Technology Solutions

There are technologies available that could reduce fraud. An overhaul of the fraud-prone cards that are currently used in the U.S. market is long overdue. As I noted, requiring the use of a PIN is one way to reduce fraud. Doing so takes a vulnerable piece of data (the card number) and makes it so that it cannot be used on its own. This ought to happen not only in the brick-and-mortar environment in which a physical card is used but also in the online environment in which the physical card does not have to be used. Canada, for example, is exploring the use of a PIN for online purchases. The same should be true here. Doing so would help di-

---

[13] "How PCI Failed Target and U.S. Consumers," by Avivah Litan, Gartner Blog Network, Jan. 20, 2014, available at *http://blogs.gartner.com/avivah-litan/2014/01/20/how-pci-failed-target-and-u-s-consumers/*.

[14] *See* 77 Fed. Reg. 46261 (Aug. 3, 2012) reporting $1.11 billion in signature debit fraud losses and $181 million in PIN debit fraud losses.

[15] *Id.* at 46262.

[16] Merchants assume 74 percent of fraud losses for online and other card-not-present signature debit transactions. 77 Fed. Reg. 46262.

rectly with the 90 percent of U.S. fraud which occurs online. It is not happenstance that automated teller machines (ATMs) require the entry of a PIN before dispensing cash. Using the same payment cards for purchases should be just as secure as using them at ATMs.

Protecting all cards with a PIN instead of a signature is the single most important fraud protection step that could be taken quickly. It's proven, it's effective, and it's relatively easily implementable. PIN debit cards are close to ubiquitous worldwide, and readily producible in the U.S. Chip is desirable add-on. If speed of implementation is of importance, then substituting PIN for signature is preferable to implementing Chip. More than twice as many U.S. terminals are ready to accept PIN cards today, than are chip ready. Despite this, one major card brand continues to denigrate PINs in favor of signature, in part because they can collect more fees with fraud-prone signature transactions.[17]

Cards should also be smarter and use dynamic data rather than magnetic stripes. In much of the world this is done using computer chips that are integrated into physical credit and debit cards. It is important to note, however, that there are many types of technologies that may be employed to make this upgrade. EMV, which is an acronym for Europay, MasterCard and Visa, is merely one particular proprietary technology. As the name indicates, EMV was established by Europay, MasterCard and Visa. A proprietary standard could be a detriment to the other potentially competitive networks.[18] Adopting a closed system, such as EMV, means we are locking out the synergistic benefits of competition.

But even within that closed framework, it should also be noted that everywhere in the world that EMV has been deployed to date the card networks have required that the cards be used with a PIN. That makes sense. But here, the dominant card networks are proposing to force chips (or even EMV) on the U.S. market without requiring PIN authentication. Doing that makes no sense and loses a significant part of the fraud prevention benefits of chip technology. To do otherwise would mean that merchants would spend billions to install new card readers without they or their customers obtaining PINs' fraud-reducing benefits. We would essentially be spending billions to combine a 1990s technology (chips) with a 1960s relic (signature) in the face of 21st century threats.

Another technological solution that could help deter and prevent data breaches and fraud is encryption. Merchants are already required by PCI standards to encrypt cardholder data but, as noted earlier, not everyone in the payments chain is required to be able to accept data in encrypted form. That means that data may need to be de-encrypted at some points in the process. Experts have called for a change to require "end-to-end" (or point-to-point) encryption which is simply a way to describe requiring everyone in the payment-handling chain to accept, hold and transmit the data in encrypted form.

According to the September 2009 issue of the Nilson Report "most recent cyberattacks have involved intercepting data in transit from the point of sale to the merchant or acquirer's host, or from that host to the payments network." The reason this often occurs is that "data must be decrypted before being forwarded to a processor or acquirer because Visa, MasterCard, American Express, and Discover networks can't accept encrypted data at this time." [19]

Keeping sensitive data encrypted throughout the payments chain would go a long way to convincing fraudsters that the data is not worth stealing in the first place—at least, not unless they were prepared to go through the arduous task of trying to de-encrypt the data which would be necessary in order to make use of it. Likewise, using PIN-authentication of cardholders now would offer some additional protection against fraud should this decrypted payment data be intercepted by a criminal during its transmission "in the clear."

---

[17] See Appendix A. This document was unsealed in 2010 from the record of the *In re Visa Check/MasterMoney* antitrust litigation.

[18] There are issues with EMV because the technology is just one privately owned solution. For example, EMV includes specifications for near field communications that would form the technological basis of Visa and MasterCard's mobile payments solutions. That raises serious antitrust concerns for retailers because we are just starting to get some competitors exploring mobile payments. If the currently dominant card networks are able to lock-in their proprietary technology in a way that locks-out competition in mobile payments, that would be a bad result for merchants and consumers who might be on the verge of enjoying the benefits of some new innovations and competition.

So, while chip cards would be a step forward in terms of improving card products, if EMV is forced as the chip card technology that must be used—rather than an open-source chip technology which would facilitate competition and not predetermine mobile payment market-share—it could be a classic case of one step forward and two steps backward.

[19] The Nilson Report, Issue 934, Sept. 2009 at 7.

Tokenization is another variant that could be helpful. Tokenization is a system in which sensitive payment card information (such as the account number) is replaced with another piece of data (the "token"). Sensitive payment data could be replaced with a token to represent each specific transaction. Then, if a data breach occurred and the token data were stolen, it could not be used in any other transactions because it was unique to the transaction in question. This technology has been available in the payment card space since at least 2005.[20] Still, tokenization is not a panacea, and it is important that whichever form is adopted be an open standard so that a small number of networks not obtain a competitive advantage, by design, over other payment platforms

In many models tokenization occurs "after the fact"—generally post authorization. Thus some fraud risk remains. To deal with this point-to-point encryption is preferred and would be complimentary to tokenization. The former would occur between the card being read and the assignment of a token. From the merchant's perspective, tokenization involves significant operational changes and could carry significant out-of-pocket costs. Despite that, for the majority of transactions, tokenization still may not address both ends of the security/authentication equation as well as would PIN and Chip. It has greatest utility in the 6 percent of transactions that currently do not occur face-to-face. Consequently, while point-to-point encryption and tokenization could be valuable adjuncts to PIN and Chip authentication, they are not a substitute.

In addition, in some configurations, mobile payments offer the promise of greater security as well. In the mobile setting, consumers won't need to have a physical card—and they certainly won't replicate the security problem of physical cards by embossing their account numbers on the outside of their mobile phones. It should be easy for consumers to enter a PIN or password to use payment technology with their smart phones. Consumers are already used to accessing their phones and a variety of services on them through passwords. Indeed, if we are looking to leapfrog the already aging current technologies, mobile-driven payments may be the answer.

Indeed, as much improved as they are, chips are essentially dumb computers. Their dynamism makes them significantly more advanced than magstripes, but their sophistication pales in comparison with the common smartphone. Smartphones contain computing powers that could easily enable comparatively state-of-the-art fraud protection technologies. The phones soon may be nearly ubiquitous, and if their payment platforms are open and competitive, they will only get better.

The dominant card networks have not made all of the technological improvements suggested above to make the cards issued in the United States more resistant to fraud, despite the availability of the technology and their adoption of it in many other developed countries of the world, including Canada, the United Kingdom, and most countries of Western Europe.

In this section, we have merely described some of the solutions available, but the United States isn't using any of them the way that it should be. While everyone in the payments space has a responsibility to do what they can to protect against fraud and data theft, the card networks have arranged the establishment of the data security requirements and yet, in light of the threats, there is much left to be desired.

A Better System

How can we make progress toward the types of solutions that would reduce the crimes of data theft and fraud? One thing seems clear at this point: we won't get there by doing more of the same. We need PIN-authentication of card holders, regardless of the chip technology used on newly issued cards. We also need chip cards that use open standards and allow for competition among payment networks as we move into a world of growing mobile commerce. Finally, we need companies throughout the payment system to work together on achieving end-to-end encryption so that there are no weak links in the system where sensitive card payment information may be acquired more easily than in other parts of the system.

Steps Taken by Retailers After Discovery of a Breach of Security

In our view, it is after a fulsome evaluation of data breaches, fraud, the payments system and how to improve each of those areas in order to deter and prevent problems that we should turn to the issue of what to do when breaches occur. Casting blame and trying to assign liability is, at best, putting the cart before the horse and,

---

[20] For information on Shift4's 2005 launch of tokenization in the payment card space see *http://www.internetretailer.com/2005/10/13/shift4-launches-security-tool-that-lets-merchants-re-use-credit.*

at worst, an excuse for some actors to ignore their own responsibility for trying to prevent these crimes.

One cannot reasonably demand greater security of a system than the system is reasonably capable of providing. Some participants act as if the system is more robust than it is. Currently, when the existing card products are hit in a criminal breach, that company is threatened from many sides. The threats come from entities seeking to exact fines and taking other penalizing action even before the victimized company can secure its network from further breaches and determine through a forensic analysis what has happened in order to notify potentially affected customers. For example, retailers that have suffered a breach are threatened with fines for the breach based on allegations of non-compliance with PCI rules (even when the company has been certified as PCI-compliant). Other actors may expect the breached party to pay for all of the fraudulent transactions that take place on card accounts that were misused, even though the design of the cards facilitated their subsequent counterfeiting. Indeed, some have seriously suggested that retailers reimburse financial institutions for the cost of reissuing more fraud-prone cards. And, as a consequence of the breach, some retailers must then pay higher fees on its card transactions going forward. Retailers pay for these breaches over and over again, despite often times being victims of sophisticated criminal methods not reasonably anticipated prior to the attack.

Breaches require retailers to devote significant resources to remedy the breach, help inform customers and take preventative steps to ward off future attacks and any other potential vulnerabilities discovered in the course of the breach investigation. Weeks or months of forensic analysis may be necessary to definitively discover the cause and scope of the breach. Any discovered weaknesses must be shored up. Quiet and cooperative law enforcement efforts may be necessary in an effort to identify and capture the criminals. Indeed, law enforcement may temporarily discourage publication of the breach so as to not alert the perpetrators that their efforts have been detected.

It is worth noting that in some of these cases involving payment card data, retailers discover that they actually were not the source of the breach and that someone else in the payments chain was victimized or the network intrusion and theft occurred during the transmission of the payment card data between various participants in the system. For this reason, early attempts to assign blame and shift costs are often misguided and policy makers should take heed of the fact that often the earliest reports are the least accurate. Additionally, policy makers should consider that there is no independent organization devoted to determining where a breach occurred, and who is to blame—these questions are often raised in litigation that can last for years. This is another reason why it is best to at least wait until the forensic analysis has been completed to determine what happened. Even then, there may be questions unanswered if the attack and technology used was sophisticated enough to cover the criminals' digital tracks.

The reality is that when a criminal breach occurs, particularly in the payments system, all of the businesses that participate in that system and their shared customers are victimized. Rather than resort to blame and shame, parties should work together to ensure that the breach is remedied and steps are taken to prevent future breaches of the same type and kind.

Legislative Solutions

In addition to the marketplace and technological solutions suggested above, NRF also supports a range of legislative solutions that we believe would help improve the security of our networked systems, ensure better law enforcement tools to address criminal intrusions, and standardize and streamline the notification process so that consumers may be treated equally across the Nation when it comes to notification of data security breaches.

From many consumers' perspective payment cards are payment cards. As has been often noted, consumers would be surprised to learn that their legal rights, when using a debit card—i.e. their own money—are significantly less than when using other forms of payment, such as a credit card. It would be appropriate if policy makers took steps to ensure that consumers' reasonable expectations were fulfilled, and they received at least the same level of legal protection when using their debit cards as they do when paying with credit.

In addition, NRF supports the passage by Congress of the bipartisan "Cyber Intelligence Sharing and Protection Act" (H.R. 624) so that the commercial sector can lawfully share information about cyber-threats in real-time and enable companies to defend their own networks as quickly as possible from cyber-attacks as soon as they are detected elsewhere by other business.

We also support legislation that provides more tools to law enforcement to ensure that unauthorized network intrusions and other criminal data security breaches are thoroughly investigated and prosecuted, and that the criminals that breach our systems to commit fraud with our customers' information are swiftly brought to justice.

Finally, and for nearly a decade, NRF has supported passage of legislation that would establish one, uniform Federal breach notification law that would be modeled on, and preempt, the varying breach notification laws currently in operation in 46 states, the District of Columbia and Federal territories. A Federal law could ensure that all entities handling the same type of sensitive consumer information, such as payment card data, are subject to the same statutory rules and penalties with respect to notifying consumers of a breach affecting that information, Further, a preemptive Federal breach notification law would allow retailers and other businesses that have been victimized by a criminal breach to focus their resources on remedying the breach and notifying consumers rather than hiring outside legal assistance to help guide them through the myriad and sometimes conflicting set of 50 data breach notification standards in the state and Federal jurisdictions. Additionally, the use of one set of standardized notice rules would permit the offering to consumers of the same notice and the same rights regardless of where they live.

Conclusion

In closing three points are uppermost.

First, retailers take the increasing incidence of payment card fraud very seriously. We do so as Main Street members of the community, because it affects our neighbors and our customers. We do so as businesses, because it affects the bottom line. Merchants already bear at least an equal, and often a greater, cost of fraud than any other participant in the payment card system. We have every reason to want to see fraud reduced, but we have only a portion of the ability to make that happen. We did not design the system; we do not configure the cards; we do not issue the cards. We will work to effectively upgrade the system, but we cannot do it alone.

Second, the vast majority of breaches are criminal activity. The hacked party, whether a financial institution, a card network, a processor, a merchant, a governmental institution, or a consumer is the victim of a crime. Traditionally, we don't blame the victim of violence for the resulting stains; we should be similarly cautious about penalizing the hackee for the hack. The payment system is complicated. Every party has a role to play; we need to play it together. No system is invulnerable to the most sophisticated and dedicated of thieves. Consequently, eliminating all fraud is likely to remain an aspiration. Nevertheless, we will do our part to help achieve that goal.

Third, it is long past time for the U.S. to adopt PIN and chip card technology. The PIN authenticates and protects the consumer and the merchant. The chip authenticates the card to the bank. If the goal is to reduce fraud we must, at a minimum, do both.

APPENDIX A

Exhibit 499

Visa U.S.A. Inc.

Debit Advisors Meeting

Phoenix, Arizona
February 28 - March 1, 1990

Agenda

Wednesday, February 28	
Continental Breakfast	7:30 a.m. - 8:00 a.m.
Welcome and Introduction	8:00 a.m. - 8:15 a.m.
UK Market Update	8:15 a.m. - 8:45 a.m.
Review of Merchant Visits/ FMI and Research Update	8:45 a.m. - 9:15 a.m.
Fraud Experts Conclusions	9:15 a.m. - 9:45 a.m.
Break	9:45 a.m. - 10:00 a.m.
Product Concept "Z," Version 3	10:00 a.m. - 10:45 a.m.
Group Session Introduction	10:45 a.m. - 11:00 a.m.
Group Sessions	11:00 a.m. - 12:00 noon
Lunch	12:00 noon - 1:00 p.m.
Group Sessions (continued)	1:00 p.m. - 4:30 p.m.
Cocktail Reception and Dinner	6:00 p.m.
Thursday, March 1	
Continental Breakfast	8:00 a.m. - 8:30 a.m.
Group Presentations and Discussion	8:30 a.m. - 10:00 a.m.
Break	10:00 a.m. - 10:15 a.m.
Business Case Review	10:15 a.m. - 11:30 a.m.
Wrap-up	11:30 a.m. - 12:00 noon

Visa U.S.A. Inc.

Debit Advisors Meeting

Phoenix, Arizona
February 28 - March 1, 1990

Table of Contents

UK MARKET UPDATE

The banks in the United Kingdom have recently introduced debit products into their marketplace, which is a well established credit card market. The combination of the product positioning and marketing caused significant merchant backlash resulting in major price concessions by the banks.

To provide background for the Advisors' discussions on debit product introduction into the U.S. market, a presentation will be given covering these events in the UK.

REVIEW OF MERCHANT VISITS

The "Z" debit product concept was defined by Visa and presented to the Advisory Committee in November 1989. To better assess the marketability of the service, it was determined that the "Z" product concept should be shared with the merchant community. Because November and December were such busy months for retailers, a wide-scale merchant survey was impractical during this time. However, it was decided that a limited number of on-site merchant interviews could be accomplished quickly.

Therefore, during the month of December 1989, Visa and Global Concepts visited ten (10) merchants to better understand their payment operations, and to solicit their opinions on a variety of debit card attributes such as PINs, signatures, electronic returns, tiered offerings including a guarantee, service value, target marketing, etc.

The ten (10) merchants that were visited are shown below:

Company	Location	Contact
Safeway	San Francisco, CA	Melanie Hobden
Ralph's	Los Angeles, CA	Roger Borneman
Farm Fresh	Norfolk, VA	Glenn Sharpe
Giant Food	Landover, MD	Mike Mann
Exxon	Houston, TX	Richard Phegley
Texaco (telephone)	Houston, TX	Ken Zell
Southland	Dallas, TX	Keith Jenkins
Circle K	Phoenix, AZ	Anita Best
Radio Shack	Fort Worth, TX	Virginia Meyer
Target	Minneapolis, MN	Carrie Lichtenberg

In most cases the acquiring Visa bank provided the contact name at the merchant, and in some instances the acquirer even participated in the interview.

The purpose of the visits was to test the "Z" product attributes against both the current merchant payment procedures and their desired future payment procedures.

A presentation to review the major findings will be made at the meeting.

FRAUD EXPERTS CONCLUSIONS

PROJECT OBJECTIVES AND SCOPE

The primary objectives of the fraud project and the January 9-11, 1990, fraud experts meeting are to identify and rank fraud risks associated with the "Z" debit product concept that is currently under development by Visa U.S.A. Merchant, acquirer and issuer fraud risks are included in this evaluation. Additionally, the experts will specify controls for the fraud risks they identify and rank.

SELECTION CRITERIA FOR EXPERTS

"Z" does not currently exist in the marketplace; therefore, experts from related fields are evaluating fraud risks associated with the product concept.

Professionals from Visa Member banks, retailers from food and oil companies, industry vendors and Visa Security & Risk Management staff experts are participating in the project. They are recognized experts on POS debit, credit card, ATM and check fraud and are principally senior business managers with direct responsibility for risk management and/or fraud at their companies.

METHODOLOGY

A modified Delphi technique, a set of procedures designed to balance individual expert opinions with group consensus, was used to develop a consensus among industry fraud experts. The process is as follows:

Round 1: Development of Individual Positions

Prior to the group meeting, each expert was asked to develop their own fraud position based on their interpretation of the debit product concept. A questionnaire was sent to each expert on December 15, 1989, to rank fraud risks associated with the proposed debit product. The completed questionnaires were returned to Visa, consolidated and summarized for the Fraud Experts Meeting in January.

Round II: Development of Group Positions

Through group and breakout discussions at the January meeting, group positions were developed. Individuals contributed to one another's understanding of the issues and the difficulties involved, and personal opinions were refined as a result of Round II discussions. Individual and group opinions were discussed to eliminate misinterpretations and to bring to light knowledge available from one or a few members of the group. To facilitate this process, the format was:

- At the onset of the meeting, experts with divergent views presented their positions and the group discussed them.

- The experts were then grouped together with several of their peers to discuss their individual positions and develop a joint opinion.

- Each of the three small groups reported on their position to the entire group, differences were questioned and a consensus position developed.

Additionally, each expert completed a second questionnaire following the small group discussions.

Rounds III and IV: Finalization of Experts' Consensus

Two post meeting questionnaires were completed by the fraud experts on January 19 and February 15, 1990. The group consensus included in the project report is the position that resulted from the final, Round IV questionnaire.

INTERIM PRESENTATION TO DEBIT ADVISORS

An interim presentation will be given to the Debit Advisors at the end of February 1990 in which the experts' ranking of fraud risks to merchants, acquirers and issuers will be reviewed. Additionally, the January meeting and final fraud report will be reviewed.

FINAL REPORT

The final report will be published at the end of March 1990. It will include the experts' ranking of fraud risks, their consensus on key fraud issues, a comparison of the Debit Advisors' fraud survey and experts' consensus, a summary of the January meeting, the results of the four Delphi questionnaires, the results of the Debit Advisors Fraud Survey, biographies for the fraud experts and related background information and data.

PRODUCT CONCEPT "Z," VERSION 3

Mark

Separate from Visa bands design

Signifies POS only, not an ATM mark

Signifies debit only

Coexistence with Visa logo not permitted

Third party ACH product option not acceptable

Market

Universally issued

Medium value positioning to consumers

National issuance and acceptance

Displaces cash and checks

Point of Sale Operations

Tiered service levels

- Issuer Guaranteed (Primary service)
- Non-Guaranteed (Secondary service)
  Merchant downtime and override
  - Stand-alone service not necessary for product launch

Tiered merchant risk commensurate with price

Tiered issuer risk commensurate with interchange fee income

PIN and signature for cardholder identification

Critical Mass

Compatible with BASE I/II and Debit System

Compatible with current ATM network systems

GROUP SESSION INTRODUCTION

Brief presentations will be made to the group to explain the benefits of an on-line debit product ("Z") and an off-line debit product (Visa Debit). Following this the advisors will break into two working groups and will be asked to identify all positive aspects of only one of the products as well as the drawbacks. If possible, the group should work to resolve the drawbacks. The group may also wish to discuss reasons why the other product, which is being supported by the other working group, will not work in the marketplace.

A list of the working groups and the product each will be asked to support follows:

Off-line Debit Product Group	**On-line Debit Product Group**
Debby McWhinney, Leader	Tommy Lewis, Leader
Joel Crabtree	Loraine Boland
John Davis	Bob Copeland
Denny Dumler	Bill Fackler
Dave Fronek	Phil Heasley
Fran Gormley	Steve Iovino
Bil Lyons	Jimmy Lewin
Ken Rosfeld	Lynn Page
John Thompson	John Sikkink
<u>Staff</u>	
Wes Tallman	Gerald Hawke
Jeanne Schapp	Mary Buckley
Allen Lipis	Steve White
Chris Schellhorn	Joel Friedman

GROUP SESSIONS

PRESENTATION NOTES

Off-line Debit Product

- Internationally recognized logo
- Existing operational infrastructure
- Proven profitability
  - Merchant discount income
  - Interchange fee income
  - Cardholder fees
- Fourteen years of experience in the marketplace
  - Issuance
  - Acceptance
- Signifies acceptance at POS locations worldwide
  - Existing merchant base, 7 million
- Signifies acceptance at ATMs worldwide
  - Existing ATM network, 40,000

On-line Debit Product

- Universally issued
- Appeals to non-plastic accepting merchants
  - Cash and check
  - High transaction volume
  - Repeat business
- Safest product for banks, less fraud
- Safest product for consumers
- Carries the best guarantee for merchants
- Provides ability for merchants to fully integrate payment mechanism with their other automation activities
- Eliminates need to store paper
- Compatible with existing ATM network procedures
- Will benefit from future economies of scale
  - Costs will come down
  - Income will increase
- Consumer friendly
  - Ease to use
  - Eliminates bulky checkbook

GROUP PRESENTATIONS AND DISCUSSION

Enhanced presentations on the off-line and on-line debit products will be given. Following discussion, individuals will be asked to accept or reject either alternative and provide reasons for their selection.

BUSINESS CASE REVIEW

Visa has hired Andersen Consulting to assist in the development of a business case for debit at the point of sale. A presentation will be made explaining the process, the major business assumptions that have been made, and the current status.

RETAIL INDUSTRY LEADERS ASSOCIATION
Arlington, VA, March 26, 2014

Hon. JAY ROCKEFELLER,
Chairman,
Committee on Commerce, Science, and Transportation,
United States Senate
Washington, DC.

Hon. JOHN THUNE,
Ranking Member,
Committee on Commerce, Science, and Transportation,
United State Senate,
Washington, DC.

Dear Chairman Rockefeller and Ranking Member Thune:

On behalf of the Retail Industry Leaders Association (RILA), thank you for the opportunity to offer our comments on the record for the Commerce, Science & Transportation Committee's hearing, "Protecting Personal Consumer Information from Cyber Attacks and Data Breaches." By way of background, RILA is the trade association of the world's largest and most innovative retail companies. RILA promotes consumer choice and economic freedom through public policy and industry operational excellence. Its members include more than 200 retailers, product manufacturers, and service suppliers, which together account for more than $1.5 trillion in annual sales, millions of American jobs and operate more than 100,000 stores, manufacturing facilities and distribution centers domestically and abroad.

Retailers take the threat of cyber-attacks extremely seriously and work diligently every day to stay ahead of the sophisticated criminals behind them. Retail companies individually, and the industry collectively, are taking aggressive steps to counter these threats. While enhanced security measures help retailers thwart thousands of cyber-attacks every day, unfortunately some attacks are successful and the resulting incidents can affect millions of our customers. For retailers, such a breach can damage the relationship that we have with our customers. However, more broadly, a breach can undermine consumers' faith in the electronic payments system as stolen information can be used to produce fraudulent cards for illicit use or put the customer at risk of identity theft.

Given these facts, retailers take extraordinary steps to strengthen overall cybersecurity and prevent attacks. Retailers secure their systems with substantial investments in experts and technology. Further, they employ many tactics and tools to secure data, such as data encryption, tokenization and other redundant internal controls, including a separation of duties. While these enhanced security measures help to rebuff attacks, retailers are constantly working to expand existing cybersecurity efforts.

Collaboration within the industry and coordination with other stakeholders is essential. In January, RILA launched its Cybersecurity and Data Privacy Initiative which focuses on strengthening overall cybersecurity. As part of this initiative, RILA has formed the Retail Cybersecurity Leaders Council (RCLC) and we are additionally calling for the development of Federal data breach notification legislation. Made up of senior retail executives responsible for cybersecurity, the RCLC will aim to improve industry-wide cybersecurity by providing a trusted forum for all stakeholders to share threat information and discuss effective security solutions.

Subsequently, RILA formed a partnership with the National Cyber-Forensics and Training Alliance (NCFTA) to enhance cybersecurity information sharing and expand retailers' proactive and vigilant approach to cyber threats to protect consumers against criminals. Partnering with the NCFTA is one of several approaches RILA is taking to enhance collaboration across the entire payments system. This partnership will help retailers leverage the NCFTA's vast network of cybersecurity threat intelligence and resources, and will advance the RCLC's mission of information sharing amongst retailers.

RILA and the retail industry have taken strides to improve security and form strategic partnerships to improve information sharing. RILA calls on Congress to enact Federal data breach notification legislation that is practical, proportional and sets a single national standard, replacing the patchwork of state laws currently in place. A Federal standard will help ensure that customers receive timely and accurate information following a breach, and any legislation considered by Congress should include three essential provisions. First, strong state pre-emption language that would create a single national standard replacing the current patchwork of 46 state notification laws that add unnecessary complexity to the process. Second, legislation should consider the practical realities following a breach. Specifically, adequate time must be given prior to notification in order to provide reasonable time to secure the breached environment, conduct a thorough forensics investigation, and then based off this assessment, the ability to determine who may have been affected by the cyber-attack and what information was compromised. Furthermore, reason-

able delay provisions should be included at the request of law enforcement for investigative purposes or for national security reasons. Third, notification requirements should be linked to risk of harm, whether or not the compromised information is in usable form to commit financial fraud or identity theft.

While retailers understand and manage their internal systems and security, they have little or no influence over the actions taken by other players in the payments universe, which may have enormous implications on fraud. Instead, retailers must rely on others in the payments ecosystem to dictate critical security decisions, including card technology, retailer terminals, and when data can be encrypted during the transmission between retailers and the card networks. Retailers have long argued that the card technology in place today is antiquated; the unfortunate reality is that criminals can use stolen consumer data to create counterfeit cards with stunning ease. For years, retailers have urged banks and card networks to adopt the enhanced fraud prevention technology in use around the world here in the United States. While their resistance to doing so has been great, retailers continue to press all other stakeholders in the payments system to make this a priority.

The RILA plan focused on four major steps that should be taken to improve the security of debit and credit cards. First, quickly establish a plan to retire antiquated magnetic stripe technology in place today. Second, require cardholders to input a PIN on all card transactions. Banks require that cardholders enter a PIN number to withdraw money from an ATM; the same fraud protection should apply to retail transactions. Third, establish a roadmap to migrate to chip-based smart card technology with PIN security, also known as Chip and PIN. Finally, recognizing that card security must outpace criminal advancements, the members of the payments ecosystem must work together to identify new technologies and long-term, comprehensive solutions to the threats.

We recognize that retailers are only one piece of the payments ecosystem, and so our Cybersecurity and Data Privacy Initiative also called for collaboration among retailers, banks and card networks to advance improved payments security. In February, RILA joined with the Financial Services Roundtable (FSR) to form the Merchant and Financial Services Industries Cybersecurity Partnership with 16 other trade associations representing both merchants and financial services companies. The Partnership will enhance system-wide collaboration and will explore paths to increased threat information sharing, better card security technology, and maintaining the trust of customers. Specifically, the partnership is focusing on improving overall security across the payments ecosystem, and bolstering consumer confidence in the security of their payment data and the systems used to process payments. The group has identified five focus areas to help achieve the goals: threat information sharing, cybersecurity risk mitigation, enhanced security for card present transactions, enhanced security for card-not-present and mobile, and data breach notification and cyber security legislation. We have little doubt that all parties share the goals of protecting consumers and maintaining confidence in our payments systems. In order to accomplish these goals, we must set aside our previous disagreements and work together on common solutions. That is why RILA is reaching out to representatives across the business community, including the card networks and financial institutions of all sizes, in an effort to work together to identify near-and long-term solutions.

In closing, by working together with public-private sector stakeholders, our ability to develop innovative solutions and anticipate threats will grow, enhancing our collective security and giving our customers the service and peace of mind they deserve. We appreciate the opportunity to submit these comments for the record and we look forward to working with you and your staff on these issues moving forward.

Sincerely,

BILL HUGHES
Senior Vice President, Government Affairs.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO HON. EDITH RAMIREZ

Question. Senators Feinstein, Pryor, Nelson, and I have introduced S. 1976, the Data Security and Breach Notification Act of 2014. The bill would, among other things, require entities that maintain personal information on consumers to establish protocols that secure information. The FTC would be tasked with issuing regulations that detail the statutory scope of this mandate.

The FTC has a long history of using its existing authority under Section 5 of the FTC Act to pursue companies that fail to adequately protect consumers' personal information. The agency has also called for data security legislation.

Given its success with using Section 5, please explain why the agency sees the need for data security legislation such as S. 1976.

Answer. The FTC supports Federal legislation such as S. 1976 that would (1) strengthen its existing authority governing data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach. While the majority of states have data breach notification laws, few have specific laws requiring general data security policies and procedures. Breach notification and data security standards at the Federal level would extend notifications to all citizens nationwide and create a strong and consistent national standard that would simplify compliance by businesses while ensuring that all American consumers are protected.

Specifically, the FTC supports legislation that would give the Commission the authority to seek civil penalties to help deter unlawful conduct, jurisdiction over non-profits, and rulemaking under the Administrative Procedure Act. We have urged Congress to allow the FTC to seek civil penalties for all data security and breach notice violations in appropriate circumstances to help ensure effective deterrence. In addition, enabling the FTC to bring cases against non-profits—such as educational institutions and health facilities, which have been the subject of a number of breaches—would help ensure that consumer data is adequately protected regardless of what type of entity collects or maintains it.

Finally, rulemaking authority under the Administrative Procedure Act would enable the FTC to respond to changes in technology when implementing the legislation. For example, whereas a decade ago it would be both difficult and expensive for a company to track an individual's precise geolocation, the explosion of mobile devices has made such information readily available. As technology and business models change and new forms of consumer data can be used to perpetrate identity theft, fraud, and other types of harm, APA rulemaking authority would help ensure that the law is kept up to date.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO HON. EDITH RAMIREZ

Question 1. In your testimony, you reference "geolocation information" as a rapidly emerging technology. The FTC has also referred previously to "precise geolocation data," for instance in a 2012 Commission report, proposing to protect the privacy of sensitive data including "precise geolocation data."

In the 2012 report, the FTC recommended that, before any firm could collect, store or use such data, it would be required to "provide prominent disclosures and obtain affirmative express consent before using data in a manner materially different than claimed at the time of collection." This sounds reasonable in certain circumstances. However, the Commission did not define the term "precise geolocation data." The Commission does advise that geolocation data that cannot be reasonably linked to a specific consumer would not trigger a need to provide a consumer protection mechanism, and further advises that if a firm takes steps to de-identify data, it would not need to provide this mechanism. However, because the FTC does not define relevant terms, I have heard that there is some concern for how practitioners in the mapping and surveying fields can comply with the guidance. Specifically, some stakeholders are concerned that a private firm would need to get a citizen's approval before developing mapping for an E–911 and emergency response management system. What does the FTC consider to be "precise geolocation data"?

Answer. Precise geolocation data includes any information that can be used to pinpoint a consumer's physical location. For example, many mobile applications ("apps") collect a user's longitude and latitude coordinates, which allows them to translate a user's exact location on a map. It does not include general location data, such as a consumer's zip code, city, or town. In the context of the Children's Online Privacy Protection Act (COPPA), the statute and the Commission's COPPA Rule require parental consent for the collection of geolocation information sufficient to identify street name and name of city or town.

Question 1a. When mapping for an E–911 or emergency response management system, what level of de-identification is needed? Does a company need to secure everyone's prior approval, or else redact from the map every citizen for whom they did not get prior consent, when mapping for an E–911 or emergency response management system?

Answer. In its 2012 Privacy Report, the Commission set forth a privacy framework that calls on companies to incorporate privacy by design, simplified consumer choice, and increased transparency into their business operations. It is important to note that the framework is a voluntary set of best practices designed to assist com-

panies as they operationalize privacy and data security practices within their businesses. It neither imposes new legal obligations, nor is it intended as a template for law enforcement.

The framework calls on companies to offer an effective consumer choice mechanism unless the data practice is consistent with the "context of the interaction" between the consumer and the company. Under this approach, whether a company should provide choice "turns on the extent to which the practice is consistent with the context of the transaction or the consumer's existing relationship with the business, or is required or specifically authorized by law."[1] Mapping for an E–911 or emergency response management system would generally fall within the context of the interaction, and therefore companies that collect and use of geolocation information for these purposes do not need to provide a consumer choice mechanism.

Question 1b. I understand the Commission received significant public comment on this issue from engineers, architects, planners, surveyors, mappers and the Federal Geographic Data Committee, which represents Federal mapping agencies. Can you tell me what the FTC's thinking is on this issue, and what its plans are to address the stakeholders' concerns?

Answer. When members of the geospatial industry collect addresses, parcel information, or other geolocation or survey data that is tied to public land records, this practice would generally fall within the "context of the interaction" standard. As any consumer who has purchased a house knows, public land record data is collected, used, and linked to specific consumers as a matter of course in connection with real estate transactions as well as property tax assessments and similar purposes. Accordingly, companies that collect and use this data for these purposes would generally not need to provide a consumer choice mechanism.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KELLY AYOTTE TO HON. EDITH RAMIREZ

Question 1. Earlier this year, the FTC testified before the Senate Banking Committee on safeguarding consumers when there is a security breach. What precisely triggers notification? There are 46 different state laws. In your opinion, what should be the threshold warranting a notification? Since the combination of certain types of personal information is more sensitive than each piece individually, what type of information being breached should warrant a notification to consumers?

Answer. It is important for both consumers and businesses that the trigger for breach notification is balanced. We want to ensure that consumers learn about breaches that could result in identity theft, fraud, or other harm so they can take steps to help protect themselves, but we do not want to notify consumers when the risk of harm is negligible, as over-notification could cause consumers to become confused or to become numb to the notices they receive.

Consumers should be given notice when information is breached that could be misused to harm consumers. At a minimum, companies should notify consumers of a breach of Social Security numbers because this information can be used to commit identity theft, even if not paired with an individual's name and address. Similarly, an account username and password can be used to gain access to an account, even if the thief does not have the name of the account holder. Additionally, in the event of changing technology or business models, the FTC should be able to exercise rulemaking authority to modify the definition of personal information.

I am happy to work with the Committee as it considers legislation on this important matter.

Question 2. You testified regarding your important work in civil law enforcement against unfair or deceptive acts in data security practices. Is it safe to assume that you believe the Commission has existing authority to pursue enforcement actions against private businesses that fail to adopt reasonable data security practices?

Answer. Yes. The Commission has authority to challenge companies' data security practices that are unfair or deceptive under Section 5 of the FTC Act, and we have used this authority to settle 52 data security cases to date. In addition, Congress has given the FTC authority to bring data security enforcement actions against nonbank financial institutions under the Gramm-Leach-Bliley Act, against consumer credit reporting agencies under the Fair Credit Reporting Act, and against websites and online services directed at children under the Children's Online Privacy Protection Act.

---

[1] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 38–39 (Mar. 2012).

The Commission has called for data security legislation that would strengthen its existing authority. For example, we currently lack authority under Section 5 to obtain civil penalties, an important remedy for deterring violations. Likewise, enabling the FTC to bring cases against non-profits, which have been the source of a number of breaches, would help ensure that whenever personal information is collected from consumers, entities that maintain such data take reasonable measures to protect it.

Question 3. What additional tools do law enforcement need to share information about ongoing threats and attacks with the private sector?

Answer. Information sharing is an important part of the fight against those who attempt to exploit consumers' personal information. Information exchanges such as Information Sharing and Analysis Centers (ISAC) enable companies to pool information about security threats and defenses so that they can prepare for new kinds of attacks and quickly address potential vulnerabilities. ISACs may also share information with law enforcement agencies, and vice-versa. The FTC is considering, at the request of members of Congress, the formation of an ISAC to enable retailers to share information. We have begun consulting with other ISACs and industry groups to explore the formation of such a group.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DEB FISCHER TO HON. EDITH RAMIREZ

Question 1. In your testimony, you state that "having a strong and consistent national requirement would simplify compliance by businesses while ensuring that all consumers are protected." Do you believe preempting state laws in favor of a strong national requirement would benefit, not harm, consumers?

Answer. I support a Federal data security and breach notification law that would preempt state law, but only if such a standard is sufficiently strong and the states are given the ability to enforce the law. If a consistent nationwide standard came at the expense of weakening existing state legal protections for consumers' information, I would not support the law.

Question 2. Would a uniform Federal data breach notification law enforced by the Commission, as well as states attorneys general, provide a significantly greater level of protection for consumers than currently exists?

Answer. While the majority of states have data breach notification laws, few have specific laws requiring general data security policies and procedures. Breach notification and data security standards at the Federal level would extend notifications to all consumers nationwide and create a level playing field so that businesses operating in numerous states can apply one standard. A Federal law could create uniform protections for all American consumers.

Question 3. Many different players in the Internet ecosystem increasingly collect and store the same or similar information. Should they all be subject to the same standards for data security?

Answer. All companies that collect and handle sensitive consumer information should be required to implement reasonable data security measures. We believe that reasonableness is the appropriate standard because it allows a company flexibility to develop a data security program based on factors such as the sensitivity and volume of consumer information it holds; the size and complexity of its data operations; and the cost of available tools to improve security and reduce vulnerabilities. The Commission has emphasized a process-based approach to data security that includes designating an individual or individuals responsible for data security; conducting risk assessments; designing a security program to address risks, including administrative, physical, and technical safeguards; and adjusting the program to address changes.

Question 4. In your written testimony, you express concern about data security legislation's ability to keep pace with technology. Would a "reasonableness" standard help address that concern because what is reasonable today may not be reasonable tomorrow as technology evolves?

Answer. That is correct. The Commission's reasonableness standard and emphasis on a process-based approach to data security encourages companies to reevaluate and adjust their programs periodically in light of changes to the types of information they collect as well as changes in the marketplace, including changes in technology.

Additionally, we support Federal data security and breach notification legislation that would, among other things, authorize rulemaking under the Administrative Procedure Act to give the Commission the flexibility to implement the statute by making changes when appropriate. For example, this authority should include the

authority to modify the definition of personal information in response to changes in technology and changing threats.

Question 5. You mention in your testimony that the data security provisions of both the Fair Credit Reporting Act and the Children's Online Privacy Protection Act rely on a "reasonableness" standard. Should comprehensive Federal data security legislation also be subject to a reasonableness standard?

Answer. Yes. A reasonableness standard would ensure that companies have strong protections in place to protect consumer information as well as flexibility when developing and implementing any data security program.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO JOHN J. MULLIGAN

Question 1. Target's representatives told us that its point-of-sale (POS) devices at U.S. stores use different operating systems and software than its devices at Canadian stores. According to published reports, U.S. stores run on Target-designed software that is used with Windows XP Embedded and Windows Embedded for Point of Service, while Canadian locations use POS devices from Retalix, an NCR company.

Please explain why Target uses different POS operating systems and software in the United States and Canada.

Answer. The U.S. and Canada have different payment card technologies in use in the respective countries, resulting in the use of different payment systems and software. As of 2013, the overwhelming majority of payment cards issued in the U.S. were not chip-enabled. This remains the case today.

In the U.S., Target processes point of sale transactions using a Target-built application. We are in the process of completing the implementation of Windows Embedded for Point of Sale (POS Ready 7) on all of our registers in 2014. In Canada, Target processes point of sale transactions using Retalix in order to process chip-enabled cards, which are required in Canada.

Question 1a. The 2013 breach was limited to Target's U.S. stores; its Canadian stores were not affected. Do you believe weaknesses in Target's POS operating system or software used for U.S. stores allowed or contributed to the breach?

Answer. As of 2013, the overwhelming majority of payment cards issued in the U.S. were not chip-enabled. This remains the case today. In Canada, credit and debit cards are required to be chip-enabled. The malware that was designed to capture card data at Target stores in the U.S. would not be able to capture the same information from a chip-enabled card transaction. Unlike Canada, however, chip-enabled cards are not common, let alone standard, in the U.S.

Target is accelerating our $100 million investment in the adoption of chip technology because we believe it is critical to enhancing consumer protections. We have already installed approximately 10,000 chip-enabled payment devices in Target stores and expect to complete the installation in all Target stores by this September, six months ahead of schedule. We also expect to begin to issue chip-enabled Target REDcards and accept all chip-enabled cards by early 2015. As a founding member and steering committee member of the EMV Migration Forum, we will continue to lead the adoption of these technologies across the payment ecosystem.

Question 1b. Going forward, does Target plan to upgrade its POS operating systems and software used in its U.S. locations? If so, how?

Answer. While it is not a requirement, we believe the adoption of chip technology is critical to enhancing consumer protections. As noted previously, we have already installed approximately 10,000 chip-enabled payment devices in Target stores and expect to complete the installation in all Target stores by this September, six months ahead of schedule. In the U.S., we are in the process of completing the implementation of Windows Embedded for Point of Sale (POS Ready 7) on all of our registers in 2014.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BILL NELSON TO JOHN J. MULLIGAN

Question 1. Looking beyond just the issue of credit and debit card data, it is my understanding that Target—and many other retailers—collect a substantial amount of personal consumer information for other purposes.

For example, it is my understanding that a number of retailers sometimes require customers to present a drivers' license—and either scan or copy all of the informa-

tion on that license—when they are making a return, even when they have a receipt for the return.

Does Target collect this type of information from consumers when they engage in returns or other related transactions?

Answer. Target swipes or scans guest government-issued identification cards (IDs) in connection with the following limited types of transactions:

1. For the purchase of age-restricted item transactions such as alcohol and M-rated video games;
2. For the purchase of certain medically restricted item transactions, such as pseudoephedrine and dextromethorphan;
3. For returns without receipt;
4. For transactions in which a guest pays for their merchandise and then leaves the store without the merchandise, but later returns to retrieve the merchandise;
5. For certain high-risk check transactions;
6. For cash transactions above $10,000 in order to complete the Internal Revenue Service (IRS) Form 8300, Report of Cash Payments over $10,000; and
7. For tax-exempt transactions, such as sales to nonprofit organizations in order to complete tax-exemption certificates.

There are a handful of states in which IDs cannot be swiped because of state laws prohibiting swiping or because of the absence of a barcode on the state ID. In these states, cashiers manually key information from a guest's ID.

When swiping a guest's ID, Target only collects the data that is relevant to the type of transaction. Additionally, information obtained during the ID swipe is not used for other purposes.

Question 1a. If so, how is this information stored and used?

Answer. When information is collected from a guest's ID, Target does not collect more personal information than necessary for the particular purpose for which the card is swiped and Target uses the information exclusively for that purpose. Guest information is stored for a fixed amount of time depending on the type of transaction. The information is secured. The information is not used for other purposes.

Question 1b. Is that information also shared with any third-parties?

Answer. Target only shares information collected through ID swipes in the following instances: (1) for high risk check transactions Target may share information with vendors that assist Target in authorizing and processing check payments; (2) in certain states, as required by state law, Target provides state authorities information relating to pseudoephedrine purchases; (3) for cash transactions over $10,000, Target submits Form 8300 to the IRS; and (4) for tax-exempt transactions, Target may share tax exemption certificates with state tax auditors upon request. However, Target does not use or share information collected through ID swipes for marketing purposes.

Question 1c. Is it ever deleted from your systems?

Answer. Yes. Guest information is stored for a fixed amount of time depending on the type of transaction. The information is secured.

Question 2. Do you allow customers to request a copy of any personal information file that Target maintains on them?

Answer. In accordance with our privacy policy, Target guests can access or update their personal information.

Question 2a. If so, how do they request it?

Answer. Our privacy policy is available to our guests on Target.com. A guest can click a hyperlink, "Contact Us" to complete a form and submit their request. A guest can also contact Target by phone, e-mail or mail. If a guest has created a Target.com account, they can log in and update their account information, including contact, billing, and shipping information.

Question 2b. If not, why not?

Answer. N/A

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KELLY AYOTTE TO JOHN J. MULLIGAN

Question 1. As a former Attorney General, I can appreciate how crucial information sharing is by law enforcement to both retail stores and financial institutions. Can you both discuss your relationship with the FBI and the Secret Service (or DHS

in general) when it comes to the flow of information that would affect a potential cyber-attack or data breach? Could this relationship be improved? What do you see as the best role for state and local law enforcement in this area?

Answer. All businesses and their customers are facing frequent and increasingly sophisticated attacks by cyber criminals. In order to address this threat, none of us can go it alone. Protecting American businesses and consumers is a shared responsibility.

Target deeply values our longstanding and ongoing partnership with law enforcement. For more than 20 years, we've established ourselves as a valuable partner to law enforcement in their efforts to strengthen public safety. We partner with public safety agencies on the local, state, and national level.

Target participates in a number of initiatives to enhance information sharing including with the U.S. Department of Homeland Security (DHS). This outreach is focused on raising awareness, educating and informing these leaders on our vast public safety efforts, and educating them on our priorities and capabilities. Through this outreach we are able to highlight our unique approach and non-traditional partnerships to address public safety challenges by developing crime solutions and supporting preparedness and resiliency initiatives. Target has played the convener role enabling them to share best practices across jurisdictions. Target also shared organizational leadership insights that could be applied across groups and hosts leadership training programs centered on Target's most effective leadership development courses, but revised and geared toward law enforcement and emergency managers.

The Secret Service has been a valuable partner to Target as they continue to investigate the breach that occurred at Target in late 2013. For example, on the evening of December 12, we were notified by the Justice Department of suspicious activity involving payment cards used at Target stores. We immediately started our internal investigation. On December 13, we met with the Justice Department and Secret Service.

Target is a charter member and serves on the board of the FBI's Domestic Security Alliance Council (DSAC). DSAC is a strategic partnership between the U.S. Government and U.S. Private Industry. Its goal is to advance the Federal Bureau of Investigation (FBI)'s mission of preventing, detecting, and deterring criminal acts by facilitating strong, enduring relationships among its private industry members. In March 2014, Target became the first retailer to join the Financial Services Information Sharing and Analysis Center (FS–ISAC). The *Financial Services Information Sharing & Analysis Center* (FS–ISAC), is a non-profit private sector initiative developed by the financial services industry to help facilitate the detection, prevention, and response to cyber attacks and fraud activity.

Target works closely with state and local law enforcement through our accredited forensic laboratories that specialize in forensics, audio and video analysis, and latent fingerprints. In addition, Target operates 14 Investigations Centers (ICs) nationwide that focus on providing investigative support to our stores and to law enforcement. Today, 30 percent of Target's lab caseload provides pro bono services to law enforcement agencies for violent felony cases that have nothing to do with Target.

Question 2. What steps did Target take internally before notifying your customers that the company had potentially suffered a breach of security that may have affected their payment cards? Were you able to complete a forensic analysis of the breach before notifying customers? If not, why not?

Answer. Our actions leading up to our public announcement on December 19—and since—have been guided by the principle of serving our guests. We moved quickly to share accurate and actionable information with the public. While the forensic analysis of the breach was far from complete, on December 15, we confirmed that criminals had infiltrated our system, installed malware on our point-of-sale network and potentially stolen guest payment card data. We then began notifying the payment processors and card networks, preparing to publicly notify our guests, and equipping call centers and stores with the necessary information and resources to address our guests' concerns. When we announced the intrusion on December 19, we used multiple forms of communication, including a mass-scale public announcement, e-mail, prominent notices on our website, and social media. The forensic analysis is estimated to be completed later in 2014.

Question 3. What steps do you believe are reasonable, if not necessary, for breached companies to take before notifying potentially affected customers of a breach? In Target's breach over the holidays, for example, did you have all of the customer contact information you needed to individually contact your customers to let them know that they might be affected by the breach?

Answer. Our actions leading up to our public announcement on December 19—and since—have been guided by the principle of serving our guests. We moved quickly to share accurate and actionable information with the public. On December 15, we confirmed that criminals had infiltrated our system, installed malware on our point-of-sale network and potentially stolen guest payment card data. We then began notifying the payment processors and card networks, preparing to publicly notify our guests, and equipping call centers and stores with the necessary information and resources to address our guests' concerns. When we announced the intrusion on December 19, we used multiple forms of communication, including a mass-scale public announcement, e-mail, prominent notices on our website, and social media.

Question 3a. For customers who simply made purchases in your store with payment cards and where you had no other contact information, did you subsequently obtain that information in order to notify these customers individually? If so, how did you do so?

Answer. Target sent e-mails to guests for whom we had e-mail addresses. Target did not seek to obtain personal contact information for those whom which we did not already have personal contact information but we did take steps to notify individuals by following state statutes that allowed for substitute notice. State substitution notice methods include: (1) posting notice on our website; (2) providing notice by e-mail to each relevant guest for whom Target had an e-mail address; and (3) providing notice to national and state media.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. KELLY AYOTTE TO ELLEN RICHEY

Question. As a former Attorney General, I can appreciate how crucial information sharing is by law enforcement to both retail stores and financial institutions. Can you both discuss your relationship with the FBI and the Secret Service (or DHS in general) when it comes to the flow of information that would affect a potential cyber-attack or data breach? Could this relationship be improved? What do you see as the best role for state and local law enforcement in this area?

Answer. Law enforcement plays a critical role in the response to any cyber-attack, and Visa works closely with state and Federal law enforcement agencies to identify, impede, and stop cyber criminals. We feel that broad and regular communication with law enforcement is imperative to an effective cyber-security response policy.

Visa has relationships with a range of law enforcement agencies in the U.S, including the United States Secret Service and the Federal Bureau of Investigation. In addition, we maintain strong contacts with law enforcement in many countries around the world and work cooperatively on fraud and compromise investigations. While Visa engages regularly with law enforcement, we do not share any personal customer or merchant information without a subpoena or its equivalent.

Visa has varied systems for sharing information with industry stakeholders as well as law enforcement, including through our website, data security alerts, client communications, webinars, newsletters and more. Visa has been actively involved in training and education programs with law enforcement and lending our expertise on payment system security issues.

Visa sees a key role for both state and Federal law enforcement to address cyber-attacks, and in particular we regularly work with the United States Secret Service and the FBI offices around the country to address specific situations as they occur. Law enforcement gathers information through criminal investigations that can assist in deconstructing attacks which lend valuable insight into the prevention of future breaches. We also partner with Electronic Crime Task Force entities that have relationships with forensic investigation companies to gather and analyze breach data. These entities are a rich source of information to issuers and payment networks alike. Visa looks forward to continuing to work with a broad spectrum of cybersecurity and data breach specialists, both public and private, to further our efforts to prevent and contain future breaches. We welcome all efforts to strengthen and promote the involvement of state, local, and Federal law enforcement in breach response activities.

○