PROTECTING CONSUMER INFORMATION: CAN DATA BREACHES BE PREVENTED?

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

FEBRUARY 5, 2014

Serial No. 113–115

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
88–611 WASHINGTON : 2015

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

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

RALPH M. HALL, Texas
JOE BARTON, Texas
Chairman Emeritus
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
Vice Chairman
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Missouri
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York
JOHN A. YARMUTH, Kentucky

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

LEE TERRY, Nebraska
Chairman

LEONARD LANCE, New Jersey
Vice Chairman
MARSHA BLACKBURN, Tennessee
GREGG HARPER, Mississippi
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVE B. MCKINLEY, West Virginia
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Missouri
BILLY LONG, Missouri
JOE BARTON, Texas
FRED UPTON, Michigan, *ex officio*

JANICE D. SCHAKOWSKY, Illinois
Ranking Member
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
JOHN A. YARMUTH, Kentucky
JOHN D. DINGELL, Michigan
BOBBY L. RUSH, Illinois
JIM MATHESON, Utah
JOHN BARROW, Georgia
DONNA M. CHRISTENSEN, Virgin Islands
HENRY A. WAXMAN, California, *ex officio*

CONTENTS

[1] Ms. Madigan did not respond to submitted questions for the record.

PROTECTING CONSUMER INFORMATION: CAN DATA BREACHES BE PREVENTED?

WEDNESDAY, FEBRUARY 5, 2014

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 9:30 a.m., in room 2123, Rayburn House Office Building, Hon. Lee Terry (chairman of the subcommittee) presiding.

Present: Representatives Terry, Lance, Blackburn, Harper, Guthrie, Olson, McKinley, Pompeo, Kinzinger, Bilirakis, Johnson, Long, Barton, Upton (ex officio), Schakowsky, Sarbanes, McNerney, Welch, Yarmuth, Dingell, Barrow, Christensen, and Waxman (ex officio).

Staff Present: Charlotte Baker, Press Secretary; Kirby Howard, Legislative Clerk; Nick Magallanes, Policy Coordinator, CMT; Brian McCullough, Senior Professional Staff Member, CMT; Gibb Mullan, Chief Counsel, CMT; Shannon Weinberg Taylor, Counsel, CMT; Michelle Ash, Minority Chief Counsel; and Will Wallace, Minority Professional Staff Member.

OPENING STATEMENT OF HON. LEE TERRY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEBRASKA

Mr. TERRY. So, good morning everyone, and we have an impressive two panels to testify this morning. Our first are government witnesses. I will introduce you each as we go down, but I want to thank all of you for being here. And the way we do it, some of you haven't testified before us before, others have, each side has basically 10 minutes of opening statements, and then we get right into your testimony, so I will begin my opening statement at this time.

And I just want to thank everyone for being here, and today we are turning our focus to an important issue that has affected nearly one-quarter of American consumers, a string of recent data breaches at nationwide retailers, which resulted in the loss of consumer payment card data, personal information for millions of consumers. Millions of consumers are seeking answers to questions about their personal and financial security.

I am grateful to both Target and Neiman Marcus for agreeing to appear before our subcommittee today. It is my hope that they will be able to give the subcommittee as clear a view as possible of what transpired, what was being done to protect consumer information before these breaches, what steps have been taken to miti-

gate the harm to consumers in the wake of these breaches, and what more is being done and can be done to prevent such breaches in the future.

We will also hear from public and private entities who participated in developing security standards, protecting consumer data, and taking enforcement actions against the criminals who perpetrate these crime. Our objective today is not to cast blame or point fingers. It's just like, just like you, don't blame the homeowner whose home is broken into; nevertheless, we must ensure that breaches like these do not become the new norm.

Private sector has worked to try and prevent these crimes to different degrees, including cooperation with government entities. Clearly, there is more that can be done, which is the reason for convening this hearing today. Already, the U.S. accounts for 47 percent of the fraud credit and debit losses worldwide while only accounting for 30 percent of the transactions. We need to be realistic and recognize there is no silver bullet that is going to fix this issue overnight. If we are to seriously address the problem surrounding consumer data security, it will take thoughtful and deliberate actions at all stages of the payment chain.

I don't believe we can solve this problem by codifying detailed technical standards or with overlaying cumbersome mandates. Flexibility, quickness, and nimbleness are all attributes that absolutely are necessary in the cybersecurity, but run contrary to government's abilities. We must encourage the private sector to keep improving on its consensus-driven standards which are built to adapt over time changing threats to data security.

While I have more of a statement, I would like to yield to Mr. Olson the remainder of the time.

[The prepared statement of Mr. Terry follows:]

PREPARED STATEMENT OF HON. LEE TERRY

Welcome to our subcommittee's first hearing of 2014 and the 20th meeting of the 113th Congress.

Today, we are turning our focus to an important issue that has affected nearly one-quarter of American consumers: a string of recent data breaches at nationwide retailers, which resulted in the loss of consumer payment card data and personal information for millions of consumers.

Millions of consumers are seeking answers to questions about their personal and financial security. I'm grateful to both Target and Neiman Marcus for agreeing to appear before our subcommittee today. It is my hope that they will be able to give the subcommittee as clear a view as possible of what transpired, what was being done to protect consumer information before these breaches, what steps have been taken to mitigate the harm to consumers in the wake of these breaches, and what more is being done to prevent such breaches in the future.

We will also hear from public and private sector entities who participate in developing security standards, protecting consumer data, and taking enforcement actions against the criminals who perpetrate these crimes.

Our objective today is not to cast blame or point fingers—just like you don't blame the homeowner whose home is broken into. Nevertheless, we must ensure that breaches like these do not become the "new normal."

The private sector has worked to try and prevent these crimes to different degrees, including cooperation with government entities. Clearly, there is more than can be done, which is the reason for convening today's hearing.

Already, the U.S. accounts for 47 percent of the fraudulent credit and debit losses worldwide, while only accounting for 30 percent of the transactions.

We need to be realistic and recognize there is no "silver bullet" that is going to fix this issue overnight. If we are to seriously address the problems surrounding

consumer data security, it will take thoughtful and deliberate actions at all stages of the payment chain.

I do not believe that we can solve this whole problem by codifying detailed, technical standards or with overly cumbersome mandates. Flexibility, quickness, and nimbleness are all attributes that are absolutely necessary in cyber security but run contrary to government's abilities.

I do believe that information sharing is an area that we can be involved with. I would like to explore with our witnesses today a role for Congress in information sharing and analysis centers (ISACs).

We must encourage the private sector to keep improving on its consensus-driven standards, which are built to adapt over time to changing threats to data security.

There are areas where Congress can take action and lead in a way in protecting consumers and combatting fraud. One such area is a uniform data breach notification standard. Right now, national retailers have to comply with as many as 46 different state and territory notification rules, which can slow down how quickly a business can notify customers of a breach by creating confusion over who must be notified, how they must be notified, and when they must be notified. Consumers need to know quickly if their information is breached so that they protect themselves. I am working on legislation that would foster quicker notification by replacing the multiple—and sometimes conflicting—state notification regimes with a single, uniform federal breach notification regime.

The security of data itself is paramount in this conversation, but as I have said, cumbersome statutory mandates can be ill equipped to deal with evolving threats. Nonetheless, I think this subcommittee would benefit from hearing about how companies are dealing with this issue now, as well as in the future.

I understand that the four largest credit card companies have put a deadline of October 1, 2015, for merchants to adopt point-of-sale portals that accept EMV-enabled cards—the so-called chip-and-PIN. I am interested in hearing about how this technology could benefit consumers, as well as what Congress' role should be with regard to data security in general.

I look forward to hearing from these stakeholders and officials on our panel today and I thank them for appearing.

Mr. OLSON. Thank you, Mr. Chairman, and thank you to our witnesses for coming this morning. As you all know, data breaches are a very serious matter, and you must remember past this issue that regardless of security measures taken to protect data, the bad guys are always trying, always trying to find new ways to grab that data. We have to be right 24 hours a day, 7 days a week, 365 days a year, 366 during leap year, and as you have seen, the bad guys can access data in less time it takes to swipe a credit card.

It is a tough battle, but it is a battle we have to fight, it is a battle we have to win. As we say in Houston, failure is not an option. With that, I yield back, look forward to the discussion. Thank you, Mr. Chairman.

Mr. TERRY. Anybody else? Mr. Lance.

Mr. LANCE. Thank you, Mr. Chairman, and I welcome the very distinguished panel. The issue of data security has been prominent in public debate dating back to at least 2005 when 160,000 records were acquired by hackers in the Choice Point data breach. Over the last 8 years, 660 million records have been made public through various data breaches. Data breaches occur not just in commercial settings, but also hospitals, educational institutions, banks, and insurance companies. There is no doubt that every American could be at risk of a data breach.

Since our last data security hearing in July, we have learned of several additional data breach incidents that occurred in 2013. Data breach incidents at Target, Neiman Marcus and Michael's are recent reminders of the dangers data breaches present to our economy. In our hearing last July, this subcommittee examined the issue of data breach notification; namely, what to do when data se-

curity has been compromised. While that issue is still of paramount concern, equal if not more attention should be given to how to prevent data breaches from occurring in the first place.

Major credit card carriers have created a global data security standard for businesses that accept payment cards called the "payment card industry data security standard." I look forward to examining the best practices for today's economy and for the safety of the American people.

Since the Choice Point data breach in 2005, technology has evolved considerably. While data hackers' tactics have also evolved, so has the potential to provide greater security for Americans at risk of a data breach. I am pleased to have before us today a distinguished panel from the public and private sectors with expertise and personal experience in these issues. I look forward to examining the issues before us today. Thank you, Mr. Chairman.

Mr. TERRY. The ranking member, Jan Schakowsky, is now recognized for her 5 minutes.

OPENING STATEMENT OF HON. JANICE D. SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Ms. SCHAKOWSKY. Thank you, Mr. Chairman. I am really happy that we are having this important hearing on data security. I think it is of great concern to the public, who is probably watching carefully what happens here. As we discussed previously, I hope and expect that we will work together to address these issues.

I thank all of our witnesses for being here, but I would like to take a moment to pay special attention and give special thanks to my friend, Illinois Attorney General Lisa Madigan, who has been at the forefront of this issue since taking office in 2003 leading several efforts at the state level to defend against cyber crime and prosecute those responsible. She is also co-leading an investigation into the Target, Neiman Marcus, and Michael's data breaches, and I look forward, as we all do, I think, to gaining from her perspective about how we can better protect data and inform consumers in the future.

The threat of data breaches isn't new. The Privacy Rights Clearinghouse has identified over 650 million records containing consumers' personal information that have been compromised through thousands of data breaches since 2005; nonetheless, the recent attacks at some of this country's most popular retail stores should give us all renewed motivation to address data security and breach notification.

I think every one of our witnesses today and every member of the subcommittee wants to make sure that we do everything we can to reduce the risk of future massive data breaches. Tens of billions of dollars each year are lost to cyber fraud and identity theft threatening consumer credit and stretching law enforcement resources. The Target breach alone could cost as much as $18 billion, and analysts suggest the company itself could be on the hook for more than $1 billion in costs from fraud. There are also Homeland Security concerns that we, I hope, will hear about today.

It is important to note that there is no foolproof regulatory scheme or encryption program to totally prevent data breaches.

Cyber criminals are incredibly innovative, and as soon as we invent and implement new technologies, they are hard at work looking for new vulnerabilities. But just because we can't absolutely 100 percent guarantee the protection of consumer data doesn't mean that we should not do anything. There is currently no comprehensive Federal law that requires companies to protect consumer or user data, nor is there a federal requirement that companies inform their customers in the event of a data breach. I believe it is critical that the subcommittee move forward with legislation that will ensure that best practices are followed at all retailers and that consumers are informed as soon as possible after cyber theft is discovered. That legislation should be technology neutral, in my view, allowing the FTC and other regulatory agencies to update requirements at the speed of innovation.

In the 111th Congress, I was one of four original co-sponsors of H.R. 2221, the Data Accountability and Trust Act data offered by Mr. Rush. The bill was bipartisan, and Chairman Emeritus Barton was a co-sponsor. The bill had two main provisions. One, an entity holding data containing personal information had to adopt what we said were reasonable and appropriate security measures to protect such data; and two, that same entity had to notify affected consumers in the event of a breach. Seems to me that those basic requirements should be the basis for data security and breach legislation coming out of this committee.

I want to thank our witnesses for appearing today. I look forward to hearing from them about how we can better protect against cyber theft in the future and ensure consumers are informed as soon as possible when those protections fail, and I yield back.

[The prepared statement of Ms. Schakowsky follows:]

PREPARED STATEMENT OF HON. JANICE D. SCHAKOWSKY

Thank you Mr. Chairman for holding this important hearing on data security and breach notification. As we've discussed previously, I hope and expect we will work together to address these issues.

I thank all of our witnesses for being here, but I'd like to take a moment to pay a special thanks to my friend, Illinois Attorney General Lisa Madigan. She has been at the forefront of this issue since taking office in 2003, leading several efforts at the state level to defend against cyber crime and prosecute those responsible. She is also co-leading an investigation into the Target, Neiman Marcus, and Michaels data breaches. I look forward to gaining from her perspective about how we can better protect data and inform consumers in the future.

The threat of data breaches isn't new: the Privacy Rights Clearinghouse has identified over 650 million records containing consumers' personal information that have been compromised through thousands of data breaches since 2005. Nonetheless, the recent attacks at some of this country's most popular retail stores should give us all renewed motivation to address data security and breach notification.

I think every one of our witnesses today and every member of this subcommittee wants to make sure that we do everything we can to reduce the risk of future massive data breaches. Tens of billions of dollars each year are lost to cyber fraud and identity theft, threatening consumer credit and stretching law enforcement resources. The Target breach alone could cost as much as $18 billion, and analysts suggest the company itself could be on the hook for more than $1 billion in costs from fraud.

It is important to note that there is no foolproof regulatory scheme or encryption program to prevent data breaches. Cyber criminals are incredibly innovative, and as soon as we invent and implement new technologies, they are hard at work looking for vulnerabilities.

But just because we can't absolutely guarantee the protection of consumer data doesn't mean we shouldn't try. There is currently no comprehensive federal law that

requires companies to protect consumer or user data. Nor is there a federal requirement that companies inform their customers in the event of a data breach.

I believe it is critical that this subcommittee move forward with legislation that will ensure that best practices are followed at all retailers and that consumers are informed as soon as possible after cyber theft is discovered. That legislation should be technology-neutral, allowing the FTC and other regulatory agencies to update requirements at the speed of innovation.

In the 111th Congress, I was one of 4 original cosponsors of HR 2221, the Data Accountability and Trust Act, offered by Mr. Rush. The bill was bipartisan and counted Chairman Emeritus Barton as a cosponsor. The bill had two main provisions: (1) an entity holding data containing personal information had to adopt reasonable and appropriate security measures to protect such data; and (2) that same entity had to notify affected consumers in the event of a breach. Those basic requirements should be the basis for data security and breach legislation coming out of this committee.

Our constituents can't afford another massive data breach that threatens their credit and the protection of their identity. We owe it to them to take steps to limit the likelihood of data breach and ensure that they are informed when that happens.

I thank our witnesses for appearing today, and I look forward to hearing from them about how we can better protect against cyber theft in the future and ensure that consumers are informed as soon as possible when those protections fail.

Mr. TERRY. Mr. Upton, you are recognized for your 5 minutes, and you control the time.

OPENING STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. UPTON. Well, thank you, Mr. Chairman. The recent data thefts of consumer information at well known companies are a reminder of the challenges that we certainly face today in a digital-connected economy. We are well aware of the benefits to consumers and businesses of instant communication and e-commerce. The rapid evolution of technology allows consumers to purchase goods and services on demand whenever and wherever they want.

Despite the many new conveniences and efficiencies, the unfortunate reality is that technology also facilitates the ability of criminals to commit identity theft or other serious crimes that can potentially injure far more consumers. What originated as paper based fraud or identity theft gathered from a dumpster or mailbox has changed with the times and adapted to the Internet and digital economy.

Today, indeed, most transactions we conduct are either transmitted or stored in a connected environment ensuring almost every citizen has some digital footprint or profile, and that the most sophisticated cyber criminals are successful in infiltrating digital databases, they certainly can gain access to data on millions of individuals. As long as the risk reward payoff is sufficient to attract criminals, the problem will not go away.

Congress recognized the importance of protecting our personal information as the crimes of identity theft and financial fraud became more pervasive in our economy. It is the reason that we enacted laws specifically to address sensitive consumer data that can be used by criminals for identity theft or financial fraud, including the Gramm-Leach-Bliley Act for financial institutions and HIPAA as well for the health care industry. Additionally, we have also empowered the FTC to address data breaches through the use of section 5 of the FTC Act under which they have settled 50 data security cases.

Federal government is not the only layer of protection. A handful of State laws mandates security for the data of their citizens, and the private sector has developed extensive standards through the PCI Security Standards Council, yet breaches, identity theft, financial fraud continue, affecting virtually every sector from the federal government to merchants, banks, universities, and hospitals. We must consider whether the current multi-layer approach to data security, federal, state, and industry self-regulation can be more effective, or whether we need to approach the issue differently.

In short, the title of today's hearing is an appropriate question to ask, "Can data breaches be prevented?" This is the right venue to discuss what businesses can reasonably do to protect data. Equally important, we need to find ways to minimize or eliminate the ability of criminals to commit fraud with data that they acquire. Americans deserve to have the peace of mind that the government, law enforcement officials, and private industry are doing everything necessary to protect the public from future breaches, and I yield the balance of my time to Mrs. Blackburn.

[The prepared statement of Mr. Upton follows:]

PREPARED STATEMENT OF HON. FRED UPTON

The recent data thefts of consumer information at well-known companies are a reminder of the challenges that we face in a digital, connected economy. We are well aware of the benefits to consumers and businesses of instant communication and e-commerce. The rapid evolution of technology allows consumers to purchase goods and services on demand—whenever and wherever they want. Despite the many new conveniences and efficiencies, the unfortunate reality is that technology also facilitates the ability of criminals to commit identity theft or other crimes that can potentially injure far more consumers.

1What originated as paper-based fraud or identity theft gathered from a dumpster or mailbox has changed with the times and adapted to the Internet and the digital economy. Today, most transactions we conduct are either transmitted or stored in a connected environment, ensuring almost every citizen has some digital footprint or profile. If the most sophisticated cybercriminals are successful in infiltrating digital databases, they can gain access to data on millions of individuals. As long as the risk-reward payoff is sufficient to attract criminals, the problem will not go away.

Congress recognized the importance of protecting our personal information as the crimes of identity theft and financial fraud became more pervasive in our economy. It is the reason we enacted laws specifically to address sensitive consumer data that can be used by criminals for identity theft or financial fraud, including the Gramm Leach Bliley Act for financial institutions and HIPAA (Health Information Portability and Accountability Act) for healthcare industry participants. Additionally, we also have empowered the FTC to address data breaches through the use of Section 5 of the FTC Act, under which they have settled 50 data security cases.

The federal government is not the only layer of protection. A handful of state laws mandate security for the data of their citizens, and the private sector has developed extensive standards through the PCI Security Standards Council.

Yet breaches, identity theft, and financial fraud continue, affecting every sector from the federal government to merchants, banks, universities and hospitals. We must consider whether the current multi-layer approach to data security—federal, state, and industry self-regulation—can be more effective, or whether we need to approach the issue differently.

In short, the title of today's hearing is an appropriate question to ask: "Can Data Breaches be Prevented?" This is the right venue to discuss what businesses can reasonably do to protect data. Equally important, we need to find ways to minimize or eliminate the ability of criminals to commit fraud with data they acquire. Americans deserve to have the peace of mind that the government, law enforcement officials, and private industry are doing everything necessary to protect the public from future breaches.

Mrs. BLACKBURN. I thank the chairman, and I want to welcome each of you. We are pleased to have you here. Privacy data security is something that we are hearing about more and more from our constituents. I sum it up by saying my constituents want to know who owns the virtual you, which is you in your presence online. Who has the rights to that? And I hope that from listening to you-all and talking with you today, we can gather some information to add to the work that we have been doing in our bipartisan privacy data security working group here at the committee.

What our constituents want to do is figure out how to build out this toolbox that will allow them to protect themselves online. They want to know what you are doing to provide the assurance of data security, what are those protocols? They want to know what the process will be, a kind of a standard business process, for data breach notification. What are the expectations? And then they want, both the private sector and government, to meet and fulfill those expectations.

So, you have experience, some lessons learned, you have made some mistakes, all of you, you are learning from those mistakes, and we are looking at how we take the rules that are on the books in the physical space, and apply that to the virtual space and encourage commerce and the interaction, transaction, and movement of data and commerce. I yield back the balance of the time.

Mr. TERRY. Mr. Johnson, you are recognized for 10 seconds.

Mr. JOHNSON. Well, thanks. As a 30-year IT professional myself before coming to Congress, including a stint as the director of the CIO staff for U.S. Special Operations Command, I can tell you I understand the complexities of data security and how complex it is. I am really looking forward to hearing from you folks today on what we can do to position both our commercial sector and our public sector to handle this problem.

Mr. TERRY. Thank you. That concludes our time, but before I officially recognize him, Mr. Waxman, ranking member of the full committee, had made a surprise announcement and stunned all of us that he is going to conclude his time with Congress at the end of this session, and I just want to thank him for his 40 years of service to the United States Congress, to the people of California, and the United States, and job well done.

We may not agree on everything, but you are passionate, you are zealous, and you are very involved, and you command respect from everybody, Henry. Thank you for your service.

Mr. WAXMAN. Thank you, Mr. Chairman.

Mr. TERRY. And you are recognized for 5 minutes.

OPENING STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. WAXMAN. Thank you for your kind words and for holding this hearing today. I think this may be the first of a series of troubling cyber attacks on prominent retailers that are going to tell us today about their experience, and we want to evaluate how businesses and government can better protect the security of consumers' personal information.

Late last year, Target, Neiman Marcus, and reportedly Michael's all experienced breaches in which criminal intruders stole consumers' payment card information leaving them at risk for fraudulent charges. The Target breach, which involves not only payment card data, but also marketing data that could be used in phishing attacks is now reported to affect between 70 million and 110 million people, roughly one-third of the adult U.S. population. Reports indicated that similar attacks have likely affected many other retailers as well. Just last week, White Lodging, a major hotel operator, announced that he was investigating a potential breach affecting thousands of guests who stayed at hotels under various brand names, including Hilton, Marriott, Sheraton, and Westin. Given these constant security threats, I hope that today's hearing will provide us with the facts necessary to chart a path forward where consumers can be more confident that companies will keep their data safe.

The unprecedented scope and scale of these breaches is alarming. It affects the confidence of consumers who rely on retailers, banks, and payment card processors and networks to safeguard their personal information, including their credit card and debit card information. Millions of Americans have had to contend with fraudulent charges on their financial statements, identity theft schemes in which criminals open phony accounts in their names, and the fear and uncertainty about how criminals may use their information next.

There are many unanswered questions about these recent attacks, including how they were carried out, and of course, who was responsible. These breaches also raise important questions about how well the industry polices itself, whether these companies responded to early warnings and whether they notified consumers in a timely manner. We also need to understand the appropriate Federal role in both data security and breach notification. Nearly all U.S. States and territories now have laws that require notice for their own residents when a data breach occurs.

The effectiveness of these laws vary greatly, but several are quite strong, ensuring that consumers receive prompt, adequate, and clear notification when their personal information is breached, and providing them with resources to protect their financial wellbeing. It could be a model for a minimum Federal requirement.

After the fact, breach notification is only half of what is needed. The private sector must also take stronger steps to safeguard personal information. There could be a Federal rule in ensuring they are proactive. There will always be bad actors who will try to compromise large databases and obtain sensitive information that can be leveraged for financial gain. We need to have effective law enforcement to stop them. We also need to make sure companies are doing enough to prevent breaches because consumers are paying the price. Protecting consumer data needs to be priority number 1.

I look forward to the witnesses' testimony and to our discussion today of this important topic. I thank the witnesses for being here. I want to apologize in advance because there is another subcommittee that is meeting simultaneously with this one, and I have to be at that subcommittee as well. But looking forward to your testimony. In the short time I have left, is anybody on the majority

wish to take the 47, -6, -5, -4 seconds noted. If not, Mr. Chairman, I yield back.

Mr. TERRY. You said majority. Are you talking——

Mr. WAXMAN. Oh, did I say majority? I am always looking to the future, Mr. Chairman, and I thank you for your kind words, and I, of course, I am going to be here till December so we will all be able to work together some more. Thank you.

Mr. TERRY. Very good. Thank you, Henry.

Now, time to introduce our first panel. Edith Ramirez is the chairwoman of the Federal Trade Commission, thank you for your second appearance before this committee; Lisa Madigan, Attorney General for the State of Illinois, thank you for coming; William Noonan, deputy special agent in charge, Criminal Investigation Division, Cyber Operations, United States Secret Service, and I said it all in one breath. Mr. Noonan, thank you for your appearance here today; Lawrence Zelvin, director, National Cybersecurity and Communications Integration Center, Department of Homeland Security. We always go from my left to right, so we will start with Chairman Ramirez. You are now recognized for your 5 minutes.

STATEMENTS OF HON. EDITH RAMIREZ, CHAIRWOMAN, FEDERAL TRADE COMMISSION; HON. LISA MADIGAN, ATTORNEY GENERAL, STATE OF ILLINOIS; WILLIAM NOONAN, DEPUTY SPECIAL AGENT IN CHARGE, CRIMINAL INVESTIGATIONS DIVISION, CYBER OPERATIONS, UNITED STATES SECRET SERVICE; AND LAWRENCE ZELVIN, DIRECTOR OF THE NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER, DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF HON. EDITH RAMIREZ

Ms. RAMIREZ. Thank you. Chairman Terry, Ranking Member Schakowsky, and members of the committee, thank you for the opportunity to appear before you to discuss the Federal Trade Commission's data security enforcement program. We live in an increasingly connected world in which vast amounts of consumer data is collected. As recent breaches of Target and other retailers remind us, this data is susceptible to compromise by those who seek to exploit security vulnerabilities. This takes place against the background of the threat of identity theft, which has been the FTC's top consumer complaint for the last 13 years. According to estimates of the Bureau of Justice statistics, in 2012, this crime affected a staggering 7 percent of all people in the United States age 16 and older.

The Commission is here today to reiterate its bipartisan and unanimous call for Federal data security legislation. Never has the need for such legislation been greater. With reports of data breaches on the rise, Congress needs to act. We support legislation that would strengthen existing data security standards and require companies, in appropriate circumstances, to notify consumers when there is a breach. Legislation should give the FTC authority to seek civil penalties where warranted to help ensure that FTC actions have an appropriate deterrent effect.

It should also provide rulemaking authority under the Administrative Procedure Act and jurisdiction over nonprofits, which have

been the source of a large number of breaches. Such provisions would create a strong consistent standard and enable the FTC to protect consumers more effectively. Using its existing authority, the FTC has devoted substantial resources to encourage companies to make data security a priority.

The FTC has brought 50 civil actions against companies that we alleged put consumer data at risk. We have brought these cases under our authority to combat effective and unfair commercial practices as well as more targeted laws such as the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act. 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. Significantly, a number of FTC enforcement actions have involved large breaches of payment card information. For example, in 2008, the FTC settled allegations that security deficiencies of retailer TJX permitted hackers to obtain information about tens of millions of credit and debit cards. To resolve these allegations, TJX agreed to institute a comprehensive security program and to submit to a series of security audits. At the same time, the Justice Department successfully prosecuted a hacker behind the TJX and other breaches. As the TJX case illustrates well, the FTC and criminal authorities share complementary goals.

FTC actions help ensure, on the front end, that businesses do not put their customers' data at unnecessary risk while criminal enforcers help ensure that cyber criminals are caught and punished. The dual approach to data security leverages government resources and best serves the interest of consumers, and to that end, the FTC and criminal enforcement agencies have worked together to coordinate all respective data security investigations.

The FTC appreciates the work of our fellow law enforcement agencies at the Federal and State level. In addition to the Commission's enforcement work, the FTC offers guidance to consumers and businesses. For those consumers affected by recent breaches, the FTC has posted information online about steps they should take to protect themselves. These materials are in addition to the large stable of other FTC resources we have for ID theft victims, including an ID theft hotline. We also engage in extensive policy initiatives on privacy and data security issues.

For example, we recently conducted workshops on mobile security and emerging forms of ID theft, such as child ID theft and senior ID theft.

In closing, I want to thank the Committee for holding this hearing and for the opportunity to provide the Commission's views. Data security is among the Commission's highest priorities, and we look forward to working with Congress on this critical issue. Thank you.

Mr. TERRY. Thank you, Chairman.

[The prepared statement of Ms. Ramirez follows:]

PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Protecting Consumer Information: Can Data Breaches Be Prevented?

Before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

February 5, 2014

I. INTRODUCTION

Chairman Terry, Ranking Member Schakowsky, and members of the Subcommittee, 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.

We live in an increasingly connected world, and information is the new currency. Businesses in this data-driven economy are collecting more personal information about consumers than ever before, and storing and transmitting across their own systems as well as the Internet. But, as recent publicly announced data breaches remind us,[2] these vast systems of data are susceptible to being compromised. Hackers and others seek to exploit vulnerabilities, obtain unauthorized access to consumers' sensitive information, and potentially misuse it in ways that can cause serious harms to consumers as well as businesses.

All of this takes place against the background of the threat of identity theft, a pernicious crime that harms both consumers and financial institutions. 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.[3]

As the nation's leading privacy enforcement agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector and has settled 50 law

---

[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* 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 (discussing Michaels Stores' announcement of potential security breach involving payment card information).

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

enforcement actions against businesses that we alleged failed to protect consumers' personal information appropriately. 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 and other harm, along with a potential loss of consumer confidence in particular business sectors or entities, payment methods, or types of transactions. Accordingly, the Commission has undertaken substantial efforts for over a decade to promote data security in the private sector through civil law enforcement, education, policy initiatives, and recommendations to Congress to enact legislation in this area. The FTC has also worked with the Department of Justice and criminal investigative agencies, as well as state Attorneys General, to coordinate efforts and leverage government resources more effectively.

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 needs to act. This testimony provides an overview of the Commission's efforts and restates the Commission's support for data security legislation.

II. THE COMMISSION'S DATA SECURITY PROGRAM

A. Law Enforcement

To promote data security, the Commission enforces several statutes and rules that impose obligations upon businesses that collect and maintain 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.[4] The Fair Credit

[4] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).

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,[5] and imposes safe disposal obligations on entities that maintain consumer report information.[6] The Children's Online Privacy Protection Act ("COPPA") requires reasonable security for children's information collected online.[7]

In addition, the Commission enforces the proscription against unfair or deceptive acts or practices in Section 5 of the FTC Act.[8] If a company makes materially misleading statements or omissions about a matter, including data security, and such statements or omissions are likely to mislead reasonable consumers, they can be found to be deceptive in violation of Section 5.[9] Using its deception authority, the Commission has settled more than 30 matters challenging companies' express and implied claims that they provide reasonable security for consumers' personal data when, the Commission charged, the companies failed to employ available, cost-effective security measures to minimize or reduce data risks.

Further, if a company's 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, those practices can be found to be unfair and violate Section 5.[10] Congress expressly codified these criteria in Section 5.[11] The

---

[5] 15 U.S.C. § 1681e.

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

[7] 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312 ("COPPA Rule").

[8] 15 U.S.C. § 45(a).

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

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

[11] 15 U.S.C. § 5(n).

Commission has settled over 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice.[12]

In the data security context, the FTC conducts its investigations with a focus on 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 examines such factors as whether the risks at issue were well known or reasonably foreseeable, the costs and benefits of implementing various protections, and the tools that are currently available and used in the marketplace. This same reasonableness requirement is the basis for sectoral laws that have data security requirements, including the GLB Act and the FCRA.

Since 2001, the Commission has used its authority under these laws to settle 50 cases against businesses that it charged with failing to provide reasonable and appropriate protections for consumers' personal information.[13] The practices at issue were not merely isolated mistakes. In each of these cases, the Commission examined a company's practices as a whole and challenged alleged data security failures that were multiple and systemic. And through these settlements, the Commission has made clear that it does not require perfect security; that reasonable and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law.

---

[12] Some of the Commission's data security settlements allege both deception and unfairness.

[13] *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.

In its most recent case, the FTC settled allegations that GMR Transcription Services, Inc., and its owners violated Section 5 of the FTC Act.[14] According to the complaint, GMR provides audio file transcription services for their clients, which include health care providers, and relies on service providers and independent typists to perform this work. GMR exchanged 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 resolving the case 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 its first data security settlement concerning the "Internet of Things" – *i.e.*, Internet-connected refrigerators, thermostats, cars, and many other products and devices which can communicate with each other and/or consumers. The TRENDnet settlement involved a video camera designed to allow consumers to monitor their homes remotely.[15] The complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring, and claimed in numerous product descriptions that they were "secure." However, the cameras had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet

---

[14] *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.

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

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.

Finally, the FTC has also 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.[16] For example, the Commission alleged that TJX's failure to use reasonable and appropriate security measures resulted in a hacker obtaining 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.[17] Banks also claimed that tens of millions of dollars in fraudulent charges were made, and cancelled and reissued millions of cards. Meanwhile, criminal law enforcement authorities investigated and prosecuted the hackers involved in this and other data breaches.[18] As this matter illustrates, the goals of FTC and federal criminal agencies are complementary: FTC actions send a message that businesses need to protect their customers' data on the front end, and actions by criminal agencies send a message to identity thieves that their efforts to victimize consumers will be punished.

---

[16] *See, e.g., Dave & Busters, Inc.*, No. C-4291 (F.T.C. May 20, 2010), *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), *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), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2005/09/bjs-wholesale-club-inc-matter.

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

[18] *See, e.g.*, Kim Zetter, *TJX Hacker Gets 20 Years in Prison*, Wired, Mar. 25, 2010, *available at* http://www.wired.com/threatlevel/2010/03/tjx-sentencing/.

B. Policy Initiatives

The Commission also undertakes policy initiatives to promote privacy and data security, including by hosting workshops on emerging business practices and technologies affecting consumer data. This testimony describes two such recent initiatives that addressed information security issues.

In November, the FTC held a workshop on the Internet of Things.[19] 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, health and fitness devices, and cars.

Last June, the Commission hosted a public forum on mobile security issues, including potential threats to U.S. consumers and possible solutions to them.[20] 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.

The Commission has also hosted programs on emerging forms of identity theft, such as child identity theft[21] and senior identity theft.[22] In these programs, the Commission discussed

---

[19] 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/.

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

[21] 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.

unique challenges facing children and seniors, and worked with stakeholders to develop outreach messages and plans for these two communities. Since the workshops took place, the Commission has continued to engage in such tailored outreach.

C. Consumer Education and Business Guidance

The Commission also promotes 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.[23] OnGuard Online and its Spanish-language counterpart, Alerta en Línea,[24] average more than 2.2 million unique visits per year.

As directed by Congress, the Commission maintains the nation's main repository of identity theft complaints, housed within our Consumer Sentinel consumer complaint database, and provides centralized resources for victims of identity theft.[25] Identity theft has been the top consumer complaint to the FTC for 13 consecutive years, and tax identity theft – which often begins by thieves obtaining Social Security numbers and other personal information from consumers in order to obtain their tax refund – has been an increasing share of the Commission's identity theft complaints.[26] To address these concerns, Commission staff have worked with members of Congress to host numerous town hall meetings on identity theft in order to educate their constituents. And, just last month, the FTC hosted 16 events across the country, along with

---

[22] FTC Workshop, *Senior Identity Theft: A Problem in This Day and Age* (May 7, 2013), *available at* http://www.ftc.gov/news-events/events-calendar/2013/05/senior-identity-theft-problem-day-and-age.

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

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

[25] 18 U.S.C. § 1028 note.

[26] In 2012, tax identity theft accounted for more than 43% of the identity theft complaints, making it the largest category of identity theft complaints by a substantial margin. *See* Press Release, *FTC Releases Top 10 Complaint Categories for 2012* (Feb. 26, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/02/ftc-releases-top-10-complaint-categories-2012.

a series of national webinars and Twitter chats as part of Tax Identity Theft Awareness Week.[27] The events were designed to raise awareness about tax identity theft and provide consumers with tips on how to protect themselves, and what to do if they become victims. 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.[28]

The Commission directs its outreach to businesses as well. The FTC widely disseminates a business guide on data security, [29] along with an online tutorial based on the guide.[30] These resources are designed to provide diverse businesses – and especially small businesses – with practical, concrete advice as they develop data security programs and plans for their companies. The Commission has also released articles directed towards a non-legal audience regarding basic data security issues for businesses.[31] 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.[32] The FTC also creates

---

[27] Press Release, *FTC's Tax Identity Theft Awareness Week Offers Consumers Advice, Guidance* (Jan. 10, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/01/ftcs-tax-identity-theft-awareness-week-offers-consumers-advice.

[28] *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.

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

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

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

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

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[33] and how to properly secure and dispose of information on digital copiers.[34]

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.[35] 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

---

[33] *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.

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

[35] *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/110615datasecurityhouse.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/081021taskforcereport.pdf.

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, rulemaking authority under the Administrative Procedure Act, and jurisdiction over non-profits. 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.[36] 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[37] would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it.[38] Finally, rulemaking authority under the Administrative Procedure Act would enable the FTC to respond to changes in technology in implementing the legislation.

VI. 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 Congress on this critical issue.

---

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

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

[38] 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.

Mr. TERRY. Now, the gentlelady from Illinois, Ms. Madigan, you are now recognized for 5 minutes.

STATEMENT OF HON. LISA MADIGAN

Ms. MADIGAN. Thank you, Chairman Terry, Ranking Member Schakowsky, and members of the subcommittee, I appreciate having an opportunity to testify on this important issue. Addressing data breaches and preventing them is critical to our financial security and our economy. Over the past decade, we have faced an epidemic of data breaches that has affected almost every American and has inflicted billions of dollars of damage to our economy. Many have become accustomed to their occurrence, but the recent Target breach served as a wake-up call that government and the private sector need to take serious meaningful actions to curb this growing problem.

To assist the subcommittee, I will explain the impact data breaches have on consumers, the role the States play in responding to breaches, the data security lapses we have seen in the private sector, and the steps that private sector and government can take to prevent future breaches.

Since 2005 there have been over 4,000 data breaches nationally and over 733 million records compromised. The amount of money lost because of identity theft is also sobering. In 2012, it was $21 billion. And over the last year alone, the number of complaints my office has received on data breaches has jumped more than 1,000 percent. When these breaches occur, consumers are harmed primarily two ways: First, they are exposed to the likelihood of unauthorized charges on their existing accounts, and second, they are much more likely to become victims of more costly identity theft. Consumers affected by breaches must constantly monitor their financial accounts for unauthorized charges, and when consumers discovery them, clean up requires notifying their credit and debit card issuers, closing accounts, canceling cards and waiting for new cards to arrive, and for consumers with automatic bill pay, alerting companies about the new account numbers to prevent late fees, and those are the easy situations.

Victims of identity theft can spend months reporting instances of fraud to creditors and reporting bureaus to restore their credit. During this time, these victims are often prevented from fully participating in our economy. Identity theft takes a variety of forms and while it most commonly affects consumers' financial account, identity thieves also use consumers' information to open utility accounts and obtain medical treatment and prescription drugs. All of these things can happen simply because the consumers share their sensitive data in the usual course with a business, a medical provider, or the government.

The States have been inundated with consumers who need help understanding and recovering from breaches and identity theft damage. Because of this, I created an identity theft unit and hotline back in 2006. Since then, we have received more than 40,000 requests for assistance and have helped remove over $26 million worth of fraudulent charges for Illinois residents. In addition to this direct consumer assistance, my office also conducts investigations of data breaches.

To confirm that companies complied with State laws by notifying consumers of breaches within a reasonable time, and to ensure that companies suffering breaches took reasonable steps to protect their consumer sensitive data from disclosure. My office, along with the Connecticut AG's office, is currently leading multi-State investigations into breaches that affected millions of Target and Neiman Marcus and Michael's customers. During private breach investigations, we have instances where companies failed to take basic steps to protect consumer data. So the notion that companies are already doing everything they can to prevent breaches is false.

We have found repeated instances where breaches occurred because companies allowed consumer data to be maintained unencrypted, failed to install security patches for known software vulnerabilities, and retained data for longer than necessary. The recent breaches have also led to discussions about security technology that was available but not deployed for reasons that allegedly ranged from high cost and increased checkout times to disputes between banks and retailers.

Frankly, it is negligent that the United States is behind the rest of the world when it comes to the security of our payment networks, and it is the main reason that U.S. consumers' information is targeted by criminals. It is past time for the private sector to take data security seriously. Consumers are rapidly losing confidence in companies' ability to safeguard their personal information. Based upon our experiences at the State level, I recommend the Congress take the following actions. First, pass data security and breach notification legislation that does not preempt State law. Second, Congress should also recognize that the Federal Government should assist the private sector in the same manner it already does in other critical areas.

Congress should give an agency the responsibility and authority to investigate large sophisticated data breaches in a manner similar to NTSB investigations of aviation accidents.

Finally, please remember that States have been on the front lines of this battle for a decade. Illinois residents appreciate the important role my office plays, and they are not asking for our State law to be weakened by preemption, but they are panicked and they are angered the companies are not doing more to protect their personal and financial information and prevent these breaches from occurring in the first place. I am happy to answer any questions you have. Thank you.

Mr. TERRY. Thank you, General Madigan.

[The prepared statement of Ms. Madigan follows:]

Prepared Statement
Illinois Attorney General Lisa Madigan
"Protecting Consumer Information: Can Data Breaches Be Prevented?"

Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy & Commerce
United States House of Representatives

February 5, 2014

I. INTRODUCTION

Chairman Terry, members of the Subcommittee, thank you for inviting me to testify today about this important issue. Addressing data breaches and preventing them is critical to our financial security and our economy. Over the past decade, we have faced an epidemic of data breaches that has affected almost every American and has inflicted billions of dollars of damage to our economy.

The most frustrating aspect of this problem is that data breaches are not new. No one is surprised to hear the latest data breach reported in the news. We have become too accustomed to their occurrence, and it is time the government and the private sector take serious, meaningful actions to curb this growing problem. As we become more dependent on technology in our everyday lives, breaches will increasingly affect more consumers and, in the process, do more damage.

To assist the Subcommittee, I will explain:

- the impact data breaches have on consumers;
- the role the states play in responding to breaches;
- the data security lapses we have seen in private companies; and
- the steps the private sector and the government can take to prevent future breaches.

II. IMPACT ON CONSUMERS

Since 2005, there have been over 4,000 data breaches nationally and over 733 million records compromised.[1] In the last year alone, the number of complaints my office has received on data breaches has jumped more than 1,000%.[2] Since 2006, identity theft has been the highest or second highest source of complaints to my office every year, totaling 31,100 complaints.[3] When data breaches occur, consumers are harmed primarily for two reasons:

- they face the likelihood of unauthorized charges on their existing accounts; and
- they are much more likely to become victims of identity theft.

A. Fraud on Existing Accounts

When financial information is compromised, consumers must constantly monitor their financial accounts for any unauthorized charges. Once a consumer does discover unauthorized charges, cleanup requires:

- notifying their credit and debit card issuers of the compromised cards;
- closing accounts, canceling cards, and waiting for new cards to arrive; and
- for consumers with automatic bill pay, alerting companies about the new account numbers to prevent late fees.

---

[1] Figure includes publicly reported data breaches between 2005 and 2014 compiled by Privacy Rights Clearinghouse (663,182,386 as of February 3, 2014) in addition to the publicly reported 70 million records compromised in the 2013 Target Data Breach. *See* Privacy Rights Clearinghouse, Chronology of Data Breaches, *available at* http://www.privacyrights.org/data-breach/new; Press Release, Target Corp., "Target provides Update on Data Breach and Financial Performance," *available at* http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance.

[2] In 2012 the Illinois Attorney General's office received 34 complaints regarding data breaches, compared to 605 in 2013.

[3] *See* Press Release, Office of Illinois Attorney General Lisa Madigan, "Top Ten Consumer Complaints" for 2006, 2007, 2008, 2009, 2010, 2011, and 2012, *available at* http://www.illinoisattorneygeneral.gov/consumers/index.html.

These issues are more than mere inconveniences. Consumers and banks can also easily miss unauthorized charges on accounts. And when that happens, the consumer will be responsible for the fraud.

Everyday my office contends with the enormous amount of time, effort, and stress consumers face when they attempt to sort out the impact of data breaches involving their existing financial accounts.

B. Identity Theft

The amount of money consumers lose because of identity theft is sobering. In 2012 alone, $21 billion was lost to identity theft.[4] The fraud takes a variety of forms. Identity theft most commonly affects consumers' financial accounts. But identity thieves also:

- open fake utility accounts;
- obtain prescription drugs and medical treatments using others' identities;
- receive government benefits using compromised consumer data; and
- target children because of their clean credit history.

Since 2010, my office has assisted nearly 350 minors who have been victims of identity theft.[5] We have helped shut down hundreds of fraudulent accounts, which were opened using the identities of children.

Victims of identity theft can spend months contacting banks, credit card companies, credit reporting agencies, public utility companies, and the police to report instances of fraud and to restore their credit. These victims can also be prevented from fully participating in our

[4] Javelin Strategy & Research, *How Consumers can Protect Against Identity Fraudsters in 2013*, 4 (Feb. 2013). This statistic includes all types of identity theft, not just identity theft related to data breaches.

[5] Social Security Number Protection Task Force, *Report to Governor Pat Quinn, Attorney General Lisa Madigan, Secretary of State Jesse White, and Illinois General Assembly*, 6 (Dec. 31, 2013).

economy, meaning their entire lives can be put on hold. An identity theft can prevent a consumer from purchasing a home or finding a place to rent. All this can happen because a consumer shared their sensitive data with a business, a hospital, or the government.

III. Role of the States

The states have seen firsthand how damaging this is for consumers. In response, my office created a dedicated Identity Theft Unit and Hotline in 2006.[6] Since then, we have received more than 40,000 requests for assistance and have helped thousands of Illinois residents. The unit and hotline are staffed with experts who walk consumers through the lengthy and complicated process they face when reporting fraud and restoring their credit. We have also developed a fifty-six page, comprehensive Identity Theft Resource Guide for Illinois residents to use when facing identity theft.[7]

The states began focusing in earnest on data breaches in 2005 when ChoicePoint, a very large data broker, experienced a significant data breach that harmed thousands of consumers.[8] In response, Illinois passed a data breach law to ensure companies notify consumers when their

[6] Press Release, Office of Illinois Attorney General Lisa Madigan, "Madigan Announces Activation of ID Theft Hotline; Help Line is First of Its Kind in the Nation" (Feb. 7, 2006).

[7] Identity Theft Resource Guide, *available at* http://www.illinoisattorneygeneral.gov/consumers/Identity_Theft_Resource_Guide.pdf.

[8] Press Release, Office of Illinois Attorney General Lisa Madigan, "Attorney General Madigan Reaches Agreement with ChoicePoint" (May 31, 2007).

sensitive information is compromised.[9] Since then, nearly every other state has passed a law requiring companies to notify consumers of data breaches that compromise sensitive data.[10]

My office also leads the National Association of Attorneys General (NAAG) Privacy Working Group, which consists of more than forty states. We convene regularly to discuss and investigate privacy issues, including data breaches that affect consumers in multiple states. With respect to the recent data breaches, my office, along with the Connecticut Attorney General's office, is leading multi-state investigations into the breaches that have impacted millions of customers of Target, Neiman Marcus, and Michaels.[11]

While I cannot comment on the specifics of an ongoing investigation, I can explain why we conduct these investigations in the first place:

---

[9] Illinois Personal Information Protection Act (PIPA), 815 Ill. Comp. Stat. 530/1 et. seq. (2006). PIPA requires notification to a consumer when an unauthorized acquisition of computerized data compromises the security, confidentiality, or integrity of personal information maintained by the data collector. Personal information means an individual's first name or first initial and last name, in combination with any one or more of the following data elements, when either the name or the data element are not encrypted or redacted: social security number, driver's license number or State identification card number, account number or credit card number, or account number or credit card number in combination with any required security code, access code, or password. Notice to consumers must occur in the most expedient time possible and without unreasonable delay.

[10] Alaska Stat. §45.48.010 et seq.; Ariz. Rev. Stat. §44-7501; Ark. Code §4-110-101 et seq.; Cal. Civ. Code §§1798.29, 1789.80 et. seq.; Colo. Rev. Stat. §6-1-716; Conn. Gen Stat. 36a-701(b); Del. Code tit. 6, §12B-101 et seq.; Fla. Stat. §817.5681; Ga. Code §§10-1-910, -911, -912; § 46-5-214; Haw. Rev. Stat. §487N-1 et. seq.; Idaho Stat. §§28-51-104 to -107; 815 ILCS 530/1 to 530/25; Ind. Code §§24-4.9 et seq., 4-1-11 et seq.; Iowa Code §715C.1, 715C.2; Kan. Stat. 50-7a01 et. seq.; La. Rev. Stat. §51:3071 et seq.; Me. Rev. Stat. tit. 10 §§1347 et seq.; Md. Code, Com. Law §14-3501 et seq.; Mass. Gen. Laws §93H-1 et seq.; Mich. Comp. Laws §§ 445.63, 445.72; Minn. Stat. §§325E.61, 325E.64; Miss. Code § 75-24-29; Mo. Rev. Stat. §407.1500; Mont. Code §§30-14-1704, 2-6-504; Neb. Rev. Stat. §§87-801, -802, -803, -804, -805, -806, -807; Nev. Rev. Stat. 603A.010 et seq.; N.H. Rev. Stat. §§359-C:19, -C:20, -C:21; N.J. Stat. 56:8-163; N.Y. Gen. Bus. Law §899-aa; N.C. Gen. Stat §75-65; N.D. Cent. Code §51-30-01 et seq.; Ohio Rev. Code §§1347.12, 1349.19, 1349.191, 1349.192; Okla. Stat. §74-3113.1, §24-161 to -166; Oregon Rev. Stat. §646A.600 et seq.; 73 Pa. Stat. §2303; R.I. Gen. Laws §11-49.2-1 et seq.; S.C. Code §39-1-90; Tenn. Code §47-18-2107; Tex. Bus. & Com. Code §521.002, 521.053; Utah Code §§13-44-101, -102, -201, -202, -310; Vt. Stat. tit. 9 §2430, 2435; Va. Code §18.2-186.6, §32.1-127.1:05; Wash. Rev. Code §19.255.010, 42.56.590; W.V. Code §§46A-2A-101 et seq.; Wis. Stat. §134.98 et seq.; Wyo. Stat. §40-12-501 to -502; D.C. Code §28- 3851 et seq.; Guam 9 GCA § 48-10 et. seq.; 10 Laws of Puerto Rico §4051 et. seq.; V.I. Code §2208. *See* State Security Breach Notification Laws, Nat'l Conference Of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last updated Jan 21, 2014).

[11] Bloomberg, "Connecticut Attorney General Probing Neiman Marcus Breach," Jan. 14, 2014, *available at* http://www.bloomberg.com/news/2014-01-13/connecticut-attorney-general-probing-neiman-marcus-breach.html.

- to confirm that companies notified their customers within a reasonable timeframe and satisfied the requirements of Illinois law and other states; and
- to ensure that companies suffering breaches took reasonable steps to protect their customers' sensitive data from disclosure.

IV. Weaknesses in Security Systems

During past investigations, we have repeatedly found instances where companies failed to take basic steps to protect consumer data. The notion that companies are already doing everything they can to prevent data breaches is false. We have found instances where companies:

- failed to encrypt consumer data;
- failed to install updated security patches for software; and
- needlessly stored sensitive consumer data that was not necessary for any business purpose

The recent breaches have also led to discussions about security technology that was available, but not deployed, allegedly because of the cost. It is embarrassing that our country is behind most of the world when it comes to the security of our payment networks. It is past time for the private sector to take data security seriously.

V. Next Steps for the Private Sector and the Government

Based upon our experiences at the state level, I recommend that Congress take the following actions.

First, pass data security legislation that does not preempt state law and requires companies to:

- adopt reasonable data security practices;

- only collect information from consumers that is necessary for legitimate business needs;
- delete consumer data as soon as it is no longer needed; and
- notify consumers in a timely manner when a data breach occurs.

Second, Congress should also recognize that the federal government should assist the private sector in the same manner it already assists in other critical areas. For that reason, Congress should give an agency the responsibility and authority to investigate large, sophisticated data breaches in a similar manner that the NTSB conducts investigations of aviation accidents.

Finally, please remember that the states have been on the front lines of this battle for a decade. Illinois residents understand the important role my office plays and they are not asking for our state law to be preempted. But they are asking why companies are not doing more to protect their personal and financial information and prevent these breaches from occurring in the first place.

I am happy to answer any questions you have.

Thank you.

Mr. TERRY. And now, Mr. Noonan, you are recognized for your 5 minutes.

STATEMENT OF WILLIAM NOONAN

Mr. NOONAN. Good morning, Chairman Terry, Ranking Member Schakowsky, and distinguished members of the subcommittee. Thank you for the opportunity to testify on behalf of the Department of Homeland Security regarding the ongoing trend of criminal exploiting cyberspace to obtain sensitive, financial, and identity information as part of a complex criminal scheme to defraud our Nation's payment systems. Our modern financial system depends heavily on information technology forconvenience and efficiency.

Accordingly, criminals motivated by greed have adapted their methods and are increasingly using cyberspace to exploit our Nation's financial payment systems to engage in fraud and other illicit activities. The widely reported data breaches of Target and Neiman Marcus are just recent examples of this trend. The Secret Service is investigating these recent data breaches, and we are confident that we will bring the criminals responsible to justice.

However, data breaches like these recent events are part of a long trend. In 1984, Congress recognized the risk posed by increasing use of information technology and established 18 USC sections 1029 and 1030 through the Comprehensive Crime Control Act. These statutes define access device fraud and misuse of computers as Federal crimes, and explicitly assign the Secret Service authority to investigate these crimes.

In support of the Department of Homeland Security's mission to safeguard cyberspace, the Secret Service investigates cyber crime through efforts of our highly trained special agents in the work of our growing network of 33 electronic crimes task forces which Congress assigned the mission of preventing, detecting, and investigating various forms of electronic crimes.

As a result of our cyber crime investigations, over the past 4 years, the Secret Service has nearly arrested 5,000 cyber criminals. In total, these criminals were responsible for over a billion dollars in fraud losses, and we estimate our investigations prevented over a $11 billion in fraud losses. The data breaches, like the recent reported occurrences, are just one part of a complex criminal scheme executed by organized cyber crime. These criminal groups are using increasingly sophisticated technology to conduct a criminal conspiracy consisting of five parts.

One, gaining unauthorized access to computer systems carrying valuable protected information; two, deploying specialized malware to capture and exfiltrate the data; three, distributing or selling the sensitive data to their criminal associates; four, engaging in sophisticated and distributed frauds using the sensitive information that was obtained; and five, laundering the proceeds of their illicit activity.

All five of these activities are criminal violations in and of themselves, and when conducted by sophisticated transnational networks of cyber criminals, this scheme has yielded hundreds of millions of dollars in illicit proceeds.

The Secret Service is committed to protecting the Nation from this threat. We disrupt every step of their five-part criminal

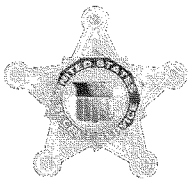
scheme through proactive criminal investigations and defeat these transnational cyber criminals through coordinated arrests and seizure of assets. Foundational to these efforts are the private industry partners as well as close partnerships that we have with State, local, Federal, and international law enforcement. As a result of these partnerships, we are able to prevent many cyber crimes by sharing criminal intelligence regarding the plans of cyber criminals and minimizing financial losses by stopping their criminal scheme.

Through our Department's National Cybersecurity and Communications Integration Center, the NCCIC, the Secret Service also quickly shares technical cybersecurity information while protecting civil rights and civil liberties in order to allow organizations to reduce their cyber risks by mitigating technical vulnerabilities.

We also partner with the private sector in academia to research cyber threats and publish information on cyber crime trends through reports like Carnegie Mellon CERT Insider Threat Study, the Verizon Data Breach Study, and the Trustwave Global Security Report. The Secret Service has a long history of protecting our Nation's financial system from threats. In 1865, the threat we were founded to address was that of counterfeit currency. As our financial payment system has evolved from paper to plastic, now digital information, so, too, has our investigative mission. The Secret Service is committed to protecting our Nation's financial system even as criminals increasingly exploit it through cyberspace. Through the dedicated efforts of our electronic crimes task forces and by working in close partnerships with the Department of Justice, in particular, the criminal division and the local U.S. Attorney's offices, the Secret Service will continue to bring cyber criminals that perpetrate major data breaches to justice. Thank you for the opportunity to testify on this important topic, and we look forward to your questions.

Mr. TERRY. Thank you, Mr. Noonan.

[The prepared statement of Mr. Noonan follows:]



William Noonan

Deputy Special Agent in Charge
United States Secret Service
Criminal Investigative Division
Cyber Operations Branch

Prepared Testimony

Before the

United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing and Trade

February 5, 2014

Good afternoon Chairman Terry, Ranking Member Schakowsky, and distinguished Members of the Committee. Thank you for the opportunity to testify on the risks and challenges the Nation faces from large-scale data breaches like those that have been recently reported and are of great concern to our Nation. The U.S. Secret Service (Secret Service) has decades of experience investigating large-scale criminal cyber intrusions, in addition to other crimes that impact our Nation's financial payment systems. Based on investigative experience and the understanding we have developed regarding transnational organized cyber criminals that are engaged in these data breaches and associated frauds, I hope to provide this committee useful insight into this issue from a federal law enforcement perspective to help inform your deliberations.

The Role of the Secret Service

The Secret Service was founded in 1865 to protect the U.S. financial system from the counterfeiting of our national currency. As the Nation's financial system evolved from paper to plastic to electronic transactions, so too has the Secret Service's investigative mission. Today, our modern financial system depends heavily on information technology for convenience and efficiency. Accordingly, criminals have adapted their methods and are increasingly using cyberspace to exploit our Nation's financial payment system by engaging in fraud and other illicit activities. This is not a new trend; criminals have been committing cyber financial crimes since at least 1970.[1]

Congress established 18 USC § 1029-1030 as part of the Comprehensive Crime Control Act of 1984; these statutes criminalized unauthorized access to computers[2] and the fraudulent use or trafficking of access devices[3]—defined as any piece of information or tangible item that is a means of account access that can be used to obtain money, goods, services, or other thing of value.[4] Congress specifically gave the Secret Service authority to investigate violations of both statutes.[5]

Secret Service investigations have resulted in the arrest and successful prosecution of cyber criminals involved in the largest known data breaches, including those of TJ Maxx, Dave & Buster's, Heartland Payment Systems, and others. Over the past four years Secret Service cyber crime investigations have resulted in over 4,900 arrests, associated with approximately $1.37 billion in fraud losses and the prevention of over $11.24 billion in potential fraud losses. Through our work with our partners at the Department of Justice (DOJ), in particular the local U.S. Attorney Offices, the Computer Crimes and Intellectual Property section (CCIPS), the International Organized Crime Intelligence and Operations Center (IOC-2), and others, we are confident we will continue to bring the cyber criminals that perpetrate major data breaches to justice.

---

[1] Beginning in 1970, and over the course of three years, the chief teller at the Park Avenue branch of New York's Union Dime Savings Bank manipulated the account information on the bank's computer system to embezzle over $1.5 million from hundreds of customer accounts. This early example of cyber crime not only illustrates the long history of cyber crime, but the difficulty companies have in identifying and stopping cyber criminals in a timely manner—a trend that continues today.

[2] *See* 18 USC § 1030

[3] *See* 18 USC § 1029

[4] *See* 18 USC § 1029(e)(1)

[5] *See* 18 USC § 1029(d) & 1030(d)(1)

The Transnational Cyber Crime Threat

Advances in computer technology and greater access to personally identifiable information (PII) via the Internet have created a virtual marketplace for transnational cyber criminals to share stolen information and criminal methodologies. As a result, the Secret Service has observed a marked increase in the quality, quantity, and complexity of cyber crimes targeting private industry and critical infrastructure. These crimes include network intrusions, hacking attacks, malicious software, and account takeovers leading to significant data breaches affecting every sector of the world economy. The recently reported data breaches of Target and Neiman Marcus are just the most recent, well-publicized examples of this decade-long trend of major data breaches perpetrated by cyber criminals who are intent on targeting our Nation's retailers and financial payment systems.

The increasing level of collaboration among cyber-criminals allows them to compartmentalize their operations, greatly increasing the sophistication of their criminal endeavors and allowing for development of expert specialization. These specialties raise both the complexity of investigating these cases, as well as the level of potential harm to companies and individuals. For example, illicit underground cyber crime market places allow criminals to buy, sell and trade malicious software, access to sensitive networks, spamming services, credit, debit and ATM card data, PII, bank account information, brokerage account information, hacking services, and counterfeit identity documents. These illicit digital marketplaces vary in size, with some of the more popular sites boasting membership of approximately 80,000 users. These digital marketplaces often use various digital currencies, and cyber criminals have made extensive use of digital currencies to pay for criminal goods and services or launder illicit proceeds.

The Secret Service has successfully investigated many underground cyber criminal marketplaces. In one such infiltration, the Secret Service initiated and conducted a three-year investigation that led to the indictment of 11 perpetrators allegedly involved in hacking nine major U.S. retailers and the theft and sale of more than 40 million credit and debit card numbers. The investigation revealed that defendants from the United States, Estonia, China and Belarus successfully obtained credit and debit card numbers by hacking into the wireless computer networks of major retailers — including TJ Maxx, BJ's Wholesale Club, Office Max, Boston Market, Barnes & Noble, Sports Authority and Dave & Buster's. Once inside the networks, these cyber criminals installed "sniffer" programs[6] that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks. After the data was collected, the conspirators concealed the information in encrypted computer servers that they controlled in the United States and Eastern Europe. The credit and debit card numbers were then sold through online transactions to other criminals in the United States and Eastern Europe. The stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The defendants then used these fraudulent cards to withdraw tens of thousands of dollars at a time from ATMs. The defendants were able to conceal and launder their illegal proceeds by using anonymous Internet-based

[6] Sniffers are programs that detect particular information transiting computer networks, and can be used by criminals to acquire sensitive information from computer systems.

digital currencies within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe.[7]

In data breaches like these the effects of the criminal acts extended well beyond the companies compromised, potentially affecting millions of individual card holders. Proactive and swift law enforcement action protects consumers by preventing and limiting the fraudulent use of payment card data, identity theft, or both. Cyber crime directly impacts the U.S. economy by requiring additional investment in implementing enhanced security measures, inflicting reputational damage on U.S. firms, and direct financial losses from fraud—all costs that are ultimately passed on to consumers.

Secret Service Strategy for Combating this Threat

The Secret Service proactively investigates cyber crime using a variety of investigative means to infiltrate these transnational cyber criminal groups. As a result of these proactive investigations, the Secret Service is often the first to learn of planned or ongoing data breaches and is quick to notify financial institutions and the victim companies with actionable information to mitigate the damage from the data breach and terminate the criminal's unauthorized access to their networks. One of the most poorly understood facts regarding data breaches is that it is rarely the victim company that first discovers the criminal's unauthorized access to their network; rather it is law enforcement, financial institutions, or other third parties that identify and notify the likely victim company of the data breach by identifying the common point of origin of the sensitive data being trafficked in cyber crime marketplaces.

A trusted relationship with the victim is essential for confirming the crime, remediating the situation, beginning a criminal investigation, and collecting evidence. The Secret Service's worldwide network of 33 Electronic Crimes Task Forces (ECTF), located within our field offices, are essential for building and maintaining these trusted relationships, along with the Secret Service's commitment to protecting victim privacy.

In order to confirm the source of data breaches and to stop the continued theft of sensitive information and the exploitation of a network, the Secret Service contacts the owner of the suspected compromised computer systems. Once the victim of a data breach confirms that unauthorized access to their networks has occurred, the Secret Service works with the local U.S. Attorney's office, or appropriate state and local officials, to begin a criminal investigation of the potential violation of 18 USC § 1030. During the course of this criminal investigation, the Secret Service identifies the malware and means of access used to acquire data from the victim's computer network. In order to enable other companies to mitigate their cyber risk based on current cyber crime methods, we quickly share information concerning the cybersecurity incident with the widest audience possible, while protecting grand jury information, the integrity of ongoing criminal investigations, and the victims' privacy. We share this cybersecurity information through:

[7] Additional information on the criminal use of digital currencies can be referenced in testimony provided by U.S. Secret Service Special Agent in Charge Edward Lowery before the Senate Homeland Security and Governmental Affairs Committee in a hearing titled, "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies" (November 18, 2013).

- Our Department's National Cybersecurity & Communications Integration Center (NCCIC);
- The Information Sharing and Analysis Centers (ISAC);
- Our ECTFs;
- The publication of joint industry notices;
- Our numerous partnerships developed over the past three decades in investigating cyber crimes; and,
- Contributions to leading industry and academic reports like the Verizon Data Breach Investigations Report, the Trustwave Global Security Report, and the Carnegie Mellon CERT Insider Threat Study.

As we share cybersecurity information discovered in the course of our criminal investigation, we also continue our investigation in order to apprehend and bring to justice those involved. Due to the inherent challenges in investigating transnational crime, particularly the lack of cooperation of some countries with law enforcement investigations, occasionally it takes years to finally apprehend the top tier criminals responsible. For example, Dmitriy Smilianets and Vladimir Drinkman were arrested in June 2012, as part of a multi-year investigation Secret Service investigation, while they were traveling in the Netherlands thanks to the assistance of Dutch law enforcement. The alleged total fraud loss from their cyber crimes exceeds $105 million.

As a part of our cyber crime investigations, the Secret Service also targets individuals who operate illicit infrastructure that supports the transnational organized cyber criminal. For example, in May 2013 the Secret Service, as part of a joint investigation through the Global Illicit Financial Team, shut down the digital currency provider Liberty Reserve. Liberty Reserve is alleged to have had more than one million users worldwide and to have laundered more than $6 billion in criminal proceeds. This case is believed to be the largest money laundering case ever prosecuted in the United States and is being jointly prosecuted by the U.S. Attorney's Office for the Southern District of New York and DOJ's Asset Forfeiture and Money Laundering Section. In a coordinated action with the Department of the Treasury, Liberty Reserve was identified as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act, effectively cutting it off from the U.S. financial system.

Collaboration with Other Federal Agencies and International Law Enforcement

While cyber-criminals operate in a world without borders, the law enforcement community does not. The increasingly multi-national, multi-jurisdictional nature of cyber crime cases has increased the time and resources needed for successful investigation and adjudication. The partnerships developed through our ECTFs, the support provided by our Criminal Investigative Division, the liaison established by our overseas offices, and the training provided to our special agents via Electronic Crimes Special Agent Program are all instrumental to the Secret Service's successful network intrusion investigations.

One example of the Secret Service's success in these investigations is the case involving Heartland Payment Systems. As described in the August 2009 indictment, a transnational organized criminal group allegedly used various network intrusion techniques to breach security and navigate the credit card processing environment. Once inside the networks, they installed "sniffer" programs to capture card numbers, as well as password and account information. The

Secret Service investigation, the largest and most complex data breach investigation ever prosecuted in the United States, revealed that data from more than 130 million credit card accounts were at risk of being compromised and exfiltrated to a command and control server operated by an international group directly related to other ongoing Secret Service investigations. During the course of the investigation, the Secret Service uncovered that this international group committed other intrusions into multiple corporate networks to steal credit and debit card data. The Secret Service relied on various investigative methods, including subpoenas, search warrants, and Mutual Legal Assistance Treaty (MLAT) requests through our foreign law enforcement partners to identify three main suspects. As a result of the investigation, these primary suspects were indicted for various computer-related crimes. The lead defendant in the indictment pled guilty and was sentenced to twenty years in federal prison. This investigation is ongoing with over 100 additional victim companies identified.

Recognizing these complexities, several federal agencies are collaborating to investigate cases and identify proactive strategies. Greater collaboration within the federal, state and local law enforcement community enhances information sharing, promotes efficiency in investigations, and facilitates efforts to de-conflict in cases of concurrent jurisdiction. For example, the Secret Service has collaborated extensively with DOJ's CCIPS, which "prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts."[8] The Secret Service's ECTFs are a natural complement to CCIPS, resulting in an excellent partnership over the years. In the last decade, nearly every major cyber investigation conducted by the Secret Service has benefited from CCIPS contributions.

The Secret Service also maintains a positive relationship with the DOJ's Federal Bureau of Investigation (FBI). The Secret Service has a permanent presence at the National Cyber Investigative Joint Task Force (NCIJTF), which coordinates, integrates, and shares information related to investigations of national security cyber threats. The Secret Service also often partners with the FBI on various criminal cyber investigations. For example, in August 2010, a joint operation involving the Secret Service, FBI, and the Security Service of Ukraine (SBU), yielded the seizure of 143 computer systems – one of the largest international seizures of digital media gathered by U.S. law enforcement – consisting of 85 terabytes of data, which was eventually transferred to law enforcement authorities in the United States. The data was seized from a criminal Internet service provider located in Odessa, Ukraine, also referred to as a "Bullet Proof Hoster." Thus far, the forensic analysis of these systems has already identified a significant amount of criminal information pertaining to numerous investigations currently underway by both agencies, including malware, criminal chat communications, and PII of U.S. citizens.

The case of Vladislav Horohorin is another example of successful cooperation between the Secret Service and its law enforcement partners around the world. Mr. Horohorin, one of the world's most notorious traffickers of stolen financial information, was arrested on August 25, 2010, pursuant to a U.S. arrest warrant issued by the Secret Service. Mr. Horohorin created the first fully-automated online store which was responsible for selling stolen credit card data. Both CCIPS and the Office of International Affairs at DOJ played critical roles in this apprehension.

[8] U.S. Department of Justice. (n.d.). *Computer Crime & Intellectual Property Section: About CCIPS.* Retrieved from http://www.justice.gov/criminal/cybercrime/ccips.html

Furthermore, as a result of information sharing, the FBI was able to bring additional charges against Mr. Horohorin for his involvement in a Royal Bank of Scotland network intrusion. This type of cooperation is crucial if law enforcement is to be successful in disrupting and dismantling criminal organizations involved in cyber crime.

This case demonstrates the importance of international law enforcement cooperation. Through the Secret Service's 24 international field offices the Service develops close partnerships with numerous foreign law enforcement agencies in order to combat transnational crime. Successfully investigating transnational crime depends not only on the efforts of the Department of State and the DOJ's Office of International Affairs to establish and execute MLATs, and other forms of international law enforcement cooperation, but also on the personal relationships that develop between U.S. law enforcement officers and their foreign counterparts. Both the CCIPS and the Office of International Affairs at DOJ played critical roles in this apprehension. Furthermore, as a result of information sharing, the FBI was able to bring additional charges against Mr. Horohorin for his involvement in a Royal Bank of Scotland network intrusion. This type of cooperation is crucial if law enforcement is to be successful in disrupting and dismantling criminal organizations involved in cyber crime.

Within DHS, the Secret Service benefits from a close relationship with Immigration and Customs Enforcement's Homeland Security Investigations (ICE-HSI). Since 1997, the Secret Service, ICE-HSI, and IRS-CI have jointly trained on computer investigations through the Electronic Crimes Special Agent Program (ECSAP). ICE-HSI is also a member of Secret Service ECTFs, and ICE-HSI and the Secret Service have partnered on numerous cyber crime investigations including the recent take down of the digital currency Liberty Reserve.

To further its cybersecurity information sharing efforts, the Secret Service has strengthened its relationship with the National Protection and Programs Directorate (NPPD), including the NCCIC. As the Secret Service identifies malware, suspicious IPs and other information through its criminal investigations, it shares information with our Department's NCCIC. The Secret Service continues to build upon its full-time presence at NCCIC to coordinate its cyber programs with other federal agencies.

As a part of these efforts, and to ensure that information is shared in a timely and effective manner, the Secret Service has personnel assigned to the following DHS and non-DHS entities:

- NPPD's National Cybersecurity & Communications Integration Center (NCCIC);
- NPPD's Office of Infrastructure Protection;
- DHS's Science and Technology Directorate (S&T);
- DOJ National Cyber Investigative Joint Task Force (NCIJTF);
- Each FBI Joint Terrorism Task Force (JTTF), including the National JTTF;
- Department of the Treasury - Office of Terrorist Financing and Financial Crimes (TFFC);
- Department of the Treasury - Financial Crimes Enforcement Network (FinCEN);
- Central Intelligence Agency;
- DOJ, International Organized Crime and Intelligence Operations Center (IOC-2);
- Drug Enforcement Administration's Special Operations Division;
- EUROPOL; and

- INTERPOL.

The Secret Service is committed to ensuring that all its information sharing activities comply with applicable laws, regulations, and policies, including those that pertain to privacy and civil liberties.

Secret Service Framework

To protect our financial infrastructure, industry, and the American public, the Secret Service has adopted a multi-faceted approach to aggressively combat cyber and computer-related crimes.

Electronic Crimes Task Forces

In 1995, the Secret Service New York Field Office established the New York Electronic Crimes Task Force (ECTF) to combine the resources of academia, the private sector, and local, state and federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructures. In 2001, Congress directed the Secret Service to establish a nationwide network of ECTFs to "prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."[9]

Secret Service field offices currently operate 33 ECTFs, including two based overseas in Rome, Italy, and London, England. Membership in our ECTFs includes: over 4,000 private sector partners; over 2,500 international, federal, state and local law enforcement partners; and over 350 academic partners. By joining our ECTFs, our partners benefit from the resources, information, expertise and advanced research provided by our international network of members while focusing on issues with significant regional impact.

Cyber Intelligence Section

Another example of our partnership approach with private industry is our Cyber Intelligence Section (CIS) which analyzes evidence collected as a part of Secret Service investigations and disseminates information in support of Secret Service investigations worldwide and generates new investigative leads based upon its findings. CIS leverages technology and information obtained through private sector partnerships to monitor developing technologies and trends in the financial payments industry for information that may be used to enhance the Secret Service's capabilities to prevent and mitigate attacks against the financial and critical infrastructures. CIS also has an operational unit that investigates international cyber-criminals involved in cyber-intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes. The information and coordination provided by CIS is a crucial element to successfully investigating, prosecuting, and dismantling international criminal organizations.

[9] *See* Public Law 107-56 Section 105 (appears as note following 18 U.S.C. § 3056).

Electronic Crimes Special Agent Program

A central component of the Secret Service's cyber-crime investigations is its Electronic Crimes Special Agent Program (ECSAP), which is comprised of nearly 1,400 Secret Service special agents who have received at least one of three levels of computer crimes-related training.

Level I – Basic Investigation of Computers and Electronic Crimes (BICEP): The BICEP training program focuses on the investigation of electronic crimes and provides a brief overview of several aspects involved with electronic crimes investigations. This program provides Secret Service agents and our state and local law enforcement partners with a basic understanding of computers and electronic crime investigations and is now part of our core curriculum for newly hired special agents.

Level II – Network Intrusion Responder (ECSAP-NI): ECSAP-NI training provides special agents with specialized training and equipment that allows them to respond to and investigate network intrusions. These may include intrusions into financial sector computer systems, corporate storage servers, or various other targeted platforms. The Level II trained agent will be able to identify critical artifacts that will allow for effective investigation of identity theft, malicious hacking, unauthorized access, and various other related electronic crimes.

Level III – Computer Forensics (ECSAP-CF): ECSAP-CF training provides special agents with specialized training and equipment that allows them to investigate and forensically obtain digital evidence to be utilized in the prosecution of various electronic crimes cases, as well as criminally-focused protective intelligence cases.

These agents are deployed in Secret Service field offices throughout the world and have received extensive training in forensic identification, as well as the preservation and retrieval of electronically stored evidence. ECSAP-trained agents are computer investigative specialists, qualified to conduct examinations on all types of electronic evidence. These special agents are equipped to investigate the continually evolving arena of electronic crimes and have proven invaluable in the successful prosecution of criminal groups involved in computer fraud, bank fraud, identity theft, access device fraud and various other electronic crimes targeting our financial institutions and private sector.

National Computer Forensics Institute

The National Computer Forensics Institute (NCFI) initiative is the result of a partnership between the Secret Service, NPPD, the State of Alabama, and the Alabama District Attorney's Association. The goal of this facility is to provide a national standard of training for a variety of electronic crimes investigations. The program offers state and local law enforcement officers, prosecutors, and judges the training necessary to conduct computer forensics examinations. Investigators are trained to respond to network intrusion incidents and to conduct electronic crimes investigations. Since opening in 2008, the institute has held over 110 cyber and digital forensics courses in 13 separate subjects and trained and equipped more than 2,500 state and local officials, including more than 1,600 police investigators, 570 prosecutors and 180 judges from all 50 states and three U.S. territories. These NCFI graduates represent more than 1,000 agencies nationwide.

Partnerships with Academia

In August 2000, the Secret Service and Carnegie Mellon University Software Engineering Institute (SEI) established the Secret Service CERT[10] Liaison Program to provide technical support, opportunities for research and development, as well as public outreach and education to more than 150 scientists and researchers in the fields of computer and network security, malware analysis, forensic development, training and education. Supplementing this effort is research into emerging technologies being used by cyber-criminals and development of technologies and techniques to combat them.

The primary goals of the program are: to broaden the Secret Service's knowledge of software engineering and networked systems security; to expand and strengthen partnerships and relationships with the technical and academic communities; partner with CERT-SEI and Carnegie Mellon University to support research and development to improve the security of cyberspace and improve the ability of law enforcement to investigate crimes in a digital age; and to present the results of this partnership at the quarterly meetings of our ECTFs.

In August 2004, the Secret Service partnered with CERT-SEI to publish the first "Insider Threat Study" examining the illicit cyber activity and insider fraud in the banking and finance sector. Due to the overwhelming response to this initial study, the Secret Service and CERT-SEI, in partnership with DHS Science & Technology (S&T), updated the study and released the most recent version just last year, which is published at http://www.cert.org/insider_threat/.

To improve law enforcement's ability to investigate crimes involving mobile devices, the Secret Service opened the Cell Phone Forensic Facility at the University of Tulsa in 2008. This facility has a three-pronged mission: (1) training federal, state and local law enforcement agents in embedded device forensics; (2) developing novel hardware and software solutions for extracting and analyzing digital evidence from embedded devices; and (3) applying the hardware and software solutions to support criminal investigations conducted by the Secret Service and its partner agencies. To date, investigators trained at the Cell Phone Forensic Facility have completed more than 6,500 examinations on cell phone and embedded devices nationwide. Secret Service agents assigned to the Tulsa facility have contributed to over 300 complex cases that have required the development of sophisticated techniques and tools to extract critical evidence.

These collaborations with academia, among others, have produced valuable innovations that have helped strengthen the cyber ecosystem and improved law enforcement's ability to investigate cyber crime. The Secret Service will continue to partner closely with academia and DHS S&T, particularly the Cyber Forensics Working Group, to support research and development of innovate tools and methods to support criminal investigations.

Legislative Action to Combat Data Breaches

While there is no single solution to prevent data breaches of U.S. customer information, legislative action could help to improve the Nation's cybersecurity, reduce regulatory costs on

[10] CERT—not an acronym—conducts empirical research and analysis to develop and transition socio-technical solutions to combat insider cyber threats.

U.S. companies, and strengthen law enforcement's ability to conduct effective investigations. The Administration previously proposed law enforcement provisions related to computer security through a letter from OMB Director Lew to Congress on May 12, 2011, highlighting the importance of additional tools to combat emerging criminal practices. We continue to support changes like these that will keep up with rapidly-evolving technologies and uses.

Conclusion

The Secret Service is committed to safeguarding the Nation's financial payment systems by investigating and dismantling criminal organizations involved in cyber crime. Responding to the growth in these types of crimes and the level of sophistication these criminals employ requires significant resources and greater collaboration among law enforcement and its public and private sector partners. Accordingly, the Secret Service dedicates significant resources to improving investigative techniques, providing training for law enforcement partners, and raising public awareness. The Secret Service will continue to be innovative in its approach to cyber crime and cyber security and is pleased that the Committee recognizes the magnitude of these issues and the evolving nature of these crimes.

Mr. TERRY. Mr. Zelvin, you are now recognized for your 5 minutes.

STATEMENT OF LARRY ZELVIN

Mr. ZELVIN. Chairman Terry, Ranking Member Schakowsky, distinguished members of the subcommittee. Thank you very much for the opportunity to be here before you today. In my brief opening comments, I would like to highlight the DHS National Cybersecurity and Communications Integrations Center, or NCCIC's role in preventing, responding to, and mitigating cyber incidents, and then discuss our activities during the recent point of sale compromises. I hope my remarks will demonstrate the increasing importance of building and maintaining close relationships among the wide range of partners in order to address all aspects of malicious cyber activity, as well as to reduce continuing vulnerabilities, protect against future attacks, and mitigate the consequences of incidents that have already occurred.

The importance of leveraging these complementary missions has been consistently demonstrated over the last several years, and is an increasingly critical part of the broader framework used by the government and the private sector to cooperate responding to malicious cyber activity.

As you well know, the Nation's economic vitality and the national security depends on the secure cyberspace where reasonable risk decisions can be made, and the flow of digital goods and online interactions can occur safely and reliably. In order to meet these objectives, we must share technical characteristics of malicious cyber activity in a timely fashion so we can discover, address, and mitigate cyber threats and vulnerabilities. It is increasingly clear that no single country, agency, company or individual can effectively respond to the ever-rising threats of malicious cyber activity alone.

Effective responses require a whole nation effort, including close coordination among entities such as the NCCIC, the Secret Service, the Department of Justice, to include the Federal Bureau of Investigation, the Intelligence Community, sector specific agencies such as the Department of Treasury, the private sector entities who are simply critical to these efforts, and State, local, tribal, territorial, and international governments.

In carrying out its particular responsibilities, the NCCIC promotes and implements a unified approach to cybersecurity, which enables the efforts of these diverse partners to quickly share cybersecurity information in a manner which ensures the protection of individuals' privacy, civil rights, and civil liberties.

As you may already know, the NCCIC is a civilian organization that provides an around-the-clock center where key government, private sector, and international partners can work collaboratively together in both physical and virtual environments. The NCCIC is comprised of four branches, the United States Computer Emergency Readiness Team, or US–CERT, the Industrial Control Systems Cyber Emergency Response Team, or ICS–CERT, the National Coordinating Center for Communications, and Operations and Integration component.

In response to the recent retailer compromises, the NCCIC specifically leveraged the resources and capabilities of US–CERT, whose mission focuses specifically on computer network defense that includes prevention, protection, mitigation, response, and recovery activities. In executing this mission, the NCCIC and US–CERT regularly publishes technical and nontechnical information products assessing the characteristics of malicious cyber activity, improving the ability of organizations and individuals to reduce that risk.

When appropriate, all NCCIC components have onsite response capabilities that can assist owners and operators at their facilities. In addition, US–CERT's global partnership with over 200 other CERTs worldwide allow the team to work directly with analysts from across international borders to develop a comprehensive picture of malicious cyber activity and mitigation options.

Increasingly, data from the NCCIC and US–CERT can be shared in machine-readable formats using the Structured Threat Information Expression, also known as STIX, which is being currently being implemented and utilized. In some of the recent point of sale incidents, NCCIC, US–CERT analyzed the malware provided to us by the Secret Service and other relevant technical data, and used findings, in part, to create a number of information sharing products.

The first product, which is publicly available, can be found on the US–CERT's Web site provides nontechnical overview of risks to point of sale systems along with recommendations for how businesses and individuals can better protect themselves and mitigate their losses in the event of an incident that has already occurred.

Other products have been more limited in distribution in that they are meant for cybersecurity professionals in that they provide detailed technical analysis and mitigation recommendations to better enable experts to protect, discover, respond, and recover from events. As a matter of strategic intent, the NCCIC's goal is always to share information as broadly as possible, which includes delivering products tailored to specific audiences.

These efforts ensure that actionable details associated with a major cyber incident are shared with the right partners so they can protect themselves, their families, their businesses and organizations quickly and accurately.

In the case of the point of sale compromises, we especially benefited by the close coordination of the Financial Services Information Sharing and Analysis Center, or the FS–ISAC. In particular, the FS–ISAC's Payments Processing Information Sharing Council has been particularly useful in that they provide a form for sharing information about fraud, threats, vulnerabilities and risk mitigation in the payments industry.

In conclusion, I want to again highlight that we in DHS and the NCCIC strive every day to enhance the security and resilience across cyberspace and the information technology enterprise. We will accomplish these tasks using voluntary means, ever mindful of the need to respect privacy, civil liberties, and the law. I truly appreciate the opportunity to speak with you today and look forward to your questions.

Mr. TERRY. Thank you, Mr. Zelvin.

[The prepared statement of Mr. Zelvin follows:]

Testimony of

Larry Zelvin
National Cybersecurity and Communications Integration Center Director
National Protection and Programs Directorate
U.S. Department of Homeland Security

Before the
United States House of Representatives
Energy and Commerce Committee
Subcommittee on Commerce, Manufacturing and Trade

February 5, 2014

Introduction

Chairman Terry, Ranking Member Schakowsky, and distinguished Members of the Committee, I am here today to discuss the Department of Homeland Security's (DHS) roles in responding to the recently reported breach of point of sale (POS) systems at two major retailers and the apparent compromise of sensitive personal and financial information that resulted from those breaches. I will also put these actions in the context of DHS's responsibilities to deal with cyber threats to our Nation's financial transaction systems as well as other important elements of critical infrastructure.

During the recent POS system compromises, DHS's National Protection and Program Directorate's (NPPD) strong operational and private sector outreach programs were leveraged to help other retailers secure their systems to prevent future attacks while simultaneously supporting the United States Secret Service's (Secret Service) criminal investigation. The National Cybersecurity and Communications Integration Center (NCCIC) used its unique cybersecurity analysis and mitigation capabilities to coordinate efforts to secure systems against future attacks and provided timely analysis for the Secret Service. Through close coordination among DHS components and other partners, we have not only preserved the integrity of the Secret Service law enforcement investigation, we have provided businesses and users the key information they need to protect themselves and reduce the likelihood of a similar incident occurring in the future.

Today I'd like to review in greater detail how NPPD works daily with our colleagues at the Secret Service and with interagency and cross sector partners to respond to and mitigate this and other cyber incidents. I hope this overview will demonstrate the increasing importance of building and maintaining close relationships between law enforcement officials and network defense experts in order to address both the criminal aspects of malicious cyber activity, as well as to reduce continuing vulnerabilities, protect against future attacks, and mitigate consequences of incidents. The importance of effectively leveraging these complementary missions has been consistently demonstrated over the last several years, and is an increasingly important part of the broader framework used by the government and the private sector to cooperate responding to malicious cyber activity.

A Whole of Nation Approach to Cybersecurity

As the Department has highlighted in previous testimony, cyberspace is woven into the fabric of our daily lives. According to recent estimates, the Internet encompasses more than two billion people with at least 12 billion computers and devices, including global positioning systems, mobile phones, satellites, data routers, ordinary desktop computers, and industrial control systems that run the power plants, water systems, and much more that make up our nation's critical infrastructure. While this increased connectivity has led to significant transformations and advances across our country – and around the world – it also has increased complexity and exposes us to new vulnerabilities that can only be addressed by timely action and shared responsibility. The Nation's economic vitality and national security depend on a safe cyberspace where reasonable risk decisions can be made and the flow of digital goods, transactions, and online interactions can occur safely and securely. No country, industry, community or individual is immune to the threat of a cyber-attack and timely action is required to share necessary information in order to discover, address, and mitigate the ever-growing threat of malicious cyber activity.

Furthermore, no single agency or organization by itself can effectively respond to the rising threat of malicious cyber activity. Now, more than ever, there is a need for a civilian-government capability to engage not only with affected entities but with other critical infrastructure sectors and companies that also are at risk. Successful responses to dynamic cyber intrusions require coordination among DHS, the Department of Justice—including the Federal Bureau of Investigation, Criminal Division, National Security Division, and U.S. Attorneys' Offices—the Intelligence Community, the Department of State, the specialized expertise of Sector Specific Agencies such as the Department of the Treasury, private sector partners – who are critical to these efforts – and state, local, tribal and territorial, as well as international partners, each of which have unique roles to play. In carrying out these activities, NPPD promotes and implements a unified approach to cybersecurity incident response, which enables the efforts of a diverse set of partners. Our incident response activities are synchronized with the comprehensive and timely sharing of cybersecurity information, and done in a manner which ensures the protection of individuals' privacy, civil rights and civil liberties.

The Central Role of the National Cybersecurity and Communications Integration Center

To better manage and facilitate cybersecurity information sharing efforts, analysis, and incident response activities, exemplified by the recent retailer breach, the Department operates the National Cybersecurity and Communications Integration Center (NCCIC), an around-the-clock center where key government, private sector, and international partners all work together. The NCCIC is comprised of four branches: the United States Computer Emergency Readiness Team (US-CERT), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the National Coordinating Center (NCC) for Communications, and Operations Integration (O&I). These branches provide the capabilities, skills, knowledge, and partnerships needed to serve as a focal point for coordinating cybersecurity information sharing with the private sector; provide technical assistance, onsite analysis, mitigation support, and assessment assistance to cyber-attack victims; and coordinate the National response to significant cyber incidents affecting critical infrastructure.

While responding to the recent retailer compromises, the NCCIC specifically leveraged the resources and capabilities of US-CERT. US-CERT's global partnerships allow it to work directly with analysts from across multiple sectors and international borders to develop a comprehensive picture of malicious cyber activity and mitigation options. US-CERT's mission focuses specifically on computer network defense, and it is able to apply its full resources to supporting prevention, protection, mitigation, response, and recovery efforts. US-CERT publishes technical and non-technical information products assessing the characteristics of malicious cyber activity and improving the ability of organizations and individuals to reduce their risk.

US-CERT's unique ability to aggregate, analyze, and share diverse sets of information from law enforcement, the intelligence community, the private sector – including information sharing and analysis centers – and international partners through more than 200 CERT partnerships worldwide is critical to NCCIC's information sharing mission. Increasingly, our information sharing activities are undertaken using Structured Threat Information Expression (STIX), which allows for data to be shared at machine speed in a standard, machine readable format.

Current Threat Landscape and Recent Retail Company Targeting

The NCCIC currently sees malicious cyber activity perpetrated by a variety of actors who employ diverse methods to achieve their objectives.

For some time, cyber criminals have been targeting consumer data entered into POS systems. When consumers purchase goods or services from a retailer, the transaction is processed through POS systems, which consist of the hardware (e.g. the equipment used to swipe a credit or debit card and the computer or mobile device attached to it) as well as the software that tells the hardware what to do with the information it captures. When consumers use a credit or debit card at a POS system, the information stored on the magnetic stripe of the card is collected and processed by the attached computer or device.

The data stored on the magnetic stripe is referred to as "Track One" and "Track Two" data. Track One data is personal information associated with the account. Track Two data contains information such as the credit card number and expiration date. In some circumstances, criminals attach a physical device to the POS system to collect card data, which is referred to as "skimming". In other cases, cyber criminals deliver malware which acquires card data as it passes through a POS system, eventually exfiltrating the desired data back to the criminal.

POS systems are connected to computers or devices, and are often enabled to access the Internet and email services. Malicious links or attachments in emails as well as malicious websites can be accessed and malware may subsequently be downloaded by an end user of a POS system.

On December 19, 2013, a major retailer publically announced it had experienced unauthorized access to payment card data from the retailer's U.S. stores. The information involved in this incident included customer names, credit and debit card numbers, and the cards' expiration dates and card verification value security codes. Another retailer also reported a malware incident involving its POS system on January 11, 2014, that resulted in the apparent compromise of credit

card and payment information. A direct connection between these two incidents has not been established.

In response to this activity, NCCIC/US-CERT analyzed the malware identified by the Secret Service as well as other relevant technical data and used those findings, in part, to create two information sharing products. The first product, which is publically available and can be found on US-CERT's website, provides a non-technical overview of risks to POS systems, along with recommendations for how businesses and individuals can better protect themselves and mitigate their losses in the event an incident has already occurred. The second product provides more detailed technical analysis and mitigation recommendations, and has been securely shared with industry partners to enable their protection efforts. NCCIC's goal is always to share information as broadly as possible, including by producing products tailored to specific audiences.

These efforts ensured that actionable details associated with a major cyber incident were shared with the private sector partners who needed the information in order to protect themselves and their customers quickly and accurately, while also providing individuals with practical recommendations for mitigating the risk associated with the compromise of their personal information. NCCIC especially benefited from close coordination with the Financial Services Information Sharing and Analysis Center during this response.

Ensuring Robust Privacy and Civil Rights and Civil Liberties Safeguards

Throughout our response to the retailer breaches we followed pre-existing protocols and control measures to protect personally identifiable information (PII) and other sensitive information that could cause harm to individuals or the critical infrastructure entities we provide assistance to. Our top level approach is to minimize the collection, retention, dissemination or use of PII, and other sensitive information that is not relevant to the cyber threat. There are also more detailed standards for handling specific types of information within specific programs and activities, tailored to the specific programs, the types of information handled and the mission requirements.

DHS remains committed to ensuring cyberspace is supported by a secure and resilient infrastructure that enables open communication, innovation, and prosperity while protecting privacy, confidentiality, and civil rights and civil liberties by design.

Public Outreach

It is important to note that the NCCIC is only one part of NPPD's overall effort to create a more secure cyberspace through working with private and public sector partners. NPPD continues to build its capabilities and our relationships by reinforcing the Department's Stop.Think.Connect.™ public awareness campaign, which is a year-round national effort designed to engage and challenge Americans to join the effort to practice and promote safe online practices. The Stop.Think.Connect.™ Campaign, launched during National Cyber Security Awareness Month in October 2010, helps Americans understand and manage the risks that come with living in a connected world. NPPD also works closely with the Secret Service Electronic Crimes Task Forces, leveraging their public/private partnerships, and works closely with other Federal agencies, including Sector Specific Agencies, to share cybersecurity

information with critical infrastructure owners and operators. We are aggressively pursuing the objectives of the Executive Order 13636, Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive 21, Critical Infrastructure Security and Resilience, to increase the quality, quantity and breadth of public/private sector information sharing, while remaining vigilant on privacy and civil liberties protections. This includes development of the EO 13636-directed voluntary program to support adoption of the NIST Cybersecurity Framework, by owners and operators of critical infrastructure and any other interested entities.

Conclusion

While the Secret Service's criminal investigation into the these activities is on-going, NPPD through the NCCIC and other organizations continues to build shared situational awareness of similar threats among our private sector and government partners and the American public at large. At every opportunity, the NCCIC and our private sector outreach program publish technical and non-technical products on best practices for protecting businesses and customers against cyber threats and provide the information sharing and technical assistance necessary to address cyber threats as quickly as possible.

Increased connectivity has led to significant transformations and advances across our country – and around the world. Our daily lives, economic vitality, and national security depend on the cyberspace. DHS, through NPPD programs and partnerships, including the NCCIC and its central role, is working to outpace the cyber threat in order to maintain security and thereby foster innovation that has resulted from this interconnectedness. I appreciate the opportunity to speak with you today about the progress that the NCCIC has made in response to an ever evolving cyber threat and the road ahead for future improvements to our nation's cybersecurity.

Mr. TERRY. And that begins our questions with the end of your testimony. It is now the start of our questions. Each member has 5 minutes for questions, and I get to go first. Jan is second.

So, Mr. Noonan, you had mentioned that part of Secret Service's job is to investigate when breaches occur like this. Is the Secret Service, or are you involved in the investigation into what happened at both Target and Neiman Marcus and other entities?

Mr. NOONAN. Yes, sir. So we are involved in the criminal investigation of the Target breach, as well as the Neiman Marcus case.

Mr. TERRY. And so far, what have you been able to find out that you can communicate to us?

Mr. NOONAN. What we can determine at this point is that the criminal organizations that we are looking at in pursuing are highly technical, sophisticated criminal organizations that study their targets and use sophisticated tools to be able to compromise those various systems.

Mr. TERRY. And the breach at Target and Neiman Marcus, we have read through the news reports, was from a sophisticated criminal entity, as you mentioned in your investigation. Does your investigation also then go into how they exploited each of those major retailers' data?

Mr. NOONAN. Yes, sir.

Mr. TERRY. And what did you find out?

Mr. NOONAN. It is still an ongoing coordination investigation in which we are working on right now; however, we do know that the malware at this point in our investigation is not the same criminal tools being used at either one of those locations.

Mr. TERRY. So they are distinct, separate attacks?

Mr. NOONAN. Yes, sir.

Mr. TERRY. By separate distinct different criminal organizations?

Mr. NOONAN. We are working on that part right now, sir.

Mr. TERRY. OK. In your investigations, do you assess whether each of the, say, Target and Neiman Marcus' cyber standards or their cyber plans were adequate or inadequate or vulnerable?

Mr. NOONAN. The Secret Service does a criminal investigation, and again, we are continuing to go after the criminal organization that is perpetrating these. Both Neiman Marcus and Target do use robust security plans in their protection of their environment, and it comes back to the criminal actors in going after the pot of gold or whatever they can monetize. So, as good as security factors are, these criminal organizations are looking at ways to go around whatever security apparatuses had been set up, so these were very sophisticated, coordinated events. It was not necessarily from a singular actor. It's a coordination of pieces that were used to do these intrusions.

Mr. TERRY. Mr. Zelvin, you also, is your organization, NCCIC, have you looked at or assessed the cybersecurity at the entities that have been hacked?

Mr. ZELVIN. Mr. Chairman, we have not. We have been working closely with the Secret Service on identifying the malware that had been used in these incidents, doing the analysis and then sharing that with our partners across both the public and private sector, but I can tell you that the malware, as we see it, as Bill has said,

is an incredibly sophisticated and could be challenging the most robust security system.

Mr. TERRY. What specifically makes it more sophisticated than what we have seen before? Mr. Noonan.

Mr. NOONAN. Sure, sir. What we have seen actually in the development of the malware is that it is not an off-the-shelf type of malware that is utilized. What makes these targeted attacks unique is that the criminals are modifying and molding specific types of malware to fit whatever network or intrusion set they are going after.

Mr. TERRY. So, it was specifically designed for that, for Target?

Mr. NOONAN. For whichever——

Mr. TERRY. And a different one specifically designed for Neiman Marcus?

Mr. NOONAN. Depending on security platforms that are available, yes, sir.

Mr. TERRY. That is interesting.

Last, in future prevention, how important is an ISAC and would it help if there was a retailer specific ISAC?

Mr. ZELVIN. Mr. Chairman, the ISACs have been absolutely critical in our ability to share information with the broadest communities possible. As you well know, they are in all 16 critical infrastructure. In some of these infrastructures, certain groups, specifically in aviation and transportation, have made ISACs that are a subset of the larger ISAC. I would be a proponent of having a retailer ISAC, but it is really for the retailers to decide if it is useful for them.

We have been using the financial services ISAC in this case, but we look forward that if the business community wants to go that way, we would look forward to working with them.

Mr. TERRY. And that is something that you would be the umbrella organization to help?

Mr. ZELVIN. Sir, these are public/private partnerships, and DHS has worked with them for quite some time, so it is a model that we are very accustomed to using.

Mr. TERRY. There may be a few people in this audience that doesn't know what an ISAC is. Can you tell what is the advantage and just very quickly what it is?

Mr. ZELVIN. Yes, sir, Information Sharing Analysis Centers are predominantly around the 16 critical infrastructure, transportation, energy, finance, health, there is obviously a number of them, and it allows us, both in a public and private way, to get out to thousands of companies and share information in both directions.

So, it is a growing community, but it really allows us to get to those cybersecurity professionals and talk to those people that really do the network defense and have a conversation with those experts in a very robust scale.

Mr. TERRY. Thank you. Now it is my pleasure to recognize the ranking member of our subcommittee, Ms. Schakowsky, for 5 minutes.

Ms. SCHAKOWSKY. Let me just say to Mr. Zelvin, I am sure that the chairman would agree, we appreciate our visit to NCCIC that we did this weekend in preparation for this hearing and the very impressive work that you are doing.

I wanted to ask Attorney General Madigan a couple of questions. You alluded to the Illinois law, the Personal Information Protection Act that followed the Choice Point breach in 2005. I believe you were here talking about that as well.

Ms. MADIGAN. It is a different privacy matter, but I think that is really when all the States started looking into it seriously.

Ms. SCHAKOWSKY. So, our law in Illinois requires corporations, financial institutions, retail operators, government agencies, universities, other government entities to discuss data breaches, and the law says "In the most expedient time possible and without unreasonable delay."

How does your office determine what that is?

Ms. MADIGAN. Well, first of all, in every circumstance we are going to look at what has taken place, but we are also going to be very cognizant of what that company or that entity needs to do in terms of ensuring that they have maintained the integrity of their system, they put security in place, and if they are ongoing, law enforcement investigations. We certainly don't want to compromise those, and so we will wait in terms of requiring notification. But as we have learned over the years, and there are studies and reports out there that demonstrate it, the sooner an individual is notified that their information has been compromised, the less likely they are to actually face any sort of unauthorized charges or even a full account takeover, which will cost them a lot more money.

So, it is a case-by-case basis, and obviously, the sooner that we can make sure that consumers are notified, the better off everybody is in terms of the damage that is going to be done to them individually and the losses to the economy.

Ms. SCHAKOWSKY. So the language is kind of general, but you make the decision on a case-by-case basis in terms of notification?

Ms. MADIGAN. Correct. We work with the companies to see where they are in the process once we are alerted to the fact that a breach has taken place, and obviously we are always supportive of the work that the Secret Service and other law enforcement agencies are doing in terms of the criminal investigation. Really, the investigations that we do are civil side, to make sure that our law is actually——

Ms. SCHAKOWSKY. Have you found companies that have not used the most expedient time possibly or unreasonable delay?

Ms. MADIGAN. We always look at it, and there is always questions, really on any side because I think there is a great concern that many companies legitimately have about the hit it is going to take to their public image if they do have to reveal this, so there have been times that we think people could move faster, and we work with them to make sure that they actually get out that notice. We have not fined anybody for that.

Ms. SCHAKOWSKY. You know, you mentioned a couple of times about preemption, and I wanted to just ask you how important it is that Illinois, and I guess other States as well, maintain the right to require the disclosure of data breaches as quickly as possible and other enforcement mechanisms?

Ms. MADIGAN. I think probably every State official who would sit in front of you would say it is very important. Obviously, over the last 10 years, the States have really been able to be, as we like to

say, and I think you also can appreciate, the lavatories of innovation. When we started seeing people coming to us because they have been victims of identity theft, we needed to respond, and we needed to respond by making sure that they were notified when their personal information had been accessed and compromised, and we needed to be able to respond to make sure that companies were actually going to be putting in place stronger security measures. So we——

Ms. SCHAKOWSKY. Well, I want to ask you about that, because the Illinois law does not explicitly require minimum standards of protection for personal data, and yet you cited that as a problem. Who should do that then?

Ms. MADIGAN. Well, we have a growing number of States that are actually putting those requirements in place in terms of security, and I would have to say that looking back over the investigations that we have done into data breaches, it is clear that that has to be done, because there really is, we like to talk about best practice of being in place, but the reality is, oftentimes when we are doing these investigations, we repeatedly see situations where information that is personal and sensitive financial information is being maintained unencrypted.

We have seen situations where literally the information is obtained because documentation with sensitive information is being thrown into a dumpster and people have gotten it out and used that for illicit purposes. So, there is a minimum standard, and then I think that, as Chairman Ramirez did a very nice job of explaining, on a case-by-case basis with companies considering the types of information, the volume of information, the sensitivity of information, we have to have increasing standards required.

Ms. SCHAKOWSKY. My time is up, but I look forward to working with all of you to figure out what is the appropriate Federal congressional response. Thank you. I yield back.

Mr. TERRY. Thank you. I now recognize Chairman Emeritus Mr. Barton for your 5 minutes.

Mr. BARTON. Thank you, Mr. Chairman. I want to thank you and the ranking member for holding this hearing. This is, I think, potentially a very important hearing because this is one of the few things that Republicans and Democrats both agree on is a problem, and I think we maybe be able, with your leadership, to reach agreement on what a solution might be, so this is one of those rare days that something might actually happen as a result of a congressional hearing.

I am a co-chairman of the Privacy Caucus in the House, along with Congresswoman Diana DeGette, and Ms. Schakowsky is a member of that caucus, and most of the Republicans on this subcommittee are members. The gentlelady to my right is a chairwoman of a task force that Mr. Terry and Mr. Upton have put together on privacy, so we have got lots of people here that are listening very closely to what you folks say.

My question is a general question. I am going to start with the chairwoman of the Federal Trade Commission.

Madam Chairwoman, do you think it is possible to legislatively eliminate, or at least severely restrict data theft?

Ms. RAMIREZ. There is certainly no perfect solution to this issue, but it is clear to me that congressional action is necessary. I think it would be very helpful if there were a robust Federal standard when it comes to data security as well as to a robust standard when it comes to breach notification, and I think it is time for Congress to act.

Mr. BARTON. OK. Do the other members of the panel agree with that statement?

Ms. MADIGAN. Yes.

Mr. BARTON. You do. Good. I thought you might disagree actually.

Ms. MADIGAN. As long as you don't completely preempt us.

Mr. BARTON. Right. OK. Mr. Noonan and Mr. Zelvin?

Mr. NOONAN. Yes, sir, from a law enforcement approach, the Secret Service believes any notification perhaps to law enforcement with jurisdiction would definitely assist in this effort as well.

Mr. ZELVIN. Chairman, I come from the operational side of the Department, and there are things that Congress could do that could be very helpful as we work across the Nation or across the globe. You know, strengthening the ability on information sharing, I will tell you it is often difficult to get sometimes companies to share information with us because there is no statutory basis, and they tend to be on the conservative side.

Promoting establishing the adoption of cybersecurity standards would be very helpful, codifying the interest of authorities to help secure Federal civilian agency networks and assist critical infrastructure and then the national data breach reporting, we can't understand it if we don't know about them, so those are just some of the things that would be helpful.

Mr. BARTON. OK. The instance with Neiman Marcus, and I believe with Target also occurred when a criminal came into their stores and used a credit card that infected their system at the point of purchase. If we went to some sort of a, well, is it possible with the current technology to prevent that type of data theft? I see a lot of blank looks here.

Mr. NOONAN. Well, sir, just to clarify, the two breaches that we are talking about in Neiman Marcus and in Target were done by people infiltrating the system through a computer network.

Mr. BARTON. Oh, I thought they came in with a card and it——

Mr. NOONAN. No, sir.

Mr. BARTON. OK.

Mr. NOONAN. So it is very difficult to decide, and again, these are very complex, sophisticated criminals that did this. So they inserted actually a malware code, a malicious code into the system which was able to collect——

Mr. BARTON. They did it by penetrating the system from outside through a computer link.

Mr. NOONAN. Yes, sir.

Mr. BARTON. Not by giving a card that they inserted? OK——

Mr. NOONAN. And our investigation at this point is indicating that it is from transnational criminals so from criminals from outside the borders of the United States.

Mr. BARTON. OK. Well, I would hope, since everybody agreed that this is a problem, and that the Federal Government should

legislate, we can come up with a best practices set of recommendations to present to the committee, and then let us massage it only the way we can, and we will try to move on something, hopefully in this Congress.

And with that, I am going to yield back 34 seconds to the chair.

Mr. LANCE [presiding]. Thank you very much, Mr. Barton.

The chair recognizes the Dean of the Congress, Mr. Dingell of Michigan.

Mr. DINGELL. Mr. Chairman, you are most courteous, and I commend you for holding this important hearing.

I think we can all agree that the breaches at Target and Neiman Marcus were tragic. We had a duty to protect the American consumers from events like this in the future.

This committee and the House must act to pass data security and breach notification legislation. The administration has proposed similar legislation. Congress must act again, and we must ensure that such legislation makes it's way to the President's desk for signature.

To that end, I am most interested to hear any opinions of the FTC, and what they may wish to share with us. All of my questions this morning will be addressed to Chairwoman Ramirez. Madam Chairman, welcome.

Now, Chairman, your written testimony indicates the Commission enforces a patchwork of Federal data security statutes, such as Gramm-Leach-Bliley, the Fair Credit Reporting Act, Children's Online Privacy Protection Act. Do any of these acts require an FTC-covered entity whose collection of personal identification has been breached to notify customers so affected? Yes or no?

Ms. RAMIREZ. No.

Mr. DINGELL. That is needed I assume?

Ms. RAMIREZ. I am sorry?

Mr. DINGELL. That is needed, I assume.

Ms. RAMIREZ. Yes, absolutely.

Mr. DINGELL. Now, Madam Chairman, similarly, do any of these acts require entities subject to the breach to notify the Federal Trade Commission or law enforcement in general of such a breach? Yes or no?

Ms. RAMIREZ. No.

Mr. DINGELL. Madam Chairman, in view of this should the Congress enact a Federal data security and breach notification law? Yes or no?

Ms. RAMIREZ. Yes.

Mr. DINGELL. Madam Chairman, under such law should FTC-covered entities be exempted from breach notification requirements if they are already in compliance with GLBA, FCRA, and COPPA? Yes or no?

Ms. RAMIREZ. No.

Mr. DINGELL. Now, Madam Chairman, should such a law be administered by one Federal agency or by some kind of a collage of agencies?

Ms. RAMIREZ. One agency.

Mr. DINGELL. One agency. Now, I happen to think that that should be the Federal Trade Commission because of its long expertise in these matter. Do you agree?

Ms. RAMIREZ. I would agree.

Mr. DINGELL. Madam Chairman, should a Federal data security breach and notification law prescribe requirements for data security practices according to the reasonableness standard already employed at the Commission? Yes or no?

Ms. RAMIREZ. Yes.

Mr. DINGELL. Madam Chairman, should that be expanded? Should that be expanded?

Ms. RAMIREZ. Yes, I think there should be a robust Federal standard.

Mr. DINGELL. All right, I will ask you to contribute for the record information on that view, if you please.

Ms. RAMIREZ. Yes.

Mr. DINGELL. I ask unanimous consent that that be inserted at the appropriate time.

And thank you, Mr. Chairman.

Now, Madam Chairman, should such a law address notification methods, content requirement, and timeliness requirements? Yes or no?

Ms. RAMIREZ. Yes.

Mr. DINGELL. Wouldn't work very well without that would it?

Ms. RAMIREZ. That is right.

Mr. DINGELL. Now, Madam Chairman, in the event of a data breach, should such a comprehensive data security and breach notification law require companies subject to a breach to provide free credit monitoring services to the affected consumers for a time certain? Yes or no?

Ms. RAMIREZ. Yes, with limited exceptions.

Mr. DINGELL. Do you have authority to do that now?

Ms. RAMIREZ. No.

Mr. DINGELL. Do you need it?

Ms. RAMIREZ. I think it would be appropriate to, again, to impose it as a requirement with limited exceptions.

Mr. DINGELL. Madam Chairman, I note that—well, let's ask this question: Should violation of such law be treated as a violation of a Federal Trade Commission rule promulgated under the Federal Trade Commission Act? Yes or no?

Ms. RAMIREZ. Yes.

Mr. DINGELL. Madam Chairman, would you please submit some additional comments on that point to the record?

Ms. RAMIREZ. Absolutely.

Mr. DINGELL. Now, Madam Chairman, should such a law be enforceable by state attorneys general? Yes or no?

Ms. RAMIREZ. Yes.

Mr. DINGELL. Madam Chairman, should such a law preempt existing State data security, and breach notification laws? Yes or no?

Ms. RAMIREZ. If the standards are robust enough, yes.

Mr. DINGELL. Would you submit some additional information to us on that point, please?

Ms. RAMIREZ. Yes.

Mr. DINGELL. Madam Chairman, given advances in criminal ingenuity which seems to be moving forward almost with the speed of light, as potential in the future, should any statutory definition of the term "personal information" included in a comprehensive

Federal data security and breach notification law be sufficiently broad so as to protect consumers best? Yes or no?

Ms. RAMIREZ. Yes.

Mr. DINGELL. Thank you, Madam Chairman.

Mr. Chairman, I want to thank you for your kindness to me this morning. I urge the committee to work with the Federal Trade Commission to draft and pass a comprehensive Federal data security and breach notification legislation. I believe that this should be done in a bipartisan fashion, and I think that the Democrats and the Republicans can work together for this purpose.

Meanwhile, I would note such legislation is not a panacea for data theft, and hopefully, it will serve to reduce it and better protect consumers.

I again, I thank you, Mr. Chairman, for your courtesy to me, and I appreciate the holding of this hearing.

Madam Chairman, thank you for your courtesy.

Mr. TERRY. Well done, and actually entertaining. So thank you, Mr. Dingell.

Ms. Blackburn, you are now recognized for 5 minutes.

Mrs. BLACKBURN. Thank you, Mr. Chairman. I appreciate that, and thank you all again.

Ms. Ramirez, I think I want to start with you for a minute. You said in your testimony: "Never has the need for legislation been greater."

And so taking that statement, it could mean that the companies who suffered the breaches did not use reasonable measures to protect consumer data. So, if that is your statement then, is the FTC involved in the forensic investigation regarding the Target, Neiman Marcus, Adobe, the hotel chains, all of these breaches?

Ms. RAMIREZ. I am afraid that I can't discuss any particular companies or discuss whether the FTC is involved in any particular investigations, but let me explain what I meant by that statement. I meant it as a general statement reflecting what we are seeing in the marketplace, and that is that companies continue to make very basic mistakes when it comes to data security. And our role at the FTC is to protect consumers and ensure that companies take reasonable and appropriate measures to protect consumer information.

Mrs. BLACKBURN. OK, then let me stop you right there. So you are saying that not due to this group, but because of general, so you are basically reworking your testimony with me on this? It is not that these specific breaches show that there has never been a greater need. So you may want to submit a little bit of clarification there.

Ms. RAMIREZ. I can answer right now if you wish.

Mrs. BLACKBURN. Well no, I want to move on. I have got 3 minutes and 14 seconds and about 5 pages of questions. So submit it.

I also would like you to talk about or to submit to us what is the reasonable standard? You have referenced it several different times, but I have not seen a reasonableness standard in writing, so what are you referencing?

Ms. RAMIREZ. We take a process-based approach to this question. Technology is changing very rapidly. The threats that companies face are also evolving very rapidly, so we think that the appropriate way to proceed in this situation is to focus on whether com-

panies are looking very closely at the threats to which their businesses are exposed, and whether they are setting reasonable program security programs putting those in place.

Mrs. BLACKBURN. OK, why don't we——

Ms. RAMIREZ. If I may, it is a very fact-specific inquiry——

Mrs. BLACKBURN. OK.

Ms. RAMIREZ [continuing]. And I think a reasonableness standard is appropriate.

Mrs. BLACKBURN. I can appreciate that, but I think to use that term repeatedly, what we need to know is what your definition of reasonableness would be.

Mr. Zelvin, let me come to you. You know, we hear the chairman say, well, you are not doing this, you are not doing that. How quickly do the cybercriminals message evolve? You have looked at this for a very long time. So and you sent out updates, you know, daily, weekly, monthly, so how quickly is the evolution of this process?

Mr. ZELVIN. Congresswoman, the evolution is incredibly fast and we are learning with each incident the complexity.

Mrs. BLACKBURN. OK.

Mr. ZELVIN. So they are moving very quickly. They are very sophisticated and we are in a chase to keep up with them.

Mrs. BLACKBURN. OK, Ms. Ramirez, back to you. Another thing, you testified that in a number of the 50 data security cases settled by the FTC, the companies simply and I am quoting you, "Failed to employee available cost-effective security measures to minimize or to reduce the data risk."

So I want you to give us some examples of the kind of measures that the companies failed to use, because you hear from Mr. Zelvin how quickly this evolution is taking place, and the need for flexibility and nimbleness, and then we hear you saying, but you have got to have a standard. And you have got to do this. And we have taken these efforts in the 50 cases we have settled. So for those of us that are looking at what legislation would look like, we have to realize that it has got to be nimble. You are saying you want something, but then you are not giving us specifics or examples of what you think people have failed to do. So I hope you are understanding, we have got a little bit of a gap here. Go ahead.

Ms. RAMIREZ. So let me just say that I think the approach that the FTC recommends for legislation is one of reasonableness. We think that that is an appropriately flexible standard that will allow for nimble action. And to give you an example, as I mentioned in our experience, companies continue to make very simple mistakes when it comes to data security. We also have data that corroborates that and that includes the Verizon data breach report that Mr. Noonan referenced in his opening remarks.

So just to give you a few examples, this can span low-tech, and high-tech mistakes but they could include the failure to use strong passwords, the failure to encrypt personal information, the failure to update security patches, so it is these very basic mistakes that we encounter frequently.

Mrs. BLACKBURN. So it is consumer and not company failures?

Ms. RAMIREZ. No, this would be, I'm referring to company failures.

Mrs. BLACKBURN. You are referring to company failures. OK, thank you.

I yield back.

Mr. TERRY. All right, thank you. And I now recognize the gentleman from Vermont for his 5 minutes.

Mr. WELCH. Thank you, Mr. Chairman.

The technology that we use is not the best, is that correct, Chairwoman Ramirez? I mean, as I understand it, the chip-and-PIN technology is what is now being used in Europe, and it has better success in preventing fraud; is that right?

Ms. RAMIREZ. We don't recommend any particular technology. We think that any legislation ought to be technology neutral. That being said, we certainly would support any steps that are taken at the payment card system end to protect or better protect consumer information.

Mr. WELCH. Well, are we still by and large using 1970s-era magnetic stripe technology, General Madigan, is that your understanding?

Ms. MADIGAN. Yes, that is accurate and so that puts us behind virtually every other country in the world in terms of the security of our payment systems.

Mr. WELCH. All right. So then there is an ability on the part of the card issuers to upgrade the technology to meet basically standards that are being employed in Europe; is that correct?

Ms. MADIGAN. That is correct. And when you look at the amount of fraud losses that these other countries where the chip-and-PIN technology is used, you can see that their levels of fraud have decreased significantly, around 50 percent. So chip-and-PIN technology won't completely eliminate fraud and breaches, but it should significantly curb the amount that we currently see.

Mr. WELCH. That is good. And what I understand now is VISA and MasterCard have announced a roadmap to chip-and-PIN technology for U.S. payment cards. Do you think it would be problematic if VISA and MasterCard decided to abandon the PIN feature on chip cards given that PINs enhance security?

Ms. MADIGAN. I think it makes sense to use PINs, and when there are problems people can obviously change their PINs as they change passwords.

Mr. WELCH. Mr. Noonan, how about you? I mean you have frontline responsibility for trying to maintain the integrity of the system and, obviously, it is extraordinarily important to our merchants, to our banks, and to our consumers.

Mr. NOONAN. Yes, sir, right now currently——

Mr. TERRY. Would you pull the mike a little closer?

Mr. NOONAN. Sure. Currently the Secret Service doesn't have a metric in which to measure chip and PIN, obviously, here in the United States it is not readily used. But however, the Secret Service does support any sort of technology which would assist in the security of that particular data.

Mr. WELCH. But it is your understanding the same as General Madigan's that technology, the chip-and-PIN technology that is widely deployed in Europe has been much more successful in reducing fraud?

Mr. NOONAN. It could give another level of security which again makes it more difficult for the criminals to get at that data. I am not saying, again, that chin and PIN is the solution. Of course, there is not 100 percent solution, technological solution for the problem.

Mr. WELCH. Right, but what it is is a better technology than the 1970s-era magnetic swipe card, correct?

Mr. NOONAN. Sure, it is. The magnetic stripe card is a 30-year technology, sir.

Mr. WELCH. Right. Mr. Zelvin, how about you?

Mr. ZELVIN. Congressman, I agree with Mr. Noonan and the other panelists, but there are other challenges as well.

Mr. WELCH. Right.

Mr. ZELVIN. Now you are using your phones now for payments. You are using your computer, your laptop for payments. But having that extra security on the card itself would be very helpful, but we have to look at other things as well.

Mr. WELCH. All right. I will go back to you, Chairwoman Ramirez. There seems to be some consensus it would be good to have a standard, but we can't pick winners and losers on technology. So what would be sort of a concrete step that Congress would take that would be practical and effective in improving the status quo?

Ms. RAMIREZ. So number one, I think that just the Congress taking action alone would be a very important statement. But what we advocate is that a reasonableness standard be employed along the lines of what the FTC has in place with the Safeguards Rule. And I would be happy to work with the committee on these issues, and my staff is available to do that.

Mr. WELCH. So it sounds like we can't, as a legislative body, prescribe what the best technology is. We have got to let industry figure that out and at least set a higher standard, but on the other hand, you need some flexibility if steps are being taken, or not taken that would enhance security——

Ms. RAMIREZ. Absolutely.

Mr. WELCH [continuing]. For consumers and merchants?

Ms. RAMIREZ. Yes. I think flexibility is important and that is one of the reasons that we are requesting that the FTC have rulemaking authority in order to implement the legislation that would allow the agency to take into account an evolution and changes when it comes to technology.

Mr. WELCH. And would this be helpful in the privacy breaches as well? I mean, thieves are going in to get monetary value, but they are ending up also with Social Security numbers, personal information, things that can be used in identity theft. So the better security, would it not only help with the economic loss, but the identity theft assault? General Madigan, I will ask you.

Ms. MADIGAN. Absolutely, so obviously, what we see is when people's personal information is taken, it is frequently used to commit identity theft. But it can certainly be used, not just financial identity theft, but there are many other types of——

Mr. WELCH. Right.

Ms. MADIGAN [continuing]. Identity theft that take place.

Mr. WELCH. I see my time is up.

I just want to thank this panel. Mr. Chairman, this is a great panel. Thank you for assembling it.

Mr. TERRY. Yes. Thank you.

And I now recognize the gentleman from New Jersey, Mr. Lance, the vice chair.

Mr. LANCE. Thank you, Mr. Chairman.

Mr. Zelvin, a recent Wall Street Journal article reported that the software virus injected into Target's payment card devices couldn't be detected by any known antivirus software; is that accurate?

Mr. ZELVIN. It is, sir.

Mr. LANCE. And could you elaborate on that?

Mr. ZELVIN. Certainly. Most of our detection systems use signatures based, so there are known problems and there is a technical formula we put into a machine that says, hey, you told me to look for this. I found it. In some cases there are intrusion prevention systems that prevent that malicious event from getting to the endpoint. In this case, it looks like the criminals modified it, what was a standard attack for point of sale and modified it in such a way that it is undetectable.

Mr. LANCE. Thank you very much.

Mr. Noonan, you stated that "The Secret Service has observed a marked increase in the quality, the quantity, and the complexity of cyber crimes targeting private industry and critical infrastructure over the decade-long trend of major criminal data breaches."

Can you give us some examples of how these criminals and their tactics have evolved, and I presume these criminals are not necessarily residents or citizens of the United States?

Mr. NOONAN. Yes, sir. So we are talking about a network of transnational cybercriminals.

You know, over time we can look back at the data breaches at T.J. Maxx, we can look at Dave And Busters and the ones that happened back around the era of 2006. And back during that time, the cybercriminal was attacking databases, and unencrypted data.

Mr. LANCE. Yes.

Mr. NOONAN. Which is credit card payments.

Mr. LANCE. Yes.

Mr. NOONAN. That got changed, it morphed in 2007, where the focus ended up going towards credit card processing companies where they were looking at ways to get into the same type of data. But they were looking at credit card data as a pass through credit card processors when it was unencrypted at that time.

So encryption modification has been made now through that system and you know information is now encrypted as it goes in these systems. Today we have seen the change now, they are looking at where the fence is and how to get around that fence. So where they are attacking now is at the point of sale piece, where from the point-of-sale terminal to back of the house server, if you will, that piece of string has not been encrypted.

Mr. LANCE. Thank you.

Mr. NOONAN. So it is happening at that point.

Mr. LANCE. Thank you very much.

Mr. NOONAN. Sure.

Madam Chairwoman, you answered Chairman Emeritus Dingell's questions regarding preemption. I didn't understand your an-

swers; my fault, not your fault. Would you explain in a little more detail your views on preemption, and I come at this having been the minority leader in the New Jersey State Senate and I certainly believe in a robust democracy with protections both here in Washington and at State capitals, and if you could just elaborate briefly on the preemption issue.

Ms. RAMIREZ. Yes, I believe that preemption is appropriate, but provided that the standard that is set is sufficiently strong, and also provided that the States have concurrent ability to enforce.

Mr. LANCE. Concurrent ability. So this——

Ms. RAMIREZ. Yes.

Mr. LANCE [continuing]. Would not mean that the States would not have a significant responsibility in this very complicated and difficult issue?

Ms. RAMIREZ. The States do tremendous work in this area and I think it is vital to have them with jurisdiction to enforce the law.

Mr. LANCE. Thank you.

Attorney General Madigan, it is a pleasure to meet you, and although I do not know you, the New Yorker Magazine has come into our house forever, and your husband is a brilliant cartoonist, and certainly my wife and I enjoy his fine work.

Could you comment on the preemption issue?

Ms. MADIGAN. Obviously——

Mr. TERRY. And could you move your microphone a little closer?

Ms. MADIGAN. Sure.

In terms of preemption, I would concur with what the chairwoman has said. As long as the Federal legislation has strong enough standards and States still retain the ability to enforce, as we do in a number of areas already, we understand that it is potentially reasonable to say, OK, we are going to preempt you in a certain manner.

And in fact, back in 2005 Congress received a letter from the National Association of Attorneys General requesting notification laws be put in place at the National level. And so as long as we still retain the ability to respond to our consumers, and this is looked at in some ways potentially either as a floor, and not a ceiling, we understand your role.

Mr. LANCE. Thank you very much.

Let me say, Mr. Chairman, that I believe that this committee will, in a bipartisan capacity, work on this issue, work to conclusion, and this is the committee in the Congress that deals on these important, nonpartisan, or bipartisan issues, and I have every confidence that we will meet the challenge working with the distinguished panel, working with the next panel, and I look forward to being involved to the greatest extent possible.

Thank you, Mr. Chairman.

Mr. TERRY. Thank you.

And I now recognize the gentleman from Kentucky, Mr. Guthrie for 5 minutes.

Mr. GUTHRIE. Thank you, Mr. Chairman, and I want to thank everybody for coming today. I have a business background, and I know that anytime you have an issue with your customers it takes a long time to build trust back up again.

So I know the incentives are for businesses to protect their data as much as they can, but at the same time, I worked in a retail store when I was in high school. My grandfather had a grocery store and we had nowhere the data that you have to deal with now. Everybody has to deal with data. So we need the right incentives and the right things in place to make sure that is protected. I want to talk to Agent Noonan.

You testified that it is really the victim company that that first discovers the criminal's unauthorized access, and why is that? Are they not paying attention?

Mr. NOONAN. No, sir. For law enforcement and for the Secret Service it is a result of a proactive approach to our law enforcement. While we are out working with sources, we are gathering information. We are working with our private-sector partners specifically in the financial services sector, where we are receiving data, and when we are receiving that data, a lot of times what can occur is we can see a point of compromise, a common point of compromise, whereas the retailer might not necessarily see compromised data that is out in the world.

And by looking at that data, we can go to that victim company, make notification to that company, and advise them that they have a leak. Now, it doesn't necessarily mean it is that company. It can potentially be that company's credit card processing company. It could be their bank, it could be a host of other systems that are hooked into the main company. But it is a point for us to us go to that potential victim and say please look at your data, and see if you have a problem.

Mr. GUTHRIE. That was my question, I guess. So who typically notices the breach first? Is it typically law enforcement who is monitoring this and they see these transactions, or is it all of a sudden one day a retailer starts getting calls from a lot of their credit card companies from a lot of their customers saying hey, I have got these charges. The charges aren't mine, the charges aren't mine, the charges aren't mine. And then it finally figures out what is in common with these people and they went to a certain store? I mean, is that, do you usually find it as it is going through your monitoring or it is people reporting that they have something done to them and you find the commonality or both.

Mr. NOONAN. So to answer your question, both.

Mr. GUTHRIE. Typical, I guess. Both.

Mr. NOONAN. I don't think that there is a typical, if you will.

Mr. GUTHRIE. All right.

Mr. NOONAN. But we do work closely with the banking community, and as banking investigators look at those anomalies and find those anomalies, obviously, they are getting calls from their consumers and saying that there is a problem. They will notice an anomaly, as well as we are targeting different criminals, and in targeting those different criminals we have different sources and we are able to some different things that are happening in the criminal underground. And that is another effective tool that we have at our disposal to be proactive in, sometimes it is notification.

But you have got to realize, in law enforcement under that approach, sometimes we are stopping the occurrence from actually occurring, too. So we might go to a victim, a potential victim com-

pany to allow them to know that they have been compromised and in doing so, we stop the company from losing a single dollar.

Mr. GUTHRIE. Yes the——

Mr. NOONAN. As a result of a proactive approach, that is a very successful method in which law enforcement is a tool for consumers. They are out there out in front looking for that type of behavior.

Mr. GUTHRIE. We certainly appreciate that effort. And Mr. Zelvin, you mentioned the NCCIC's mitigation capabilities were leveraged to coordinate efforts to secure assistance against these attacks. Does the NCCIC provide technical recommendations on how to secure systems?

Mr. ZELVIN. We do, sir. And it is probably the most important part of what we do. So it is not necessarily about finding the fires and putting them out, but preventing them from happening to begin with. So, and I think this is another great example on the point of sale systems. Obviously, these companies had to compromise. Our responsibility is to assist them, but also to let the broader community know what they need to go look for so they can go see if it is on their systems, take it off, and then prevent it from hopefully happening to them as well.

Mr. GUTHRIE. And also you described a product that you recently disseminated to the industry that contains detailed technical analysis, the mitigation recommendations regarding the recent point of sale tax. Can you generally describe what you mean by mitigation recommendations and tell us who develops those recommendations?

Mr. ZELVIN. Certainly, sir.

We work with a cross-section across the Nation with the financial services sector, with technical experts from the manage security services. And so we canvas the Nation as a whole. And then we put out recommendations. In some cases it is as simple as changing your passwords, but there is also patching your systems. And I think the other panel is going to talk about that.

If you just do some of the routine hygiene of cyberspace you are in a far better place. A couple of things, are you using fire walls and antivirus, restricting your Internet access, and disabling remote access. Some of these things are common sense. Some of the things are new as we discover, but regardless, we want to get out as much information as we can to help people defend their networks.

Mr. GUTHRIE. Yes, you even see a place where I buy gas quite often has a little, like of strip of tape that says, if this seal is broken, please notify us to keep people from, where you do the pay at the pump.

And in your testimony, I guess the one thing I just want to point out, and just to let you, I have got about, well, I am about out of time. But you say: "No country, industry, community or individual is immune to the threat."

Mr. TERRY. Five seconds.

Mr. GUTHRIE. So everybody has to be vigilant continuously because nobody is impervious to cyberthreats, right?

Mr. ZELVIN. That would be correct, sir. And I would be happy as elaborate later as needed.

Mr. GUTHRIE. I am sorry, I just ran out of time.

Mr. TERRY. All right. The gentleman's time is expired.

The chair recognizes the gentleman from Texas, Mr. Olson, for 5 minutes.

Mr. OLSON. I thank the chair, and welcome to our witnesses.

If you review the testimony of this panel and the second panel, and combine that information with my career as a naval officer, we are engaged in combat here. It is warfare. In combat, the first thing you do is get the lay of the battlefield. A witness on the second panel names four separate phases of an attack: Infiltration, access to data, propagation, moving around by and as how you want, aggregation for the big package, and then exfiltration, get it out to the black market.

All four steps have to happen, obviously, for a breach to occur. It seems like we force the public sector to focus on exfiltration, the last step; the private sector, at infiltration the first step.

And obviously, if we get to exfiltration we are closing the barn door after the cows have gotten out. Not an effective way to fight this battle.

So my question is first to you, Mr. Zelvin. How can your part of the public sector, the NCCIC, help with all four phases of an attack, not just exfiltration. It seems like you have done some outstanding work with that.

Mr. ZELVIN. Yes, thank you, Congressman.

Where I tried to focus our efforts at the NCCIC and my staff is just getting at that very first phase of the adversaries' actions. We do not want to be the responders. We want to be the prevention mechanisms and protection and mitigation. So unfortunately, a lot of times where we discover challenges is after they have already happened. So what we are hoping to do is just learn from the bad experiences of one or a few to hopefully protect the many.

I would like to highlight that our Industrial Control System CERT, and we are doing more of this with the US–CERT. We are actually doing experimentation to see if we can crack into some boxes, see the vulnerabilities. And we work with the private sector very closely to see where the vulnerabilities are, and then close those doors as quickly as we find them.

Mr. OLSON. Thank you. Mr. Noonan, you as well, sir. You are law enforcement so you are probably, that is your nature. Right at the end of the line there when those events happen. You mention that just by having something out there you can delay some future damages. So is that what you are limited to, or is there something else you can do to attack the other phases?

Mr. NOONAN. So in our investigations, we are pulling evidence out of the crimes that have happened, too, in a reactive approach. But the proactive approach, the former proactive approach to that is we are information sharing. So as we are seeing different tactics, different trends that are happening in these intrusions, we are taking that information and we are sharing that with our partners at the 33 electronic crimes task forces that the Secret Service has set up around the country and internationally, as well as we are taking in information and we are pushing it to Mr. Zelvin's group at the NCCIC. And that information is being pushed out to the sector. So by observing the evidence and sharing what we are finding in

these different intrusions, we are better protecting the bigger infrastructure, if you will.

Mr. OLSON. General Madigan, any comments, ma'am, in law enforcement for Illinois?

Ms. MADIGAN. Well, one of the things I would say in terms of the last two responses is from our perspective there is an enormous amount of work that also needs to be done to educate the public as to how to protect themselves, and so many people have adopted technology so quickly, they are not necessarily putting in place the safeguards and monitoring their accounts, and putting in place transaction alerts so that when these types of breaches occur they can minimize the damage that they have to their finances.

Mr. OLSON. And finally Ms. Ramirez, any comments, Ma'am on——

Ms. RAMIREZ. I will just say that I agree with Attorney General Madigan. This issue is a complex one that requires a multifaceted solution and that includes, again, companies taking appropriate and reasonable measures to protect information, and also of course, consumers also being educated about how what they can do to protect information.

The main point and why I believe that action is really needed today, is that these breaches remind us of how important it is, how important this issue is, and given the amount of personal information that is being collected from consumers and used and retained, this is truly critically important.

Mr. OLSON. Thank you.

One final question for you, General Madigan. A legal question, I am curious. I went to law school at the University of Texas, passed the bar, never practiced, but I am concerned and wonder, why did you announce publicly the investigation of Target, but not Neiman Marcus. Any reason why that——

Ms. MADIGAN. We announced both of them.

Mr. OLSON. Both, OK. I thought you just announced Target, so thanks for the clarification.

I yield back.

Mr. TERRY. Thank you.

The chair now recognizes the gentleman from Kansas, Mr. Pompeo, for 5 minutes.

Mr. POMPEO. Thank you, Mr. Chairman. I am not quite as sanguine that we are in a place where we are quite ready to move down this path. I am glad we are having this hearing, but we often, when the New York Times gets wound up we in Congress sometimes react in ways that I think are inappropriate to the true challenge. And I want to talk about that for just a second.

Ms. Ramirez, typically we regulate when there is a market failure. That is the reason the Federal Government would come in and regulate in this space is because we don't think that private actions can respond to a particular concern or threat in an appropriate way. I can understand the potential justification for notification because sometimes someone might not know that their material had been stolen, so I can understand a potential justification for regulating with respect to notification.

Why is it the case that consumers can't figure out that if they are not happy with Target or Neiman Marcus, or whomever it is

allowed their data to be stolen, that they wouldn't migrate somewhere else? Why is it the consumers won't analyze the risk of their data being stolen and respond appropriately without the Federal Government stepping into try and regulate?

Ms. RAMIREZ. I don't believe that the burden should be placed on consumers when it comes to this issue.

Mr. POMPEO. Why is that, Ms. Ramirez? We do that in so many other places. If you think your material is going to be stolen from your home, you can buy a home security system. We have lots of places where there are risks to our private property, and we allow consumers to step in and decide if they want to pay $60 a month, $200 a month, or $1,000 a month for their own security.

Ms. RAMIREZ. I think consumers do have a role to play here, as I mentioned earlier. I think there are steps that consumers can take to be vigilant in this area, but I believe the role of the FTC is to protect consumers. And when you look back at the data that is available and that is out there, and it is also consistent with our experience, let me cite specifically the Verizon data breach report. They have an annual report that studies what is happening in the area of data security, and that information tells us that companies continue to make very fundamental mistakes when it comes to data security. They are not taking the reasonable and necessary steps that they need to in order to protect the consumer information that they collect, use, and retain.

Mr. POMPEO. I appreciate that, and that report is there, and consumers might choose not to pick Verizon as a direct result of that. I think we ought to make sure we appreciate that.

Attorney General Madigan, do you have data that tells you when folks call in, how much they are prepared to pay for protection? That is, if they call and say, my data was stolen. Do you know how much they are prepared to pay per incident? Will they only bay $0.50 or $5 million to protect their data? Do you have an analysis of what——

Ms. MADIGAN. We don't and we——

Mr. POMPEO. Because you said consumers are panic and angered.

Ms. MADIGAN. Right.

Mr. POMPEO. I would presume that they are prepared to take some of their hard-earned money to protect themselves. Do you have data with respect to that?

Ms. MADIGAN. I can tell you that we have had $26 million worth of fraudulent charges removed from Illinois residents' accounts. And I can tell you based on the 34,224 people we have had to work through to do that with, on average, these individuals have lost or at least not lost, but had $762 in fraudulent account amounts removed.

So I haven't asked them how much they would like to pay for security. They feel as if they are having to actually pay the price simply for engaging in everyday activity whether it is commercial activity, or interacting with the government, or being provided with medical services.

Mr. POMPEO. Do you think if we head down the path that you are proposing that they ultimately won't pay for that, that these costs won't be borne by consumers ultimately?

Ms. MADIGAN. I know that costs are going to be borne by consumers, absolutely.

Mr. POMPEO. So might it not at be least an idea we should consider to have them pay for that directly so they can see those costs, and they respond appropriately, as opposed to having them removed from their bills, or have the Federal Government mask that real cost to them so they don't really know the risk that they are presenting by particular use of their own data?

Ms. MADIGAN. I am not exactly sure the scheme you are trying to propose here, but you are correct in the sense that if we are going to update, for instance, credit card technology to adopt chips-and-PINs, obviously, consumers are going to pay an increased cost. Retailers, they are going to pay in terms of increased costs and fees at their banking institutions. So consumers will pay and hopefully we will be able to improve our security.

Mr. POMPEO. Thirty seconds. I am going to try two yes or no questions. Do you think that there should be private rights of actions associated with these rules as well?

Ms. MADIGAN. At this point we have been able to handle these at the State level.

Mr. POMPEO. Great. And then you made a statement. You said, in fact I will quote, "Nearly ever other country in the world is ahead of us."

Surely, you don't mean Niger.

Ms. MADIGAN. There may be several African countries that——

Mr. POMPEO. I just came back from Europe and I will tell you, they think our system is pretty good here, too. They are very comfortable doing business across Asia, Europe, and North America. And so I actually think our system may not be as dire a situation as has been suggested this morning.

I yield back.

Mr. TERRY. Thank you.

I now recognize the gentleman from Ohio, Mr. Johnson for 5 minutes.

Mr. JOHNSON. Thank you, Mr. Chairman, and I, again, want to thank you folks for being here today.

I am very concerned about the increase and the sophistication of the cyberattacks. And just to kind of get your opinion on it, Mr. Noonan, how does the increasing level of collaboration among cybercriminals that you referenced increase the potential harm to companies and consumers?

Mr. NOONAN. So the increasing collaboration between cybercriminals just increases their capabilities, so when we say that there is collaboration between these groups, these are loosely-affiliated organized criminal groups that are doing this. I have used the analogy of Oceans 11, of what this group and what this network does.

So they have groups that will do infiltration into the system to gain access. They have other people that will design malware. They have people that go and map the different network to figure out exactly how to get through the networks. There is exfiltration of data that occurs in these situations as well, and there is monetization so that data that is stolen has to be sold. And then, of course there is money laundering, the movement of money. So when you bring

together a coordinated group of sophisticated criminals, it does, it is a, you know, they will find the edge of the fence and perpetrate our system.

Mr. JOHNSON. Now, once we identify who these folks are that are perpetrating these attacks, well, first of all, are they State side, or are they overseas for the most part?

Mr. NOONAN. The majority of the criminals that we are looking at are transnational criminals.

Mr. JOHNSON. OK, so outside of the United States.

Mr. NOONAN. Yes, sir.

Mr. JOHNSON. OK. To what degree do we have the authority to go after those folks when we identify them?

Mr. NOONAN. Sure.

Mr. JOHNSON. And do you know of any ongoing actions to shut them down?

Mr. NOONAN. Sure. The Secret Service actually has a unique history of success in this area. We have brought many of these different perpetrators to justice. I mean, we go back and talk about the TJX investigation as well as many others. But in the TJX investigation, we were successful. We arrested domestically in this case, Albert Gonzales. He is sentenced to 20 years in prison here in the United States.

We, also in the summer of 2012, we arrested Dimitri Salience and Vladimir Drinkman, responsible also in that investigation over in the Netherlands. We were able to bring to justice Aleksandr Suvorov in the Dave And Busters case where he was sentenced to 7 years in prison here domestically. We also were able to pick up three different Romanian hackers that were responsible for the Subway sandwich shop intrusions that occurred in 2008, and we have brought them to justice, where the main leader was sentenced to 15 years in prison.

We have a rich history of being able to effectively identify who these targets are, have them arrested, and work with our international partners. We have a host of international offices, and international working groups, and I think it comes back to the relationships that we build internationally that are assisting us in bringing these different actors to justice.

Mr. JOHNSON. Well, obviously, most developed nations that have a high degree of sophistication within their networks, they are vulnerable to these things as well. So how robust are our agreements with other nations to go after the criminals that might reside in their countries?

Mr. NOONAN. Absolutely, sir, we do. We have many different agreements with numerous other countries over in Europe, and we have been working successfully in partnering with those. We worked very closely with the British, with the National Crime Agency, in the Netherlands with the Dutch High Tech Crime Unit. In German we the BKA. We have working groups in the Ukraine, as well as an office that we established not too long ago in Estonia. So it is through that host of relationships, and in the laws that we are enforcing with them, that we are able to gather some success in those areas.

Mr. JOHNSON. Good. Mr. Zelvin, you testified that no country, industry, community, or individual is immune to threat of a

cyberattack. Does this mean, in your opinion, that you believe no one can be impervious to cyberattacks?

Mr. ZELVIN. Sir, I think it is one of those challenges that it is like trying to prevent automobile deaths. You can do a lot of things, but ultimately unfortunately, people may still pass. I think there is a lot more we can do and should do, but ultimately, I believe there will be vulnerabilities that unfortunately will be exploited by very sophisticated actors.

Mr. TERRY. Thank you, Mr. Johnson.

At this time I recognize the gentleman from Mississippi, Mr. Harper for 5 minutes.

Mr. HARPER. Thank you, Mr. Chairman, and thank each of you for being here.

And if I may start with you Agent Noonan, I know this is obviously ongoing investigations here, but do you have an early indication, without revealing anything you shouldn't as to how you think this might have been prevented?

Mr. NOONAN. Again, I don't think it comes back to how it could have been potentially prevented. I think what the important part here is that we know that this is a sophisticated criminal group. The different companies, they had a plan, I think is the important takeaway here. The response plan is something that every company should also think of. We shouldn't think of if this is going to happen.

We should potentially think when this potentially may happen to them. So a response plan is one in which you incorporate law enforcement into your response plan. And it brought back the information sharing piece. If you don't incorporate law enforcement in your plan to help you find and mitigate the problem, and then share that information with the whole of government, with the infrastructure to better protect other infrastructure, that is not necessarily a good plan.

We obviously would like to see companies have robust forensic companies assigned to them so that when an intrusion does happen, they are able to go in and effectively quickly mitigate it so that there is no longer any bleeding that were to occur.

Additionally, counsel is important for them to have, and then also a plan for notification to victims. Again, those are the important takeaways that we see in this case.

Mr. HARPER. And are you satisfied in these cases that the response has been satisfactory?

Mr. NOONAN. Yes, sir.

Mr. HARPER. OK, thank you.

Mr. NOONAN. Thank you.

Mr. HARPER. Chairwoman Ramirez, if I may ask you a few questions.

Is there overlap between FTC's Safeguards Rule, and the PCI data security standards and do the PCI standards incorporate provisions of the Safeguards Rule, or do they go beyond the Safeguards Rule. Can you shed a little light on that?

Ms. RAMIREZ. Sure. I am happy to speak to this. The way the FTC approaches its data security enforcement work is that we, again, we impose a reasonableness standard so we don't mandate or prescribe any specific standard or technology, but we think that

as a matter of course, a company should of course, look to relevant industry standards, best practices in evaluating what measures they should have in place.

Mr. HARPER. OK, would the PCI data security standards meet the reasonable standards for purposes of Section 5 of the FTC act?

Ms. RAMIREZ. Every case that we look at is really a fact-specific one, so I really can't comment on hypotheticals. But what I can tell you is that a company should of course be looking to industry standards. They can be very valuable, and that would be certainly one factor that we would examine in looking at any matter.

Mr. HARPER. You know, you make the point that the mere fact that breaches occur does not mean a company violated the law, and the companies need not have perfect security. Yet, we have been told that it is unlikely any company subject to the PCI standards that suffers a breach would be found to be 100 percent compliant at the time of the breach. While the PCI standards provide an admirable and needed push to keep companies vigilant, would there be problems of making that a Federal Standard enforceable by the FTC if it is setting up businesses to fail because it is often possible to find some violation of the standards?

Ms. RAMIREZ. Again, we are going to be looking at each situation, in a fact-specific way. We certainly understand that there is no perfect solution. Security will not be perfect. We have many more investigations than we do actual enforcement cases.

Mr. HARPER. How many cases has the Commission brought for violation of Safeguards Rule?

Ms. RAMIREZ. Of the Safeguards Rule specifically, we have brought approximately a dozen cases.

Mr. HARPER. Has industry compliance improved over time as the rule becomes more mature and the industry becomes more familiar with it?

Ms. RAMIREZ. Generally speaking, and I am speaking broadly, we continue to see basic failures when it comes to data security and the data that we have available to us suggests the companies do need to do more in this area.

Mr. HARPER. OK, I yield back.

Mr. TERRY. Thank you.

At this time, we recognize the gentleman from Florida, Mr. Bilirakis, for 5 minutes.

Mr. BILIRAKIS. Thank you, Mr. Chairman, I appreciate it very much and I thank the panel for their testimony.

This is for the entire panel. Data often moves without respect to borders, as you know. Mr. Russo notes in his testimony that championing stronger law enforcement efforts worldwide can improve payment data security.

Mr. Noonan, in your testimony, you mentioned successful cooperation with law enforcement entities during investigations into these cybercrimes. Would you, as well as Mr. Zelvin expand on what you believe Congress can do to enhance those international efforts going forward? Is there a role for examination of this issue, and future trade discussions such as the Transatlantic Trade and Investment Partnership?

Mr. NOONAN. I would recommend the continued support for our efforts in our international field offices, as well as the other work-

ing groups in which we are placing strategically around the world. We have had a lot of great success in some of those Eastern European countries. Within the last 2 years, we have had some great successes. We have had an extradition of a Romanian citizen from Romania to the United States based on the collaboration that we have made here between Romanian authorities and U.S. authorities.

A big part of that is the relationships that the DOJ has also expanded in those different countries. The computer crimes, intellectual property section, CCIPS as well as the Office of International Affairs, have helped us in strategically working with those different countries to bring criminals that are affecting us here domestically to justice.

Mr. BILIRAKIS. Thank you.

Mr. Zelvin, you are welcome to——

Mr. ZELVIN. Yes, sir.

My organization is neither a law enforcement, nor an intelligence organization. We are purely civilian, and we have a relationship with over 200-like CERTS around the world. So it is really a technical-to-technical exchange.

Last week I was in Tel Aviv and in London and I will tell you, I got to really see firsthand where our counterparts are, and they are making extraordinary progress but in many cases we in the United States are leading the way especially in the Government's role in cybersecurity.

So I think a continued engagement, because as Mr. Noonan had said, many of these threats are coming from overseas. Many come from within our own countries, but it would be far better if we could engage with our international partners and have them use their legal means to go after these threats, and then also provide an ability to cooperate with us such as when we find an intrusion in their country to get them to shut it down if they have the legal ability.

Mr. BILIRAKIS. Thank you.

Anyone else like to comment on that?

Ms. RAMIREZ. Just briefly, if I may.

I think the international cooperation is a very important dimension of this issue. And we engage with international counterparts in all of the work, all of the enforcement work that we do, and this would be among them.

Mr. BILIRAKIS. Thank you. Thank you very much.

The next question for Chairwoman Ramirez. I represent Florida's 12th congressional district. While more and more seniors are becoming technologically adept, how would you recommend notifying seniors of a data breach in a timely manner if they are not reachable by email?

Ms. RAMIREZ. I think it is an issue that I am happy to work with you on. I think seniors are increasingly becoming more adept at email, but of course, if email is not an option then mail notification would be appropriate, but we are happy to work with the committee on addressing this and other issues.

We do look and have recently held a workshop on issues relating to senior ID theft and understand that this population can be particularly vulnerable to these set of issues so I think mail notifica-

tion would be the, you know, one option, but there may be other ideas and we would be happy to discuss those with you.

Mr. BILIRAKIS. Yes, I would like to work with you on that. Thank you very much.

I appreciate it and I yield back.

Mr. TERRY. Thank you.

At this time the gentleman from West Virginia is recognized for 5 minutes.

Mr. MCKINLEY. Thank you, Mr. Chairman.

I think we are going to have to go through an awful lot of information that is being shared here today so I want to switch horses. I think we have got something that we can chew on for a little bit.

So I want to switch horses a little bit to understand a little bit about what is happening with the data security with the Affordable Care Act, if I could. To what level so to Mr. Noonan, Mr. Zelvin, if you could participate with this, maybe you can help me.

In December the HHS has reported that there were 32 security incidents. Maybe you could say slash breaches have occurred with Obamacare. Were the individuals notified? Do you know whether or not the individuals were notified?

Mr. ZELVIN. Congressman, I apologize. I am not familiar with that. If we can take that for the record, we can get back to you.

Mr. MCKINLEY. If you would, please.

Mr. Noonan, do you know anything about those breach that occurred with Obamacare?

Mr. NOONAN. And the same thing with me, sir. I don't have any knowledge of those breaches right now.

Mr. MCKINLEY. OK. If they were given the standard that we have imposed on the private sector, should individuals be notified if there are breaches with Federal healthcare? Just your opinion.

Mr. ZELVIN. Yes, sir, if there are breaches they should be reported and people should have the opportunity to know about that, and then also take the adequate precautions.

Mr. MCKINLEY. Mr. Noonan.

Mr. NOONAN. Yes, sir, I would concur as well.

Mr. MCKINLEY. You would agree with that.

There is also a report that came out that some of the software that was developed for the Obamacare, was developed in Belarus, and there are reports that there may be some concern for malware being included in that. Where are we in that evaluation because, obviously, the people are still signing up and we may have something that is contaminating our system. Can any of you share with us what is going on internationally on this?

Mr. ZELVIN. Congressman, I can tell you what I know from last night, and from this morning things may have changed. But the intelligence product that was on that report has been withdrawn and is being reevaluated. I believe the White House did a statement last night saying that there is no evidence that there has been any Belarusian software development in the HHS. But HHS is looking at this carefully, and verifying that. So I believe that is where we are right now.

Mr. MCKINLEY. It just may have been someone just——

Mr. ZELVIN. Well, there is something in a report that is being re-evaluated. And so I think there is some more investigation to be done before reaching conclusions.

Mr. MCKINLEY. Could you get back to us then on that and let us know whether or not there is anything. I didn't understand why we were having any of our software developed in Belarus anyway, so, if there is something you can share with us, I would sure like to understand that.

Mr. ZELVIN. Absolutely, Congressman. To the best of my knowledge right now, there was no software that was developed in Belarus.

Mr. MCKINLEY. OK.

Mr. ZELVIN. And HHS is looking at it closely.

Mr. MCKINLEY. Thank you.

For Illinois, I can't see your name tag from here on the thing, but ma'am, could you, has the state of Illinois ever had a data breach?

Ms. MADIGAN. Yes. And in fact in our law, there is a requirement that state agencies notify individuals when their personal information has been compromised.

Mr. MCKINLEY. Do you use some kind of encryption extensively? Do you have some encryption that you use for your data?

Ms. MADIGAN. Different agencies will handle it different ways, but they are all requirements in terms of how data is handled for state agencies.

Mr. MCKINLEY. OK. Thank you very much.

I yield back the balance of my time.

Mr. TERRY. Thank you for yielding back.

No other members are here; therefore, that ends panel number one. I do want to follow up.

So, the talk about the criminal syndicate, there was a story that there was an 18-year old Russian boy that developed this in his basement, this malware; is that accurate?

Mr. NOONAN. Sir, don't believe everything you see in the media, please.

Mr. TERRY. I have learned that, too.

All right. Thank you. The first panel is dismissed, and we thank you. We may have questions submitted to you. We will have those to you within about 14 days if there are any, and we would appreciate about a 14-day turnaround in answers. Thank you.

We will give a few minutes break here so we can get some water or something, and then we will be ready for our panel, second panel.

[Recess.]

Mr. TERRY. Well, since everyone's seated, let's go.

So, I apologize. I was hopeful that that first panel would not last this long, but it did. So thank you, and I hope that doesn't impact your rest of the schedule for the day, but appreciate you staying around.

So, our second panel of the day is the nongovernment panel. We have Michael Kingston, senior vice president and chief information officer of Neiman Marcus Group, then John Mulligan, executive vice president and chief financial officer, Target Brands, Incorporated, Bob Russo, general manager of PCI Security Standards

Council, and then Phillip Smith, senior vice president for Trustwave. Thank you all for being here today.

As we did with the first panel, we will go from my left. So, Mr. Mulligan, you will start and you will have 5 minutes.

STATEMENTS OF MICHAEL KINGSTON, SENIOR VICE PRESIDENT & CHIEF INFORMATION OFFICER, THE NEIMAN MARCUS GROUP; JOHN J. MULLIGAN, EXECUTIVE VICE PRESIDENT & CHIEF FINANCIAL OFFICER, TARGET BRANDS INCORPORATED; BOB RUSSO, GENERAL MANAGER, PCI SECURITY STANDARDS COUNCIL, LLC; AND PHILLIP J. SMITH, SENIOR VICE PRESIDENT, TRUSTWAVE

STATEMENT OF JOHN J. MULLIGAN

Mr. MULLIGAN. Good morning, Chairman Terry, Ranking Member Schakowsky, and members of the subcommittee.

My name is John Mulligan. I am 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 recently experienced a data breach resulting from a criminal attack on our systems. To begin with, let me say how deeply sorry we are for the impact this incident has had on our guests, your constituents.

We know this breach has shaken their confidence in Target, and we are determined to work very hard to earn it back. At Target, we take our responsibility to our guests very seriously, and this attack has only strengthened our resolve. We will learn from this incident, and as a result, we hope to make Target and our industry more secure for consumers in the future.

I would now like to explain the events of the breach as I currently understand them. Please recognize that I may not be able to provide specifics on certain matters because the criminal and forensic investigations remain active and ongoing. We are working closely with the Secret Service and the Department of Justice on the investigation to help them bring to justice the criminals who committed this wide scale attack on Target, American business, and consumers.

On the evening of December 12th, we were notified by the Justice Department of suspicious activity involving payment cards used at Target stores. We immediately started an internal investigation. On December 13th, we met with the Justice Department and Secret Service. On December 14th, we hired an independent team of experts to lead a thorough forensics investigation. On December 15th, we confirmed that criminals had infiltrated our system, had installed malware on our point of sale network, and had 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 notify our guests and equipping our call centers and stores with the necessary information and resources to address the concerns of our guests. Our actions leading up to our public announcement on December 19th and since have been guided by the principle of serving all guests, and we have

been moving as quickly as possible to share accurate and actionable information with the public.

What we know today is that 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. We believe the payment card data was accessed through malware placed on our point of sale registers. The malware was designed to capture the payment card data that resides on the magnetic strip prior to its inscription within our systems.

From the outset, our response to the breach has been focused on supporting our guests and strengthening our security. In addition to the immediate steps I already described, we are taking the following concrete actions.

First, we are undertaking an end-to-end forensic review of our entire network and will make security enhancements as appropriate.

Second, we increased fraud detection for our Target Red Card guests. To date, we have not seen any fraud on our proprietary credit and debit cards due to this breach, and we have only seen a very low amount of additional fraud on our Target Visa card.

Third, we are reissuing new Target credit and debit cards immediately to any guest who requests one.

Fourth, we are offering 1 year of free credit monitoring and identity theft protection to anyone who has ever shopped in our U.S. Target stores.

Fifth, we informed our guests that they have zero liability for any fraudulent charges on their cards arising from this incident, and sixth, Target is accelerating our investment in chip technology for our Target Red Cards and our stores point of sale terminals.

For many years, Target has invested significant capital and resources in security technology, personnel, and processes. We had in place multiple layers of protection, including firewalls, malware detection, intruding detection and prevention capabilities, and data loss prevention tools, but the unfortunate reality is that we suffered a breach. All businesses and their customers are facing increasingly sophisticated threats from cyber criminals. In fact, news reports have indicated that several other companies have been subjected to similar attacks.

To prevent this from happening again, none of us can go it alone. We need to work together. Updating payment card technology and strengthening protections for American consumers is a shared responsibility and requires a collective and coordinated response. On behalf of Target, I am committing that we will be an active part of the solution.

Members of the subcommittee, I want to once again reiterate how sorry we are for the impact of this incident has had on your constituents, our guests, and how committed we are to making it right.

Thank you for your time today.

Mr. TERRY. Thank you.

[The prepared statement of Mr. Mulligan follows:]

WRITTEN TESTIMONY

BEFORE THE

HOUSE COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

HEARING ON

PROTECTING CONSUMER INFORMATION: CAN DATA BREACHES BE PREVENTED?

FEBRUARY 5, 2014

TESTIMONY OF

JOHN MULLIGAN

EXECUTIVE VICE PRESIDENT AND CHIEF FINANCIAL OFFICER

TARGET

I. Introduction

Good morning Chairman Terry, Ranking Member Schakowsky, and Members of the Subcommittee. 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 recently experienced a data breach resulting from a criminal attack on our systems. To begin, I want to say how deeply sorry we are for the impact this incident has had on our guests – your constituents. We know this breach has shaken their confidence in Target, and we are determined to work very hard to earn it back.

At Target we take our responsibility to our guests very seriously, and this attack has only strengthened our resolve. We will learn from this incident and as a result, we hope to make Target, and our industry, more secure for consumers in the future.

I'd now like to explain the events of the breach as I currently understand them. Please recognize that I may not be able to provide specifics on certain matters because the criminal and forensic investigations remain active and ongoing. We are working closely with the U.S. Secret Service and the U.S. Department of Justice on the investigation – to help them bring to justice the criminals who perpetrated this wide-scale attack on Target, American business and consumers.

II. What We Know

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 the Secret Service. On December 14, we hired an independent team of experts to lead a thorough forensic investigation.

On December 15, we confirmed that criminals had infiltrated our system, had installed malware on our point-of-sale network and had 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 our call centers and stores with the necessary information and resources to address the concerns of our guests.

On December 18 we disabled malware on about 25 additional registers which were disconnected from our system when we completed the initial malware removal on December 15. As a result, we determined that fewer than 150 additional guest accounts were affected.

Our actions leading up to our public announcement on December 19 – and since – have been guided by the principle of serving our guests, and we have been moving as quickly as possible 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, email, prominent notices on our website, and social media channels.

What we know today is that 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 partial personal data included name, mailing address, phone number or email address.

We now know that the intruder stole a vendor's credentials to access our system and place malware on our point-of-sale registers. The malware was designed to capture payment card data from the magnetic strip of credit and debit cards prior to encryption within our system.

As the forensic investigation continued, we learned that the malware also captured some strongly encrypted PIN data. We publicly shared this information on December 27, reassuring our guests that they would not be responsible for any fraudulent charges that may occur as a result of the breach.

When we subsequently confirmed the theft of partial personal data on January 9, we used various channels of communication to notify our guests on January 10 and provide them with tips to guard against possible scams.

III. Protecting Our Guests

From the outset, our response to the breach has been focused on supporting our guests and strengthening our security. In addition to the immediate actions I already described, we are taking the following concrete actions:

- First, we are undertaking an end-to-end review of our entire network and will make security enhancements, as appropriate.
- Second, we increased fraud detection for our Target REDcard guests. To date, we have not seen any fraud on our Target proprietary credit and debit cards due to this breach. And we have seen only a very low amount of additional fraud on our Target Visa card.

- Third, we are reissuing new Target credit or debit cards immediately to any guest who requests one.
- Fourth, we are offering 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 highly trained fraud resolution agent.
- Fifth, we informed our guests that they have zero liability for any fraudulent charges on their cards arising from this incident. We encouraged them to monitor their accounts and promptly alert either Target or their issuing bank of any suspicious activity.
- Sixth, Target is accelerating our investment in chip technology for our Target REDcards and stores' point-of-sale terminals. We believe that chip-enabled technologies are critical to providing enhanced protection for consumers, which is why we are a founding, and steering committee, member of the EMV Migration Forum at the SmartCard Alliance.
- Seventh, Target initiated the creation of, and is investing $5 million in, a campaign with Better Business Bureau, the National Cyber Security Alliance and the National Cyber-Forensics & Training Alliance to advance public education around cybersecurity and the dangers of consumer scams.
- And, eighth, last week Target helped launch a retail industry Cybersecurity and Data Privacy Initiative that will be focused on informing public dialogue and enhancing practices related to cybersecurity, improved payment security and consumer privacy. Target will be an active leader in this effort.

For many years, Target has invested significant capital and resources in security technology, personnel and processes. We had in place multiple layers of protection, including

firewalls, malware detection software, intrusion detection and prevention capabilities and data loss prevention tools. We perform internal and external validation and benchmarking assessments. And, as recently as September 2013, our systems were certified as compliant with the Payment Card Industry Data Security Standards.

But, the unfortunate reality is that we suffered a breach, and all businesses – and their customers -- are facing increasingly sophisticated threats from cyber criminals. In fact, recent news reports have indicated that several other companies have been subjected to similar attacks.

IV. Moving Forward

To prevent this from happening again, none of us can go it alone. We need to work together.

Updating payment card technology and strengthening protections for American consumers is a shared responsibility and requires a collective and coordinated response. On behalf of Target, I am committing that we will be an active part of that solution.

Members of the Subcommittee -- to each of you, and to all of your constituents and our guests, I want to say once again how sorry we are that this has happened. We will work with you, the business community, and other thought leaders to find effective solutions to this ongoing and pervasive challenge. Thank you very much for your time today.

Mr. Kingston, you are now recognized for 5 minutes.

STATEMENT OF MICHAEL KINGSTON

Mr. KINGSTON. Chairman Terry, Ranking Member Schakowsky, members of the subcommittee.

Good morning, my name is Michael Kingston, and I am the chief information officer at Neiman Marcus Group. I want to thank you for your invitation to appear today to share with you our experiences regarding the recent criminal cybersecurity incident at our company. I have submitted a longer written statement and appreciate the opportunity to make some brief opening remarks.

We are in the midst of an ongoing forensic investigation that has revealed a cyber attack using very sophisticated malware. From the moment I learned there might be compromise of payment card information involving our company, I have personally led the effort to ensure that we were acting swiftly, thoroughly, and responsibly to determine whether such a compromise had occurred, to protect our customers and the security of our systems, and to assist law enforcement in capturing the criminals. Because our investigation is ongoing, I may be limited in my ability to speak definitively or with specificity on some issues, and there may be some questions to which I do not have the answers. Nevertheless, it is important to us as a company to make ourselves available to you to provide whatever information we can to assist you in your important work.

Our company was founded 107 years ago. One of our founding principles is based on delivering exceptional service to our customers, in building long lasting relationships with them that have spanned generations. We take this commitment to our customers very seriously. It is part of who we are and what we do daily to distinguish ourselves from other retailers. We have never before been subjected to any sort of significant cybersecurity intrusion, so we have been particularly disturbed by this incident.

For our ongoing forensic investigation, we have learned that the malware which penetrated our system was exceedingly sophisticated, a conclusion the Secret Service has confirmed. A recent report prepared by the Secret Service crystallized the problem when they concluded that a specific type of malware comparable and perhaps even less sophisticated than the one in our case, according to our investigators, had a zero percent detection rate by antivirus software. The malware was evidently able to capture payment card data in realtime after a card was swiped and had sophisticated features that made it particularly difficult to detect, including some that were specifically customized to evade our multi-layered security architecture that provided strong protection of our systems and customer data.

Because of the malware sophisticated anti-detection devices, we did not learn that we had an actual problem in our computer system until January 2nd, and it was not until January 6th when the malware and its outputs had been disassembled and decrypted enough that we were able to determine that it was able to operate in our systems. Then, disabling it to ensure it was not still operating took until January 10th. That day we sent our first notices to customers potentially affected and made widely reported public

statements describing what we knew at that point about this incident.

Simply put, prior to January 2nd, despite our immediate efforts to have two separate firms of forensic investigators dig into our systems and attempt to find any data security compromise, no data security compromise in our systems have been identified.

Based on the current state of evidence and the ongoing investigation, one, it now appears that the customer information that was potentially exposed to the malware was payment card information from transactions in 77 of our 85 stores between July 15th and October 30th, 2013, at different periods of time within this date range in each store.

Two, the number of payment cards used at all stores during this period was approximately 1.1 million. This is the maximum number of accounts potentially exposed to the malware, although the actual number appears to be lower since the malware was not active every day at every store during this period.

Three, we have no identification that transactions on our Web sites or at our restaurants were compromised. Four, PIN data was not compromised as we do not have PIN pads and we do not request PINs. And five, there is no indication that Social Security numbers or other personal information were exposed in any way.

We have also offered to any customer who shopped with us in the last year at either Neiman Marcus Group stores or Web sites, whether their card was exposed to the malware or not, 1 year of free credit monitoring and identity theft insurance. We will continue to provide the excellent service to our customers that is our hallmark, and I know that the way we responded to the situation is consistent with that commitment.

Thank you for your invitation to testify today, and I look forward to answering your questions.

Mr. TERRY. Thank you.

[The prepared statement of Mr. Kingston follows:]

Written Testimony of Michael R. Kingston
Senior Vice President & Chief Information Officer, Neiman Marcus Group

Before the House Committee on Energy & Commerce
Subcommitee on Commerce, Manufacturing, and Trade
February 5, 2014

Chairman Terry, Ranking Member Schakowsky, members of the Subcommittee, I want to thank you for your invitation to appear today to share with you our experiences regarding the recent criminal cybersecurity incident at our company.

For over 20 years, I have held numerous positions in the information technology field, and since April 2012 I have been proud to serve as Chief Information Officer of Neiman Marcus Group. We are in the midst of an ongoing forensic investigation that has revealed a cyber attack using very sophisticated malware. From the moment I learned that there might be a compromise of payment card information at our company, I have personally led the effort, in conjunction with others in senior management, outside consultants, and counsel, to ensure that we were acting swiftly, thoroughly, and responsibly to determine whether such a compromise had occurred, to protect our customers and the security of our systems, and to assist law enforcement in capturing the criminals. Because our investigation is ongoing, I may be limited in my ability to speak definitively or with specificity on some issues, and there may be some questions to which I do not have the answers. Nevertheless, it is important to us as a company to make ourselves available to you to provide whatever information we can, as you attempt to address this important problem that confronts so many corporate and governmental entities around the world.

Introduction

Our company was founded 107 years ago. One of our founding principles is based on delivering exceptional service to our customers and building long lasting relationships with them that have spanned generations. We take this commitment to our customers very seriously. It is part of who we are and what we do daily to distinguish ourselves from other retailers.

We have never before been subjected to any sort of significant cybersecurity intrusion, so we have been particularly disturbed by this incident. It is clear that we are not alone, and that numerous retailers and others in the United States have been recently subjected to sophisticated attacks on their computer systems in an attempt to steal their customers' payment card

information. The problem is clearly widespread. And the sophistication of these unprecedented cyber attacks makes the problem very challenging.

Through our ongoing forensic investigation, we have learned that the malware which penetrated our system was exceedingly sophisticated, a conclusion the Secret Service has confirmed with us. The malware was evidently able to capture payment card data in real time right after a card was swiped, and had sophisticated features that made it particularly difficult to detect. These features included some that were specifically customized to evade our multi-layered security architecture that provided strong protection of our systems and customer data. Our security measures included numerous firewalls at the corporate and store level, network segmentation, a customized tokenization tool, numerous encryption methods, an intrusion detection system, a two-factor authentication requirement, and use of industry-standard and centrally-managed enterprise anti-virus software. However, no system – no matter how sophisticated – is completely immune from cyber attack. A recent report prepared by the Secret Service and others in federal law enforcement crystallized the problem when they concluded that comparable RAM scraping malware (perhaps less sophisticated than the one in our case, according to our investigators) had a *zero percent* anti-virus detection rate.

Because of the malware's sophisticated anti-detection devices, we did not learn that we had an actual problem in our computer system until ***January 2***, and it was not until ***January 6*** when the malware and its outputs had been disassembled and decrypted enough that we were able to determine how it operated. Then, disabling it to ensure it was not still operating took until ***January 10***. That day we sent out our first notices to customers potentially affected and made widely-reported public statements describing what we knew at that point about the incident.

Simply put, prior to January 2, despite our immediate efforts to have two separate firms of forensic investigators dig into our systems in an attempt to find any data security compromise, no data security compromise in our systems had been identified. A more detailed chronology of the period before January 2 is set out later in my testimony, but specifically:

Tues. Dec.17: We receive a "CPP report" from MasterCard showing 122 payment cards with confirmed fraud use, suggesting that the "common point of purchase" (CPP) *may* have been one Neiman Marcus store where these cards had been previously used over a several-month period.

Wed. Dec. 18: We call forensic investigative firms in order to start an investigation, consistent with the card brand protocol. A new CPP report is received showing 74 cards.

Fri. Dec. 20: We hire a leading forensic investigative firm to conduct a thorough investigation. They start immediately. A new CPP report is received showing 26 cards.

Mon. Dec. 23: We notify federal law enforcement. They follow up with us shortly thereafter and we have been working with them since then. A new CPP report is received showing 2,185 cards.

Sun. Dec. 29: The forensic investigation has not turned up any evidence of a data compromise, and we decide to bring on a second leading forensic investigative firm to accelerate the investigation and help us determine whether we have a problem.

Wed. Jan. 1: For the first time, the forensic investigators find preliminary indications of malware that may have the capability to "scrape" or capture payment card data. This is confirmed on January 2, but it remains unknown whether the malware was able to function on our systems.

Mon. Jan. 6: After days of highly technical work disassembling, decrypting, and decoding the malware and its output files, the investigators conclude that the malware appeared to have been capturing payment card data at numerous stores. The immediate focus of the Neiman Marcus team turns to containing and disabling the malware as it is unknown whether the malware is still capturing card data.

Fri. Jan. 10: The malware appears to be contained and disabled. Neiman Marcus issues public statements identifying the data security incident and begins sending notices to customers on the CPP reports. Prominent coverage follows. We subsequently send out additional notices on our website and to all customers who shopped in any Neiman Marcus store or website during 2013, whether or not potentially exposed to the malware.

Based on the current state of the evidence in the ongoing investigation: (i) it now appears that the customer information that was potentially exposed to the malware was payment card account information from transactions in 77 of our 85 stores between July and October 2013, at different time periods within this date range in each store; (ii) we have no indication that transactions on our websites or at our restaurants were compromised; (iii) PIN data was not compromised, as we do not have PIN pads and do not request PINs; and (iv) there is no indication that social security numbers or other personal information were exposed in any way.

The policies of payment card brands protect our customers from any liability for any unauthorized charges if the fraudulent charges are reported in a timely manner. Nonetheless, we have now offered to any customer who shopped with us in the last year at either Neiman Marcus Group stores or websites – whether their card was exposed to the malware or not – one year of free credit monitoring and identity-theft insurance. We will continue to provide the excellent service to our customers that is our hallmark, and I know that the way we responded to this situation is consistent with that commitment.

December: CPP Reports and Forensic Investigation

This malware was discovered as a result of forensic investigative efforts by two of the leading computer forensic firms, hired by us upon receiving very limited information suggesting that there might have been a compromise regarding payment card data.

Specifically, on the evening of Friday, December 13, we were contacted by our merchant processor that Visa had identified an unknown number of fraudulently-reported credit cards with a possible common point of purchase at a small number of Neiman Marcus stores. The merchant processor provided no details concerning the number of cards affected, the credit card account numbers, or prior Neiman Marcus transactions. This initial report did not provide any indication of a cyber-incident or that our network may have been penetrated, but because even this limited information raised a potential concern, we immediately began an internal investigation to determine what could be responsible for the card fraud and whether our systems had been compromised in any way.

Despite repeated requests to our merchant processor over that weekend and on Monday for more information, we did not receive any additional information until Tuesday, December 17. On that date, we received a Common Point of Purchase ("CPP") report listing 122 MasterCard cards that had been used in one Neiman Marcus store and had subsequently been used fraudulently elsewhere.[1]

On December 18, we received another CPP report, this one listing 74 Visa cards. That day, consistent with Visa's protocols, we began contacting forensic investigative firms. On December 20, we engaged a leading forensic investigative firm to immediately start a thorough investigation of our systems in order to determine whether there was any evidence of a data compromise that might indicate the potential theft of payment card data.

---

[1] As we understand the general practice, accounts listed on CPP reports are accounts for which the issuing bank and the cardholder are both already aware that the card has been used fraudulently. These CPP reports provide some indication that a particular merchant *may* have a compromise regarding payment card data, based on analysis by the banks and the card brands. This analysis is tentative, not definitive. The reports indicate a level of suspicion that a problem may exist but do not establish that there actually is a problem, or the nature of the problem – including whether the potential theft of the cards relates to cybercrime or more traditional criminal methods. Nevertheless, our internal investigation focused on this information immediately.

Also on December 20, we received additional CPP reports listing a total of 26 Visa and MasterCard cards, bringing the total number of cards on the CPP reports to 222, which had been used at Neiman Marcus over a period of several months. Although we take any indication of potential payment-card theft seriously, this appeared to be a very small number of cards on CPP reports, especially in light of the millions of transactions Neiman Marcus Group conducts annually. News of the Target data security incident and its potential effect on 40 million payment cards was being reported, and this added to the uncertainty about whether the source of any payment card theft was within our system. And we had not received any CPP reports listing any American Express or Neiman Marcus private label credit card accounts.

On Monday, December 23, we received another CPP report which listed 2,185 MasterCard accounts relating to transactions at numerous Neiman Marcus stores. That day, we notified federal law enforcement of the situation, even though the forensic investigators had not found anything significant. In addition to giving them notice of our situation, we wanted to see if they could shed any light on areas where we should focus our attention and to determine if they had seen anything in their other investigations that would assist us in determining whether a compromise had occurred. The Secret Service followed up with us shortly thereafter, and we have been working closely with them since then.

Meanwhile, the investigation continued but was not turning up any evidence of a data compromise. This forensic work involved, among other things, experienced computer investigators looking at hundreds of thousands of files, logs, and other items of data in our system in an attempt to find anything out of the ordinary. However, by December 28, after a week of forensic investigative work, it was still not clear whether there was a problem in our system.

The next day, December 29, we decided to bring in a second leading computer forensic investigative firm to begin conducting an additional, independent investigation. Although the first firm had not found any evidence of a data compromise in our system that appeared in any way related to the potential theft of credit card information, we wanted another expert team to examine our system. Simply put, we wanted to accelerate the investigation and ensure that we were taking the best steps to protect our customers and to learn if our systems had been compromised.

January: Discovery and containment of the malware, and notice to the public and our customers

On January 1, the first investigative firm reported that they had discovered malware that they suspected to have card "scraping" functionality (malware that attempts to fraudulently obtain or capture payment card data). On January 2, the investigators reported that the malware appeared to actually have this functionality. However, they could not say whether the malware had functioned at all in our system, whether it had the capability to successfully capture and exfiltrate card data (that is, send data to an outside source), or whether exfiltration had actually occurred. For the next several days, the two investigative firms engaged in the difficult work of trying to learn what they could about the malware and look for evidence of its operation in different parts of our systems.

Attempting to figure out how the malware functioned was complicated work, requiring the investigators to disassemble the malware program and run tests in our technology labs to try to recreate its functionality. After some time they determined that the malware's output files were encrypted. They then developed a custom decoder to decrypt the output files. They also created a custom-coded scanning tool to determine where and how the malware was operating.

By January 6, we had succeeded in decrypting the output files and in locating the malware at various points on our system. As a result, certain observations about the malware could be made for the first time: the malware apparently operated at point-of-sale registers in multiple stores, and it appeared to have been successful in "scraping" and capturing payment card data at the moment a card is swiped through our Point of Sale system. However, it was unknown whether the malware had actually managed to steal data, the dates when it had been operating, and the full scope of how and where it had been operating.

In addition, our expert computer forensic investigators told us that the malware was highly sophisticated and was different than any other malware they had ever analyzed. Its complex, specialized elements helped to explain how the malware had successfully evaded detection, despite all of the security measures we had in place, in at least five different ways. First, the malware was apparently not known to the anti-virus community and had been written to evade anti-virus signatures. Second, the malware erased its tracks by removing the disk file that had caused it to run, even while the program itself was still running in memory – a highly unusual and difficult-to-achieve feature. Third, when the malware scraped and captured card data, it created encrypted output files, so the output files did not exhibit evidence of card-

scraping activity – until they were decrypted. Fourth, the malware appeared to have features that were custom-built as a result of reconnaissance efforts within our systems that appear to have been clandestinely conducted earlier in 2013. Finally, the malware carefully covered its tracks with a built-in capability that wiped out files evidencing its operation by overwriting them with random data – making forensic detection much more difficult.

Although the investigators knew more about the malware by January 6, they did not know whether the malware was still scraping and capturing card data, and they were concerned that additional customer card data might be getting captured on an ongoing basis. The investigators discussed with us an immediate problem: since the malware was not yet contained, if the attacker learned that we had discovered the malware, there was a significant risk that the attacker might accelerate efforts to obtain captured account numbers, or that other cyber criminals might be encouraged to test our systems for vulnerabilities. Thus, our top priority at that point became disabling the malware.

From January 7 through January 10, we took a variety of steps in an attempt to ensure that the malware could not function. Since we did not yet know the full contours of how the malware functioned, designing a containment strategy was highly challenging. Nevertheless, by January 10, the investigators had a substantial level of confidence that the malware had been disabled.

That day, January 10, Neiman Marcus announced publicly that we had suffered a data security incident and that some customers' payment card information had been potentially compromised. This announcement was widely disseminated by the media in prominent print and broadcast coverage, and appeared on social media. We also sent email notices that same day to all customers whose payment cards were listed on the CPP reports (about 2,400) for whom we had email addresses. The next business day we sent letter notices to all customers in that group for whom we had postal addresses.

On January 16, our CEO Karen Katz issued a public letter, posted on our website with a prominent link from our home page, explaining that we had been the subject of a data security incident, and offering free credit monitoring and identity-theft insurance for one year to any customer who had used any payment card to conduct any transaction during the past year at any Neiman Marcus Group store or website.

Around this time, the investigators became confident that the dates during which the card-scraping malware had been active was July 16 to October 30, 2013. The number of unique

payment cards used at all Neiman Marcus Group stores during this period was approximately 1,100,000. However, the ongoing investigations have not found evidence of the malware operating in all Neiman Marcus Group stores, and it appears that the malware was probably not operating each day during this period based on current evidence. Thus, the number of payment cards that were potentially exposed during this period appears to be lower than 1,100,000, although we have not yet determined how much lower. Because the investigation is ongoing, this information is preliminary.

On January 22, we issued an updated public notice on our website explaining the July 16 – October 30 period and stating that 1,100,000 payment card accounts were potentially exposed. The same day, we sent out individual email and letter notices about the incident to any customer who used a payment card at any time in the past year for any Neiman Marcus Group purchase – whether in one of our stores or on our websites – and for whom we had address information. Our individual notices again provided information about the offer of free credit monitoring and identity-theft insurance.

Notably, we sent this notice – and offered free credit monitoring and identity-theft insurance – to a much larger group than the cardholders whose information appears to have been potentially exposed. Our expanded group included anyone who had used a payment card over a much longer period of time (one year), and website customers (who do not appear to have been exposed to the malware). We took these steps in an abundance of caution because of the ongoing nature of the investigation, and because we want all of our customers to know that we place the highest priority on the security of their personal information.

The ongoing investigation

As with other investigations, computer forensic investigations into data security incidents evolve over time, sometimes in unpredictable ways. We remain in close contact with law enforcement. My statements today are based on the current evidence from the investigations into this recent incident, and therefore should be considered tentative and subject to change. But even though we are still in the midst of discovering the facts, we are pleased to have had the opportunity to provide information to this Committee.

Thank you for your invitation to testify today, and I look forward to answering your questions.

Mr. TERRY. Mr. Russo, you are recognized for 5 minutes.

STATEMENT OF BOB RUSSO

Mr. RUSSO. Thank you.

My name is Bob Russo, and I am the general manager of the PCI Security——

Mr. TERRY. Can you pull the microphone a little closer to you?

Mr. RUSSO. Sorry. It is on now.

Mr. TERRY. And a little closer.

Mr. RUSSO. As I said, my name is Bob Russo, and I am the general manager of the PCI Security Standards Council, a global industry initiative and membership organization focused on security payment card data.

Our approach to an effective security program combines people, process, and technology as key parts of payment card data protection. We believe the development of standards to protect payment card data is something the private sector, and in particular, PCI, is uniquely qualified to do. The global reach, expertise, flexibility of PCI make it extremely effective.

Our community of over 1,000 of the world's businesses is tackling data security challenges from simple issues like password. In fact, "password" is still the most commonly used password out there to really complicated issues like proper encryption.

We understand consumers are upset when their payment card data is put at risk, and we know the harm caused by data breaches. The council was created to proactively protect consumers' payment card data. Our standards represent a solid foundation for a multi-layered security approach. We focus on removing card data if it is no longer needed. Simply put, if you don't need it, don't store it. And if it is needed, then protect it and reduce incentives for criminals to steal it.

Let me tell you how we do that. The data security standard is built on 12 principles capturing everything from physical security to logical security. This standard is updated regularly through feedback from our global community. In addition, we have developed other standards that cover software, point of sale devices, secure manufacturing of cards and much, much more. We work on technologies like tokenization and point-to-point encryption. Tokenization and point-to-point inscription work in concert with PCI standards to offer additional protections.

Another technology, EMV chip is an extremely effective method of reducing card fraud in a face-to-face environment. That is why the council supports its adoption in the U.S. through organizations such as the EMV migration from, and our standards support EMV today in other worldwide markets. However, EMV chip is only one piece of the puzzle. To move to EMV and to do no more would not solve this problem. Additional controls are needed to protect the integrity of payments online and in others' channels. These include encryption, tamper-resistant devices, malware protection, network monitoring, and much, much more. These are all addressed in the PCI standards.

Used together, EMV chip and PCI can provide strong protections for payment card data, but effective security requires more than just standards. Standards without supporting programs are only

tools and not solutions. The council's training and certification programs have educated tens of thousands of individuals and make it easy for businesses to choose products that have been lab tested and certified as secure.

Finally, we conduct global campaigns to raise awareness of payment card security. We welcome the Committee's attention to this critical issue. The recent compromises underscore the importance of a multi-layered approach to payment card security and there are clear ways in which we think the Government can help.

For example, leading stronger law enforcement efforts worldwide by encouraging stiff penalties for these crimes, promoting information sharing between the public and private sector also merits attention. The council is an active collaborator with government. We work with NIST, with DHS, with many government organizations. We are ready and willing to do much more. The recent breaches underscore the complex nature of the payment card security. A multifaceted program cannot be solved by a single technology, standard, mandate, or regulation. It cannot be solved by a single sector of society. We must work together to protect the financial and privacy interests of consumers.

Today, as this committee focuses on recent breaches, we know that the criminals are focusing on inventing the next attack vector. There is no time to waste. The PCI Security Standards Council and business must continue to provide a multi-layered security protection while Congress leads the efforts to combat global cyber crimes that threaten us. We thank the Committee for taking a leadership role in seeking solutions to one of the largest security concerns of our time.

Mr. TERRY. Thank you, Mr. Russo.

[The prepared statement of Mr. Russo follows:]

Payment Card Industry
Security Standards Council LLC
401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876-8855

Statement of Bob Russo
General Manager
Payment Card Industry Security Standards Council

Before the Energy & Commerce Committee,
Subcommittee on Commerce, Manufacturing & Trade
United States House of Representatives

Protecting Consumer Information: Can Data Breaches Be Prevented?

February 5, 2014
2123 Rayburn House Office Building

Introduction
Chairman Terry, Ranking Member Schakowsky, members of the subcommittee, on behalf of the PCI Security Standards Council, thank you for inviting us to testify today before the subcommittee.

My name is Bob Russo and I am the General Manager of the Payment Card Industry (PCI) Security Standards Council (SSC), a global industry initiative and membership organization, focused on securing payment card data. Working with a global community of industry players, our organization has created data security standards—notably the PCI Data Security Standard (PCI DSS)—certification programs, training courses and best practice guidelines to help improve payment card security.

Together with our community of over one thousand of the world's leading businesses, we're tackling data security challenges from password complexity to proper protection of PIN entry devices on terminals. Our work is broad for a simple reason: there is no single answer to securing payment card data. No one technology is a panacea; security requires a multi-layered approach across the payment chain.

The PCI Security Standards Council is an excellent example of effective industry collaboration to develop private sector standards. Simply put, the PCI Standards are the best line of defense against the criminals seeking to steal payment card data. And while several recent high profile breaches have captured the nation's attention, great progress has been made over the past seven years in securing payment card data, through a collaborative cross-industry approach, and we continue to build upon the way we protect this data.

Consumers are understandably upset when their payment card data is put at risk of misuse and—while the PCI Security Standards Council is not a name most consumers know—we are sensitive to the impact that breaches cause for consumers. And consumers should take comfort from the fact that a great number of the organizations they do business with have joined the PCI SSC to collaborate in the effort to better protect their payment card data.

Payment card security: a dynamic environment

Since the threat landscape is constantly evolving, the PCI SSC expects its standards will do the same. Confidence that businesses are protecting payment card data is paramount to a healthy economy and payment process—both in person and online. That's why to date, more than one thousand of the world's leading retailers, airlines, banks, hotels, payment processors, government agencies, universities, and technology companies have joined the PCI Council as members and as part of our assessor community to develop security standards that apply across the spectrum of today's global multi-channel and online businesses.

Our community members are living on the front lines of this challenge and are therefore well placed, through the unique forum of the PCI Security Standards Council, to provide input on threats they are seeing and ideas for how to tackle these threats through the PCI Standards.

The Council develops standards through a defined, published three year lifecycle. Our Participating Organization members told us that three years was the appropriate timeframe to update and deploy security approaches in their organizations. In addition to the formal lifecycle, the Council and the PCI community have the resources to continually monitor and provide updates through standards, published FAQs, Special Interest Group work, and guidance papers on emerging threats and new ways to improve payment security. Examples include updated wireless guidance and security guidelines for merchants wishing to accept mobile payments.

This year, on January 1, 2014, our latest version of the PCI Data Security Standard (PCI DSS) became effective. This is our overarching data security standard, built on 12 principles that cover everything from implementing strong access control, monitoring and testing networks, to having an information security policy. During updates to this standard, we received hundreds of pieces of feedback from our community. This was almost evenly split between feedback from domestic and international organizations, highlighting the global nature of participation in the PCI SSC and the need to provide standards and resources that can be adopted globally to support the international nature of the payment system.

This feedback has enabled us to be directly responsive to challenges that organizations are facing every day in securing cardholder data. For example, in this latest round of PCI DSS revisions, community feedback indicated changes were needed to secure password recommendations. Password strength remains a challenge—as "password" is still among the most common password used by global businesses—and is highlighted in industry reports as a common failure leading to data compromise. Small merchants in particular often do not change passwords on point of sale (POS) applications and devices. With the help of the PCI community, the Council has updated requirements to make clear that default passwords should never be used, all passwords must be regularly changed and not continually repeated, should never be shared, and must always be of appropriate strength. Beyond promulgating appropriate standards, we have taken steps through training and public outreach to educate the merchant community on the importance of following proper password protocols.

Recognizing the need for a multi-layer approach, in addition to the PCI DSS, the Council and community have developed standards that cover payment applications and point of sale devices. In other areas, based on community feedback, we are working on standards and guidance on other technologies such as tokenization and point-to-point encryption. These technologies can dramatically increase data security at vulnerable points along the transactional chain. Tokenization and point-to-point encryption remove or render payment card information useless to cyber criminals, and work in concert with other PCI Standards to offer additional protection to payment card data.

In addition to developing and updating standards, every year the PCI community votes on which topics they would like to explore with the Council and provide guidance on. Over the last few years the working groups formed by the Council to address these concerns have drawn hundreds of organizations to collaborate together to produce resources on third party security assurance, cloud computing, best practices for

maintaining compliance, e-commerce guidelines, virtualization, and wireless security. Other recent Council initiatives have addressed ATM security, PIN security, and mobile payment acceptance security for developers and merchants.

EMV Chip & PCI Standards—a strong combination

One technology that has garnered a great deal of attention in recent weeks is EMV chip—a technology that has widespread use in Europe and other markets. EMV chip is an extremely effective method of reducing counterfeit and lost/stolen card fraud in a face-to-face payments environment. That's why the PCI Security Standards Council supports the deployment of EMV chip technology.

Global adoption of EMV chip, including broad deployment in the U.S. market, does not preclude the need for a strong data security posture to prevent the loss of cardholder data from intrusions and data breaches. We must continue to strengthen data security protections that are designed to prevent the unauthorized access and exfiltration of cardholder data.

Payment cards are used in variety of remote channels—such as electronic commerce—where today's EMV chip technology is not typically an option for securing payment transactions. Security innovation continues to occur for online payments beyond existing fraud detection and prevention systems. Technologies such authentication, tokenization, and other frameworks are being developed, including some solutions that may involve EMV chip—yet broad adoption of these solutions is not on the short-term horizon. Consequently, the industry needs to continue to protect cardholder data across all payment channels to minimize the ongoing risks of data loss and resulting cross-channel fraud such as may be experienced in the online channel.

Nor does EMV chip negate the need for secure passwords, patching systems, monitoring for intrusions, using firewalls, managing access, developing secure software, educating employees, and having clear processes for the handling of sensitive payment card data. These processes are critical for all businesses—both large retailers and small businesses—who themselves have become a target for cyber criminals. At smaller businesses, EMV chip technology will have a strong positive impact. But if small businesses are not aware of the need to secure other parts of their systems, or if they purchase services and products that are not capable of doing that for them, then they will still be subject to the ongoing exposure of the compromise of cardholder data and resulting financial or reputational risk.

Similarly, protection from malware-based attacks requires more than just EMV chip technology. Reports in the press regarding recent breaches point to insertion of complex malware. EMV chip technology could not have prevented the unauthorized access, introduction of malware, and subsequent exfiltration of cardholder data. Failure of other security protocols required under Council standards is necessary for malware to be inserted.

Finally, EMV chip technology does not prevent memory scraping, a technique that has been highlighted in press reports of recent breaches. Other safeguards are needed to do so. In our latest versions of security standards for Point of Sale devices, (PCI PIN Transaction Security Requirements), the Council includes requirements to further counter this threat. These include improved tamper responsiveness so that devices will "self-destruct" if they are opened or tampered with and the creation of electronic signatures that prevent applications that have not been "whitelisted" from being installed. Our recently released update to the standard, PTS 4.0, requires a default reset every 24 hours that would remove malware from memory and reduce the risk of data being obtained in this way. By responding to the Council's PTS requirements, POS manufacturers are bringing more secure products to market that reflect a standards development process that incorporates feedback from a broad base of diverse stakeholders.

Used together, EMV chip, PCI Standards, along with many other tools can provide strong protections for payment card data. I want to take this opportunity to encourage all parties in the payment chain—whether they are EMV chip ready or not—to take a multi-layered approach to protect consumers' payment card data. There are no easy answers and no shortcuts to security.

Global adoption of EMV chip is necessary and important. Indeed, when EMV chip technology does become broadly deployed in the US marketplace and fraud migrates to less secure transaction environments, PCI Standards will remain critical.

Beyond Standards – building a support infrastructure

An effective security program through PCI is not focused on technology alone; it includes people and process as key parts of payment card data protection. PCI Standards highlight the need for secure software development processes, regularly updated security policies, clear access controls, and security awareness education for employees. Employees have to know not to click on suspicious links, why it is important to have secure passwords, and to question suspicious activity at the point of sale.

Most standards' organizations create standards, and no more. PCI Security Standards Council, however, recognizes that standards, without more, are only tools, and not solutions. And this does not address the critical challenges of training people and improving processes.

To help organizations improve payment data security, the Council takes a holistic approach to securing payment card data, and its work encompasses both PCI Standards development and maintenance of programs that support standards implementation across the payment chain. The Council believes that providing a full suite of tools to support implementation is the most effective way to ensure the protection of payment card data. To support successful implementation of PCI Standards, the Council maintains programs that certify and validate certain hardware and software products to support payment security. For example, the Council wants to make it easy for merchants and financial institutions to deploy the latest and most secure terminals and so maintains a public listing on its website for them to consult before purchasing products. We realize it takes time and money to upgrade POS terminals and we encourage businesses that are looking to upgrade for EMV chip to consider other necessary security measures by choosing a POS terminal from this list. Similarly, we are supporting the adoption of point-to-point encryption, and listing appropriate solutions on our website to take a solutions-oriented approach to helping retailers more readily implement security in line with the PCI standards.

Additionally, the Council runs a program that develops and maintains a pool of global assessment personnel to help work with organizations that deploy PCI Standards to assess their performance in using PCI Standards. The Council also focuses on creating education and training opportunities to build expertise in protecting payment card data in different environments and from the various viewpoints of stakeholders in the payment chain. Since our inception, we have trained tens of thousands of individuals, including staff from large merchants, leading technology companies and government agencies. Finally, we devote substantial resources to creating public campaigns to raise awareness of these resources and the issue of protecting payment card data.

The PCI community and large organizations that accept, store, or transmit payment card data worldwide have made important strides in adopting globally consistent security protocols. However, the Council recognizes that small organizations remain vulnerable. Smaller businesses lack IT staff and budgets to devote resources to following or participating in the development of industry standards. But they can take simple steps like updating passwords, firewalls, and ensuring they are configured to accept automatic security updates. Additionally, to help this population, the Council promotes its listings of validated products, and recently launched a program, the Qualified Integrator and Reseller program (QIR) to provide a pool of personnel able to help small businesses ensure high quality and secure installation of their payment systems.

The work of the Council covers the entire payment security environment with the goal of providing or facilitating access to all the tools necessary—standards, products, assessors, educational resources, and training—for

stakeholders to successfully secure payment card data. We do this because we believe that no one technology is a panacea and effective security requires a multi-layered approach.

Public – private collaboration

The Council welcomes this hearing and the government's attention on this critical issue. The recent compromises underscore the importance constant vigilance in the face of threats to payment card data. We are hopeful that this hearing will help raise awareness of the importance of a multi- layered approach to payment card security.

There are very clear ways in which the government can help improve the payment data security environment. For example, by championing stronger law enforcement efforts worldwide, particularly due to the global nature of these threats, and by encouraging stiff penalties for crimes of this kind to act as a deterrent. There is much public discussion about simplifying data breach notification laws and promoting information sharing between public and private sector. These are all opportunities for the government to help tackle this challenge.

The Council is an active participant in government research in this area: we have provided resources, expertise and ideas to NIST, DHS, and other government entities, and we remain ready and willing to do so.

Almost 20 years ago, through its passage of the Technology Transfer and Advancement Act of 1995, Congress recognized that government should rely on the private sector to develop standards rather than to develop them itself. The substantial benefits of the unique, U.S. "bottom up" standards development process have been well recognized. They include the more rapid development and adoption of standards that are more responsive to market needs, representing an enormous savings in time to government and in cost to taxpayers.

The Council believes that the development of standards to protect payment card data is something the private sector, and PCI specifically, is uniquely qualified to do. It is unlikely any government agency could duplicate the expansive reach, expertise, and decisiveness of PCI. High profile events such as the recent breaches are a legitimate area of inquiry for the Congress, but should not serve as a justification to impose new government regulations. Any government standard in this area would likely be significantly less effective in addressing current threats, and less nimble in protecting consumers from future threats, than the constantly evolving PCI Standards.

Conclusion

In 2011, the Ponemon Institute, a non-partisan research center dedicated to privacy, data protection, and information security policy wrote, "The Payment Card Industry Data Security Standard (PCI DSS) continues to be one of the most important regulations for all organizations that hold, process or exchange cardholder information."

While we are pleased to have earned accolades such as this, we cannot rest on our laurels.

The recent breaches at retailers underscore the complex nature of payment card security. A complex problem cannot be solved by any single technology, standard, mandate, or regulation. It cannot be solved by a single sector of society—business, standards-setting bodies, policymakers, and law enforcement—must work together to protect the financial and privacy interests of consumers. Today as this committee focuses on recent damaging data breaches we know that there are criminals focusing on committing inventing the next threat.

There is no time to waste. The PCI Security Standards Council and business must commit to promoting stronger security protections while Congress leads efforts to combat global cyber-crimes that threaten us all.

We thank the Committee for taking an important leadership role in seeking solutions to one of the largest security concerns of our time.

###

Mr. TERRY. Mr. Smith, you are now recognized for 5 minutes.

STATEMENT OF PHILLIP J. SMITH

Mr. SMITH. Good morning, Chairman Terry, Ranking Member Schakowsky, subcommittee members, staff, and ladies and gentlemen.

I want to thank you for the opportunity on behalf of Trustwave to provide witness testimony on this important issue related to data breaches.

I am both a former special agent of the United States Secret Service and a senior trial attorney at the Department of Justice Terrorism and Violent Crimes section. My law enforcement experience in this area includes investigation, prosecution of criminal credit card fraud, access device fraud, and counterfeiting. I left the Justice Department in 2000 to join Trustwave, a now global information security and compliance services and technology company. I currently serve in Trustwave's executive team as senior vice president, and I was general counsel for 12 years.

Businesses and government agencies hire Trustwave to help fight cyber crime, protect their sensitive data, and reduce risk. Trustwave has customers ranging from the world's largest multinational companies to small and medium-sized businesses in 96 countries. We specialize in the following areas: Compliance and risk management, managed and cloud-based security services, as well as threat intelligence, ethical hacking, security research, and we also train law enforcement on how to investigate network intrusion and data breach cases.

Today, I would offer our observations and recommendations related to data breach and broader information security trends. It is important I note that as a company we do not comment or speculate on specific data breaches, and as such, we will not be offering testimony today related to companies involved in the latest string of data breaches. However, I believe our company's experience in investigating thousands of data breaches over the past several years, our advanced security research and intelligence coming from our large global client footprint will be of value to you and the industry as a whole.

My submitted written testimony discusses how card data is stolen through malware attacks, the value of the Payment Card Industry Data Security Standard, and why businesses must go beyond PCI for increased security and technologies and processes that can help. While I generally have time to discuss each topic in depth, I would like to highlight a few items.

Each year our company publishes statistics and observations from real-world data breach investigations in our Trustwave Global Security Report. The focus of the report is around cyber crime, states that attacks are carried out by professional criminals, and most of them follow logical patterns as described by the Secret Service. The 2013 Global Security Report highlights data our experts analyzed from more than 450 data breach, incident response investigation locations, thousands in penetration tests, millions of Web site and web application attacks, tens of billions events.

The report states the retail industry is the top target in 2012, making up 45 percent of our investigation. Food and beverage in-

dustry was second, followed by the hospitality industry. Those rankings did not change in 2013. Cardholder data was the primary target. Mobile malware increased 400 percent in 2012. Seventy-three percent of the victims were located in the United States. Almost all the point of sale breach investigations involved targeted malware. SQL injection and remote access made up 73 percent of the infiltration methods used by criminals, took businesses an average of 210 days to detect a breach, most took more than 90 days, and 5 percent took more than 3 years. Only 24 percent detected the intrusion themselves. Most were informed by law enforcement.

Web applications emerged the post popular attack vector, E-commerce sites being the most targeted asset. Weak passwords with "Password1" being the most common password of choice.

I am running short on time, and refer to my written testimony where I talk about many different security areas as part of the defense and depth strategy, recommending multiple layers of defense, detection, response, and ongoing training. I would, however, make the following observations. PCI Data Security Standard plays a critical role that has increased awareness around securing data in the payment industry. The threat landscape is more complex than ever, and keeping up with and complying with the standard simply isn't enough.

A common misperception is that PCI was designed to be a catch-all for security. We believe it serves as a good baseline for security, giving businesses guidelines for basic security controls to protect cardholder data. And we heard discussions today about chip-and-PIN, end-to-end encryption and other technologies, and these are all good, but there is no silver bullet. A multi-layered approach to security involves people, process, technology, and innovation, and I would take these few minutes to highlight 3 particular ones.

Businesses should implement an incident response plan that includes advanced detection techniques, containment strategies, and response technologies. Web applications are a high value target for attackers because they are easily accessible over the net. Web applications are often at businesses' front door and often connected to systems that contain private data. While monitoring more than 200,000 Web sites, our researchers found 16,000 attacks occur on web applications per day. This is why businesses need to adopt protections that include the ability to detect vulnerabilities and prevent web applications.

Obviously, anti-malware is a big issue here, and what companies need to do is to defend against this is deploy gateways, and I stress this is not anti-virus technology. This is, gateways specifically help to protect businesses in realtime from threats like malware and zero-day vulnerabilities and data loss.

I want to thank the Chairman and Ranking Member Schakowsky for the opportunity to be here today, and happy to answer any questions.

Mr. TERRY. Thank you, Mr. Smith.

[The prepared statement of Mr. Smith follows:]

Prepared Testimony

Phillip J. Smith
Senior Vice President
Trustwave Holdings, Inc.

Hearing On

"Protecting Consumer Information: Can Data Breaches Be Prevented?"

Before The

U.S. House of Representatives
Energy & Commerce Committee
Subcommittee on Commerce, Manufacturing and Trade

Wednesday, February 5, 2014

2123 Rayburn House Office Building

Good morning, Chairman Terry and Ranking Member Schakowsky, Sub-Committee Members, staff, ladies and gentlemen. I want to thank you for requesting that I, on behalf of Trustwave, provide witness testimony on this important issue related to data breaches in our financial systems and more specifically, our payments industry.

By way of background, I am both a former Special Agent with the United States Secret Service and a Senior Trial Attorney in the Department of Justice's Terrorism and Violent Crime Section (now known as the Counterterrorism Section). My law enforcement experience in this area includes the investigation and prosecution of credit card fraud, access device fraud and counterfeiting. I left the Justice Department in July of 2000 to join Trustwave, a global information security and compliance services and technology company headquartered in Chicago. I currently serve on Trustwave's executive team as Senior Vice President of Government Solutions. In addition to early operational roles which include supervising our advanced research and ethical hacking practice, I served as General Counsel for the first 12 years with Trustwave.

Businesses and government agencies hire Trustwave to help them fight cybercrime, protect their sensitive data and reduce security risks. Trustwave has customers—ranging from some of the world's largest, multinational companies to small- and medium-sized businesses—in 96 countries. We specialize in a variety of areas: compliance and risk management, managed and cloud-based security services, as well as threat intelligence, ethical hacking and security research. We also train law enforcement on how to investigate network intrusion and data breach cases.

Today, I want to offer our observations and recommendations related to data breach and broader information security trends. It's important I note that as a company we do not comment or speculate on specific data breaches, and as such we will not be offering testimony today specifically related to specific companies involved in the latest string of data breaches. However, I believe our company's experience in investigating thousands of data breaches over the past few years, augmented by our ongoing security research and the threat intelligence gleaned from our large, global client footprint, will be of value to you and the industry as a whole.

I'd like to start with some of the macro-level trends we're seeing. In today's Internet-connected world, security is more complex than ever. Hackers are targeting businesses of all sizes and across all industries. There is a growing pool of attack vectors from which to choose, including what we now consider a basic business tool: the web, as well as emerging technologies like mobile devices and appliances (also known as "bring-your-own-device" or BYOD), social media and the cloud. Businesses also have huge amounts of information moving through their networks and applications and stored on their databases, meaning there is more data than ever to protect. Threats are growing more hostile and outpacing traditional security technologies like antivirus and firewalls. Budgets are also tight, and building and retaining a skilled security team can be challenging. According to a 2013 Frost & Sullivan Market Study, 56 percent of respondents believed there is a workforce shortage in the IT industry, compared to just two percent who believe there is a surplus. The gap is a result of simple economics—the demand has surpassed the supply. All of these factors leave in-house IT teams facing mounting pressures to ensure information security.

More specifically, I will also highlight:

- How cardholder data is being stolen through malware
- The value of the Payment Card Industry Data Security Standard (PCI DSS)
- Why businesses must go beyond PCI DSS compliance for increased security and technologies that can help.

Each year, our company publishes statistics and other observations from real-world data breach investigations in our **Trustwave Global Security Report**. The report is publicly available at www.trustwave.com/GSR. The focus of our report is around cybercrime. As our report states, attacks are carried out by professional criminals and most of them follow logical patterns of attack consisting of four common elements:

- **Infiltration** - Attackers must first find a way to penetrate an organization's environment
- **Propagation** - Pivoting from the initial point of entry to go after specific systems within an organization's network that contains sensitive data
- **Aggregation** - Identifying and collecting that sensitive data
- **Exfiltration** – Moving that data to a system (a computer or network) controlled by the attacker.

The 2013 Trustwave Global Security Report highlights data our experts analyzed from the more than **450 data breach/incident response investigations, thousands of penetration tests, millions of website and web application attacks and tens of billions of events** gathered through our security and risk assessments, managed security services and our other forms for threat intelligence including our advanced security research during 2012. The report reveals the threats and vulnerabilities businesses face. Specifically:

- The **retail industry was the top target** for data breaches in 2012 making up 45% of our investigations. Food & beverage was the second most targeted industry followed by the broader hospitality industry.
- **Cardholder data** was the primary data type targeted by attackers. There is a well-established underground marketplace for stolen payment card data.
- **Mobile malware increased 400%** in 2012. "Malware," which is short for "malicious software" is used to exploit vulnerabilities in computer systems, gather sensitive information, or gain access to private computer systems for a specific purpose—normally cybercrime.
- Out of more than 450 data breaches we investigated, the United States was the top victim location. **73% of victims were located in the U.S.**
- In 2012, almost all Point-Of-Sale (POS) breach investigations involved, what's known as, "targeted malware." That's when malware is designed for a specific computer system, business or computer user. **SQL (Structured Query Language) injection and remote access** made up 73% of the infiltration methods used by criminals. Other commonly used methods were **Blackhole exploit kits**, **malicious PDF files** (61% targeted Adobe Reader users) and "**memory scraping**." Criminals planted malware on users' machines by using all of these infiltration methods.
- It took businesses an average of **210 days to detect a breach**. Most victim organizations took more than 90 days to detect the intrusion, while 5% took more than three years to identify criminal activity.
- Only 24% of victim organizations detected the intrusion themselves. Most were informed by law enforcement or another regulatory body.
- **Web applications** emerged as the **most popular attack vector**; e-commerce sites being the most targeted asset.
- Users are continuously using weak passwords with "**Password1**" being the most common password of choice since it meets the bare minimum password requirement typically mandated by policies enforced by IT administrators. Weak default passwords and password requirements are a big problem.

How card data is being stolen

As I mentioned, most breaches follow the same patterns of attack: using infiltration, propagation, aggregation and exfiltration. Here's a breakdown of each step:

- **Infiltration**—Criminals get inside business systems by taking advantage of a variety of weaknesses—whether through web applications, social engineering, the web, zero-day vulnerabilities or remote access tools. For example, if a restaurant owner uses an IT service provider in the next state, the service provider might not be physically able to be in front of the restaurant's computer systems when action is required. So, using remote access tools, he accesses the restaurant's systems remotely. Attackers can enter the system using the same remote access tools but they also need a username and password. Oftentimes, businesses will not change their usernames and passwords when setting up their POS devices. This allows attackers to identify the POS default credentials or IT provider shared credentials and gain unauthorized access.
- **Propagation**—Once attackers gain access, they need to move from the point of infiltration to the systems that store, process, or transmit the desired data such as payment card data and other customer information. Since the attackers already have the administrative credentials, this step is often trivial.
- **Aggregation**—This is where the deployment of malware takes place. Attackers use custom malware, designed to identify cardholder data, and either encrypt or encode it, and place it in an output (or a dump) file. Custom malware does this automatically and without any visible service interruption to legitimate business activity.
- **Exfiltration**—Exfiltration can take place either automatically through the malware or the attackers will have to come back and get the data the same way they got in. Encrypted or encoded data is sent to a system controlled by the attacker. The stolen data moves undetected and is subsequently prepared to sell on the black market.

Payment Card Industry Security Standards Council (PCI SSC) and the Data Security Standard (PCI DSS)

The payments industry formed the Payment Card Industry Security Standards Council (PCI SSC) which is responsible for developing and administrating the Payment Card Industry Data Security Standard (PCI DSS) for any entity that stores, processes or transmits cardholder data. Here is our position on PCI DSS:

- The **PCI DSS plays a critical role** when it comes to data security.
- The standard has **increased awareness** surrounding data security.
- In today's environment, in which the threat landscape is more complex than ever and new business-improvement technologies are introduced everyday—keeping up with and complying with the standard simply isn't enough.
- A common misconception is that PCI was designed to be a catch-all for security. We believe the **PCI DSS serves as a baseline** for security, giving businesses guidelines for basic security controls to protect cardholder and personal data. Without PCI DSS, countless businesses would likely have fewer security controls (if any) than they do today.
- Organizations can improve their security posture by first understanding that the **PCI DSS is the floor, not the ceiling, when it comes to security**. While the PCI DSS helps businesses deploy some essential security controls, it doesn't cover security around every attack vector, such as security surrounding targeted malware, mobile devices and cloud technology.
- If organizations use a **defense-in-depth approach to security** consisting of multiple layers of defense, detection, response and ongoing testing, they can better protect themselves against attacks and inherently maintain compliance with the PCI DSS.
- Another standard for compliance, the **Payment Application Data Security Standard (PA-DSS)**, is also a good baseline. However, it does not include or require holistic manual penetration

testing against the entire Point-of-Sale platform (hardware, custom software and operating system)—testing we believe is important.

Going beyond PCI Compliance for increased security

The following are steps businesses can take, whether through policies and procedures or technologies to help prevent malware attacks on their networks, applications and databases. We recommend:

- **Incident response preparedness**—Businesses should implement an incident response plan that includes advanced detection techniques, containment strategies and response scenarios. These elements will help them see, stop and respond to an attack. Incident response plans can drastically reduce the impact of a breach on a business so that it can get back quicker to "business-as-usual."
- **Security awareness training**—Businesses should regularly provide security awareness training to all employees, including contractors and temporary workers. Executives and business leaders are also prime targets, so training should be required for anyone who has access to private information. Training can help them follow security best practices to reduce the risk of infiltration.
- **Strong passwords**—If a criminal is going to access a system remotely, he must first know where the system is located (the IP address), the appropriate remote administration protocol and login credentials (username and password). That's why strong passwords play a vital role in helping prevent a breach. Strong passwords consist of a minimum of seven characters and should include a combination of upper and lower case letters, symbols and numbers. We recommend using "passphrases" such as "MydOgisn@medBuck." Passphrases are both easier to remember and harder to crack.
- **Two-factor (or two-step) authentication**—Businesses should use two-factor authentication for employees who access the network. Two factor authentication forces users to verify their identity with information other than simply their username and password, like a special constantly-changing code sent to a user's mobile phone.
- **Business-wide security risk assessments and ongoing penetration testing**—Regular security risk assessments can help businesses identify where they store sensitive data and if that data is vulnerable to an attack. Frequent penetration testing, where ethical hackers use automated and manual tools to "break in" to business systems (at the request of that business), can help businesses identify and eliminate vulnerabilities that become the intrusion points of almost any breach.
- **Database scanning and security**—Databases hold a treasure trove of business data yet too often database security is overlooked. Businesses assume if their networks and applications are secure, so is their database. This assumption is false—and dangerous. Databases need constant vulnerability scanning and their own protection.
- **Certificates** and **firewalls**—Businesses should use certificates to further restrict remote access. Certificates help ensure the identities of both the server and user are trusted before granting the user access. Businesses should also install firewalls to help restrict any traffic that is not critical to their business.
- **Web application security**—Web applications are a high-value target for attackers because they are easily accessible over the Internet. Web applications are often a business's "front door" and are often connected to systems that contain private data. While monitoring 200,000 websites, our researchers found 16,000 attacks occurred on web applications per day. That is why businesses need to adopt protection that includes the ability to detect application vulnerabilities and prevent web application threats.
- **Advanced anti-malware protection**—Attackers often use compromised websites, or links to these sites in emails, as the point of entry to get malware on a business's network. A recent Osterman Research survey of security professionals showed that malware has infiltrated 74

percent of organizations through the web during the past year. To defend against these common attack vectors, businesses should deploy security "gateways." I must stress this is not anti-virus technology. Gateways specifically help protect businesses in real-time from threats like malware, zero-day vulnerabilities and data loss, and can help organizations use things like web and cloud applications securely.

- **Augment in-house security expertise**—Since security has become a more time-consuming, skills-specific, sometimes daunting task for many in-house IT teams, more businesses are augmenting their staff by partnering with an outside team of security experts that helps ensure more effective security tools are installed and running properly in order to prevent a data compromise. Managed security services help IT professionals maintain a higher state of security so they can focus on their primary jobs of IT projects that generate revenue for their employers.
- **End-to-end encryption**—Persistently encrypting cardholder data can help render data unreadable to unauthorized third parties, such as attackers, who try to steal sensitive information, such as credit card numbers. Encryption is another layer of defense against these malicious hackers or an unauthorized third party because even if the data is accessed they would be unable to read it. We believe this emerging technology, along with other security controls, shows great promise.
- "Chip and PIN"—Chip and PIN helps authenticate transactions and helps prove that the cardholder is the person requesting the transaction. In this scenario, the combination of an embedded microchip on a payment card and a PIN code replaces the traditional combination of the magnetic stripe data and signature. Layering this authentication method with other layers of security, such as end-to-end encryption can greatly reduce the risk of a card data compromise for brick and mortar merchants, or really anywhere that a card is present for the transaction.
- **Segmentation**—Currently the PCI DSS does not require businesses to segment or separate their systems that contain cardholder data. We recommend businesses go beyond PCI and separate their systems that contain critical data to make it more difficult for a criminal to access the target network. When businesses segment their systems, it causes the attacker to have to circumvent a second set of security controls.
- **Mobile device payment systems**—To conduct payment card transactions, some merchants may be using mobile devices that are consumer grade products with an attached card reader. These devices are designed for ease-of-use but sometimes contain serious security vulnerabilities. While the PCI DSS doesn't address these kinds of mobile devices, the standard does apply to any merchant that stores, processes, and transmits cardholder data, so the onus is on business leaders to make sure these devices comply.
- **Third-party vendor security checks**—When partnering with third-party IT providers, we recommend businesses require their provider use or do many of the items I've already discussed. Additionally, we recommend they have detailed and locked-down security policies, perform ongoing and regular penetration testing, demonstrate appropriate remote access controls, ensure software and hardware vendors are consistently patched and updated for security vulnerabilities, and that data is isolated from other customers in a shared, cloud environment.

Conclusion

I would like to thank Chairman Terry and Ranking Member Schakowsky, Sub-Committee Members, and staff for the opportunity to appear today on this important issue facing our businesses, our payment systems and our citizens. I brought several copies of the 2013 Trustwave Global Security Report and included a link to download the report as well as other information related to today's security threat landscape. We encourage the Members and their staff to review this information. I would be more than happy to address any questions related to my testimony.

Additional Information

2013 Trustwave Global Security Report
http://www.trustwave.com/GSR

Infographic: New data reveals extent of the malware problem
Trustwave Blog & Osterman Research
https://www.trustwave.com/trustednews/2014/01/infographic-new-data-reveals-extent-malware-problem#sthash.CrkMGzlU.dpbs

How security professionals are dealing with web, email and social threats
Trustwave Blog & Osterman Research
https://www.trustwave.com/trustednews/2014/01/trustwave-qa-how-security-professionals-are-dealing-web-email#sthash.zJghIaIj.dpuf

Two million stolen passwords: How to protect yourself
Trustwave Blog
https://www.trustwave.com/trustednews/2013/12/two_million_stolen_passwords_how_to_protect_yourself#sthash.AA1LaupH.dpuf

Inside a hacker's playbook: 10 targeted techniques that will break your security
Trustwave E-book
https://www2.trustwave.com/cpn-hackers-playbook-2013-sm.html

Infographic: The high cost of BYOD
Trustwave Blog
https://www.trustwave.com/trustednews/2013/04/infographic-the-high-cost-byod#sthash.WRSY7hZq.dpbs

Infographic: Keep the bad stuff out and the good stuff in
Trustwave Blog
https://www.trustwave.com/trustednews/2013/03/keep-the-bad-stuff-out-keep-the-good-stuff-in#sthash.yNtU3ckc.dpbs

Trustwave Reveals Increase in Cyber Attacks Targeting Retailers, Mobile Devices and E-Commerce
Trustwave Blog
https://www.trustwave.com/trustednews/2013/02/trustwave-reveals-increase-cyber-attacks-targeting-retailers-mobile#sthash.9S5zNEcG.dpuf

Executive Guide for Law Enforcement
Trustwave
https://www.trustwave.com/leoguide

Media Inquiries
Abby Ross
Media Relations
Trustwave
aross@trustwave.com
312-873-7648

Other Inquiries
Cas Purdy
Corporate Communications
Trustwave
cpurdy@trustwave.com
312-470-8703

Mr. TERRY. And that does conclude the testimony of our panel, and now it is time for us to ask you questions.

And I get to go first, so I recognize myself for 5 minutes.

Mr. Smith, based on your professional opinion in this industry, are we—the United States suffering an increased onslaught of data breaches and attacks or is it just simply we are paying more attention in the media?

Mr. SMITH. No, we are suffering more attacks, that is for sure,

Mr. TERRY. Can you quantify that in any way? Do you know how many——

Mr. SMITH. In numbers of attack? I mean I can only speak for our company and how many we are involved in each year, which involves, you know, a number of different investigations as well as multi-national locations within——

Mr. TERRY. Do you have an opinion why that has increased, the number of attacks have increased?

Mr. SMITH. I think any time there is something of value, and the Web now gives the ability for these multi-national attacks to occur from anywhere in the world, so as the technology increases, so will the attacks, so will the value of that data——

Mr. TERRY. Right.

Mr. SMITH [continuing]. That people are after.

Mr. TERRY. Appreciate that. Thank you.

And for Mr. Mulligan and Mr. Kingston, I appreciate that you accepted our invitation to come here. I think people should know that you didn't have to accept that invitation, you don't have to be here, but you agreed to be here, and A, I think that speaks well for both of the companies that you work for and your respect for the consumer to go on the record about what occurred and what you are offering to your customers. I want to thank you for that. It doesn't mean we don't ask you tough questions.

So, let me start off the same question to both Mr. Mulligan and Mr. Kingston. Both of you, you suffered point of sale attacks, and at least with Target there was a portion of that that was unencrypted and you were able to get the information in plain language, plain text. Is that a shortcoming? Is that standard? How much of a surprise to you or not surprise that there was that vulnerability at the point of sale, Mr. Mulligan?

Mr. MULLIGAN. Mr. Chairman, we know today——

Mr. TERRY. Pull your microphone a little closer

Mr. MULLIGAN. We know today in the U.S. that credit card information, payment card information, comes into point of sale systems from the magnetic strip unencrypted. In our case, that data was captured prior to us encrypting it. We have seen in other geographies around the world where chip-and-PIN or chip-enabled technology has been deployed, the fraud related to payment cards has come down dramatically, and that is why we have been supporters of that technology over a very long period of time.

Mr. TERRY. All right. Mr. Kingston.

Mr. KINGSTON. What we learned in our investigation, Chairman, is that the information was scraped at a time immediately following the swipe as well in basically milliseconds.

Mr. TERRY. In essence, commingled data so it was undetectable, hidden in plain sight?

Mr. KINGSTON. Literally milliseconds before it is sent through encrypted tunnels to payment processor for authorization.

Mr. TERRY. Wow. Back to Mr. Mulligan. Have you been able to determine how they were able to get into the system and place the malware at that very sensitive point?

Mr. MULLIGAN. That is my understanding the point of access was a compromised set of vendor credentials or log-on I.D. and password. Beyond that, we have an end-to-end review, forensic review of all of our systems to understand that particular question is one we share with you, Mr. Chairman.

Mr. TERRY. So, it was a process failure?

Mr. MULLIGAN. We don't understand that today. At the completion of our investigation, we are looking forward to getting the facts about what transpired.

Mr. TERRY. All right. Mr. Kingston.

Mr. KINGSTON. At this point in our investigation, we have not yet found any evidence of how attackers were able to infiltrate our network.

Mr. TERRY. A lot of discretion on breach notification. Tell us—first of all, we want to make sure that a consumer whose data, whether it was their financial or personally identifiable information, is notified in a timely manner. There is a perception that perhaps you discover breach and you should push send for notification. Does it really work that way? How much time is a reasonable amount of time before you notice a consumer of a breach? Mr. Mulligan.

Mr. MULLIGAN. Our focus was on providing certainly speed in getting notice quickly, we think, is important. Balancing that, and the lens that we were looking through was for our guests, providing them accurate information to help them understand what went on, and then actionable information, what could they do about it.

In addition, given the magnitude of our enterprise, we knew we would get significant requests from our guests, and we want to be prepared with staffing up our call centers, having our stores have the appropriate resources to respond to their requests, and I think all of that is how we approached this from a notification.

Mr. TERRY. How many days from the time that you were told of the breach versus when you were able to send them notice out?

Mr. MULLIGAN. From the time we found the breach, we found the malware on our system to the time we notified was 4 days.

Mr. TERRY. All right. Mr. Kingston, same questions.

Mr. KINGSTON. So we also at Neiman Marcus believe that prompt and specific notification is the best course of action. I think there are two important things that need to be established in order for that to happen and happen in a reasonable way as you ask the question. The first is understanding that you actually do have a breach or some sort of risk of attack, and so in our case we learned that on January 6th.

I think the second important thing is to protect customers from any potential further harm, to make sure that you contained, in our case, the malware that was discovered in our systems. It took us 4 days to do that, and at that time, on January 10th, we immediately began notifying customers.

Mr. TERRY. All right. 4 days for each of you. All right. Thank you.

And I recognize the Ranking Member Jan Schakowsky from Illinois.

Ms. SCHAKOWSKY. Thank you.

Just a quick question to Mr. Russo. I think you do good work, but you aren't suggesting that we shouldn't act as a Congress, are you, in order to set some standards?

Mr. RUSSO. No, certainly I think there are plenty of things that can be done, not the least of which is law enforcement and information sharing.

Ms. SCHAKOWSKY. I understand. I am asking that really as a yes or no question. Are you suggesting that it is inappropriate or unnecessary for Congress to act on standards, et cetera?

Mr. RUSSO. I don't know. I have no opinion in that area.

Ms. SCHAKOWSKY. OK. I wanted to ask you, Mr. Kingston. You discovered the breach internally? Neiman Marcus discovered it, the breach itself?

Mr. KINGSTON. The first idea that we had that there was anything potentially wrong in our system is on January 2nd when our forensic investigator brought to our attention that they had found some suspicious malware potentially capable of scraping card data. It wasn't until the 6th because it took them 4 days, based on the sophistication of this malware, to actually decrypt it and decompose it to understand that it actually could work in our——

Ms. SCHAKOWSKY. Who informed you?

Mr. KINGSTON. Our forensic investigator.

Ms. SCHAKOWSKY. Our?

Mr. KINGSTON. We hired a forensic investigator.

Ms. SCHAKOWSKY. Oh, your forensic investigator.

Mr. KINGSTON. Yes, forensic investigator.

Mr. TERRY. Not Mr. Smith.

Ms. SCHAKOWSKY. OK. And Mr. Mulligan, you said that the Justice Department informed you.

Mr. MULLIGAN. They came to us on December the 12th and indicated they had a handful of cards that had been compromised, and potentially one of the locations that was compromised with Target. At that point, there was no indication or evidence that there had been a breach. We found that breach 3 days later and shut it down within 12 hours.

Ms. SCHAKOWSKY. I actually wanted to talk more about the breach of marketing data and which affected fully one-fourth to one-third of all American adults, which is pretty serious, and I am asking these questions because I believe the breach of marketing data represents really a serious threat to consumer. Payment card breaches are severe incidents that criminals tend to obtain card data, spend money when they can, and then move on, but names and contact information can be used in phishing and social engineering schemes to try to perpetrate identity theft, and so while harm from payment card breaches are acute, harm from nonfinancial breaches linger, identity theft lasts.

So, I wanted to ask you about the way you informed the consumers who had these marketing data breaches. Some consumers received an email message during the week of January 12th noti-

fying them of a breach of Target customer information and received that message from TargetNews@target.bfi0.com, and scammers sometimes use legitimate names of companies and many people were alarmed when they looked up the domain name and found "permission denied" message. And so I wanted to know how Target determined it would contract with a company to send these messages and what you are doing about the confusion that consumers may have felt.

Mr. MULLIGAN. Congresswoman, we wanted to notify, confirmed on January 9th that that data had left our system, and on January 10th we started notifying consumers. We sent out 56 million email addresses. That was the number we had available to us. We also, as we did in the first breach, prior to broad public disclosure of the issue so that everyone would have information related it to, but one of the things we did and a couple of things we did in response to some of the concerns you are talking about, first, we communicated to our guest that there was a single of truth on our corporate target.com Web site. Any communication coming from Target was located there and could be trusted.

Second, we provided free credit monitoring which provides free identity theft protection, identity theft insurance for——

Ms. SCHAKOWSKY. Let me refer to that. There was a briefing organized Monday by the Bipartisan Privacy Caucus, Ed Mierzwinski of U.S. PIRG who said that credit monitoring, such as the one offered by Target, doesn't stop fraud on existing accounts and won't prevent new account identity theft. So I'm wondering what the rationale is for this program, its performance so far, and any ongoing alternatives or improvements being considered or developed by Target.

Mr. MULLIGAN. My understanding, Congresswoman, is that consumers have no liability for any fraud which occurs on their cards as a result of this breach. A part of the package that we offered in the free credit monitoring is identity theft protection, identity theft insurance, and access to a frauds protection specialist so that any guest who has ever shopped a Target store has the ability to contact them well past the year and ensure that their data is safe.

Ms. SCHAKOWSKY. So you would disagree with that conclusion that it doesn't stop fraud on existing accounts and won't prevent new account identity theft?

Mr. MULLIGAN. I can't speak to that data specifically. What I can tell you is consumers have no liability for fraud on their accounts that are a result of our breach.

Ms. SCHAKOWSKY. You are talking about fraud of——

Mr. MULLIGAN. Of existing accounts. I am sorry.

Ms. SCHAKOWSKY. Are you talking about fraud in a purchase? I am talking about identity theft.

Mr. MULLIGAN. And we provide identity theft protection as part of the free credit monitoring.

Ms. SCHAKOWSKY. Thank you.

Mr. TERRY. Thank you.

I now recognize the vice chairman Mr. Lance of New Jersey.

Mr. LANCE. Thank you very much. Mr. Chairman

To Mr. Mulligan. You testified that you were informed of the breach by law enforcement on December 12th and 13th, hired a fo-

rensic firm on the 14th, and on the 15th you both discovered the infiltration, removed the malware from your point of sale network. If it was relatively easy to find the malware once you were made aware of it, why wasn't it detected through your existing information security procedures?

Mr. MULLIGAN. It is excellent question, Congressman, one we have asked many times. Our ongoing forensic investigation, we believe, will provide the facts of what transpired and why the significant investments we have made in multiple ways of detecting and ensuring our systems are safe did not detect this.

Mr. LANCE. Can you give the committee an estimate as to when you might know the answer to that question?

Mr. MULLIGAN. That investigation is being led by our forensic investigator. They will take the time they need to assess all of the facts, and certainly from that there will be learnings and we will take action, so I don't have perspective on how long that will take.

Mr. LANCE. Thank you.

In addition to the 40 million payment card accounts that were breached, your company also detected a breach involving other personal information in 70 million consumers. Do you know, Mr. Mulligan, how many of the 70 million accounts would trigger a notice of breach under existing state laws.

Mr. MULLIGAN. I am not familiar with that, but as we considered that, what was important is, as we have had accurate and actionable information, we have disclosed information to the public, and that was our approach there. On January 9th, it was confirmed that that data was extracted from our systems, and on January 10th we provided broad public notice and began to email those guests for which we had email addresses.

Mr. LANCE. Thank you.

To Mr. Kingston at Neiman Marcus. From the time you first realized you had an actual problem in your system, and I believe that was January 2nd, until you disassembled the malware on January 10th, how did you conduct business with your consumers? Were POS terminals used during that timeframe to accept payments, and if so, how was that decision made?

Mr. KINGSTON. So, we did continue to conduct business for our customers during that time. However, as we were learning throughout the investigation more about this particular sophisticated attack, we immediately began implementing additional controls on top of all of the multi-layered security controls that we had in place at that time, and so being very, very careful with our forensic investigators as well as our internal investigation to closely monitoring for any further suspicious activity.

Mr. LANCE. Do you know yet whether the suspicious activity increased between January 2nd and January 10th?

Mr. KINGSTON. We have not seen any indication of that, no.

Mr. LANCE. So that is an open question or are you likely to concluded that——

Mr. KINGSTON. No additional suspicious activity was noted.

Mr. LANCE. Thank you.

To the panel in general, as card security evolves, it seems as though the chip is a better mouse trap. With a chip enabled card, the critical pieces of consumer information are obscured from would

be thieves, and the ability to prevent card duplication is achieved. But there are two types of chip enabled cards, as I understand it, those that require a PIN and those that require signature for authorization. To our experts, what is the difference between the two and what do you believe is preferable?

Mr. Russo, why don't we begin with you.

Mr. RUSSO. Well, the combination of PCI and EMV in any form, be that chip-and-PIN, be that chip and signature, is a powerful, powerful solution for as you indicated face-to-face fraud and counterfeit cards. However, there are other channels that that data can still be used, and so the powerful combination of PCI and EMV, once again, in any form is a powerful combination, and I think is something that needs to be considered.

Mr. LANCE. And from your professional perspective, who should consider that? Should this be required statutorily by the Congress or should this be determined at state capitals or should it be at the option of the private sector?

Mr. RUSSO. That is beyond the purview of what the standard and the security council does. Basically, we are responsible for securing that data in whatever form it comes in, so be it chip-and-PIN, chip and signature, regardless of who have determines what it is going to be and when it is going to be, our job is to make sure that that is protected.

Mr. LANCE. Thank you, Mr. Russo.

Mr. Smith, do you have an opinion on my question?

Mr. SMITH. I think the important point here is it is an additional layer of secure, right. There is no silver bullet here. There is multiple layers that need to be put in place. Chip-and-PIN with end-to-end encryption will certainly help matters, but again, nothing is going to stop the data breaches

Mr. LANCE. And would you require this as a matter either a statutory law or rule and regulation or does that go beyond what is probably appropriate for Congress, given the fact that technology advances as rapidly as it does?

Mr. SMITH. Again, the chip-and-PIN technology has been around for a long time. I think a lot of effort should be put for new technology in securing mobile payments and things like that. The technology is changing so quickly. The attack factors are going to change, right, so much more is going to the mobile side. So, implementing chip-and-PIN is a good thing for the face-to-face transactions, but having innovation towards mobile payments and other areas is just as important. Again, it is defense in depth.

Mr. LANCE. Thank you.

I have 12 seconds left. I look forward to working with everyone on the committee, and I personally enjoy shopping at Target, and I think my wife at Neiman Marcus.

Mr. TERRY. Mr. Yarmuth, you are now recognized for 5 minutes.

Mr. YARMUTH. Thank you, Mr. Chairman.

Likewise, long time customer, first time questioner, and I appreciate your testimony and your candor and forthrightness, particularly from Target and Neiman Marcus, and not that you are not being forthright.

One thing that I am curious about is that while we have some more instances of this type of breach, and I don't know if you want

to speculate why people might have singled out Target and Neiman Marcus among a group of retailers, but obviously there are a lot of retailers out there, many of whom with probably as much of a high profile as you, and my question is, are you aware, are you able to discuss with your colleagues in the industry whether they have been able to head off any cyber attack that might distinguish them in some way from your operations, or have you been informed by law enforcement of any other attacks that have been fended off? And I open it up to Mr. Russo and Mr. Smith as well.

Mr. MULLIGAN. Maybe I can start. We took several steps, once we verified there was malware in our point of sale systems. We have an ongoing relationship with law enforcement and certainly shared that with them. We also shared the malware with security firms who work with all businesses to look for these types of malware.

Beyond that, we have pushed for and are beginning an initiative with the retail industry around information sharing across all retailers to share this kind of information. It is an evolving threat. It is a shared responsibility for all of us, and we believe information sharing is one path to understanding the evolving threat and how we will collectively deal with it.

Mr. YARMUTH. I am just curious as to whether there is any indication that you have from any other source that somebody tried to attack Sak's Fifth Avenue, somebody tried to attack Walgreen, somebody tried to attack Wal-Mart, and they had failed where they succeeded in your instance. Is there any evidence of that somewhere?

Mr. SMITH. I will take a look at that. I think we describe this as a battleground every day. There are attacks going on constantly and those attacks are being defeated. The situations we are talking about are, again, sophisticated malware, but every day, retailers, banking industry, they are defending their networks against ongoing attacks, and I think that is an important point that there is a lot of effort going on today and will continue to go on. And again, increasing innovation around security technology is an important part of that, and I think that is where a lot of the players can come together and spur that innovation.

Mr. YARMUTH. All right. Is there any legal impediment to your comparing notes and talking to other competitors even? Is that something that should be, you say you are sharing information but——

Mr. MULLIGAN. We can totally benchmark, too, as well. Part of our ongoing assessment of all our particular program is to benchmark against other retailers and ensure that collectively we are providing the best protection.

Mr. YARMUTH. But specifically with regard to Target, there have been reports that some individuals received Target's notification of a data breach when they have never shopped at Target and some of it is a decade old. Are those reports accurate, and if that is the case, how would they be in your database if they had never shopped there?

Mr. MULLIGAN. Congressman, the vast majority of the data we collect is done through the normal course of business. When a guest uses our app on an iPod, when they sign up for an app called

"Cartwheel," we periodically append information to that on an existing guest, and very rarely, but from time to time we do buy some guest information to provide them promotions if we think they would benefit from the products and services that we provide.

Mr. YARMUTH. Now, you have had a relationship with Amazon for a period of time. Could any of that information have been captured because of that relationship specifically? Is that irrelevant?

Mr. MULLIGAN. It is my understanding that there was a separation of the information between Amazon's customers and our guests.

Mr. YARMUTH. OK. Well, I yield back. Thank you for your testimony. I yield back, Mr. Chairman.

Mr. TERRY. OK. At this time the Chair recognizes the vice committee of the full committee, or vice chairman of the full committee, Marsha Blackburn.

Mrs. BLACKBURN. Thank you, Mr. Chairman, and I want to thank you-all for your patience this morning. I cannot tell you how so many of our constituents have mentioned their frustration with the data breaches and their desire to get some clarity and some certainty in this process, and as you have heard me mention in the earlier questioning and opening statement, Mr. Welch, Ms. Schakowsky, and I are doing a data security and privacy working group to make certain that what we do when we do something on the issue, that we do it in the appropriate manner and that be allowed the flexibility and the nimbleness that is going to be needed. And Mr. Russo, you spoke well to the need for that.

Mr. Kingston, if I could come to you, and going back to your testimony with the malware that was there in your breach, have any of the law enforcement agencies that are working with you on this, have they ever seen this type malware before, and what is the origin of that malware?

Mr. KINGSTON. Congressman, we have been working very closely with law enforcement, specifically with the Secret Service, and what they have been able to share with us so far is that the malware is very, very, very sophisticated. As I said earlier in my testimony, had a zero detection rate by antivirus software, and it is not something that they have seen before. It was very specifically designed for an attack on our systems.

Mrs. BLACKBURN. OK. So it was designed specifically for an attack.

Mr. KINGSTON. Yes.

Mrs. BLACKBURN. And do you know the origin yet?

Mr. KINGSTON. They have not shared that with us. I am not sure at this time.

Mrs. BLACKBURN. They have not. OK.

Mr. Russo, when you look at this, and here is something designed specifically to attack and to take down their financial infrastructure, if you will, then what is your guidance to us as we seek to look at that data share, which is important, that information share, which is important. Mr. Zelvin spoke to that in the previous panel. What is your instruction to us? Because we know that the different agencies send out threats and updates on a regular basis, and you have something that is unique, so what is your instruction to us? And then the second question I have for you in the interest

of time is what are the unique identifiers that you are seeing creep up in some of this, this malware?

Mr. RUSSO. So, first of all, the council is a wonderful forum in which to share information. Companies give us feedback all the time as to what is going on. The forensic investigators tell us about trends that they are seeing, which all gets factored into creating these standards and making sure that they are not only good for today but good for what we see coming in the future.

So, it has been our experience that the standards are very, very solid. We have a lot of history around this. I think we have heard two or three times, as I can recall, during the hearings the morning, that what we saw and what we continue to see are basic threats that are being exploited, very basic threats. You have heard me say, you heard Mr. Smith say about passwords being used and so on, SQL injection is another one, lest I get technical here, very, very basic things.

Within the standards now, there are a myriad of ways to prevent this from happening and to prevent malware, as sophisticated as it may be, from getting into the system. So, at this point I don't have enough information in terms of what actually happened, but I can tell you, up until now, everything that we have seen in terms of these major breaches over the last 7 years has been exactly what the panel before us indicated, very, very basic exploits that easily, easily could have been defeated. So, until we actually have some solid information as opposed to what we are reading in the newspapers, we really can't make a determination as to what happened and if the standards need to be updated.

Mrs. BLACKBURN. I hope you will come back to us. When you look at standards and compliance, and we know even going back to the T.J. Maxx breach, they were compliant, they just weren't secure, and there is a difference there.

Mr. Mulligan, at Target, how much have you-all invested in secure networks?

Mr. MULLIGAN. Over the past several years, we have invested hundreds of millions of dollars. Part of that has been in technology, segmentation, malware detection, intrusion detection and prevention, data loss prevention. Part of that has been in teams. We have over 300 team members responsible for information security. Part of that is in assessment.

PCI is one assessment that we do certainly as part of the payment card industry. But we are constantly assessing ourselves, having other third parties come in and do penetration testing, benchmarking us against others and benchmarking us against best in class. And we train 370,000 team members annually on the importance of information security, so we have a wholistic view and we have invested significantly.

Mrs. BLACKBURN. OK. Mr. Kingston, how much has Neiman spent on security?

Mr. KINGSTON. So, we have spent tens of millions of dollars on very specific security measures, and as Mr. Mulligan said, it is really a combination of technology as well as people and process. I think one of the things that we do at Neiman Marcus that is really important that I think the subcommittee should think about is the fact that we do annual security awareness training for all

Neiman Marcus associates that access systems, and I think awareness is a big part of strong defense.

Mrs. BLACKBURN. Yes. Well, my time is expired. I will yield back.

Mr. Mulligan, I am going to submit a question to you for a written answer on the CVV security codes.

Mr. MULLIGAN. Happy to respond.

Mr. TERRY. Thank you. And the Chair now recognizes another gentleman from Kentucky, Mr. Guthrie.

Mr. GUTHRIE. Thank you, Mr. Chairman. Thank you for coming. So, Mr. Russo, to follow up on what Ms. Blackburn asked, or you said, to answer her question, you said that these breaches, I guess the two that we are talking about today were basic?

Mr. RUSSO. No, today's breaches, I don't know——

Mr. GUTHRIE. I could have been defeated?

Mr. RUSSO. We don't have enough information yet.

Mr. GUTHRIE. You said that basically it could have been defeated?

Mr. RUSSO. What we heard this morning from the other panel was all of the breaches up until now——

Mr. GUTHRIE. OK

Mr. RUSSO [continuing]. Have been basic security exploits that could have easily been prevented, and we don't actually know what the situation is yet from the latest breaches.

Mr. GUTHRIE. OK. So, but because I knew that Mr. Kingston said that they had zero detection rate by their software. It didn't sound basic. So, I mean, OK, I am willing to clarify what you said then. But based on what you do know, were Target and Neiman Marcus compliant to the PCI standards?

Mr. RUSSO. Unfortunately, they do not report their compliance to the council. The council, like many other security bodies, basically puts together the best standards that we possibly can. We are not responsible for enforcement or——

Mr. GUTHRIE. Right. I knew that.

Mr. RUSSO. Nor do people report their compliance to us.

Mr. GUTHRIE. OK. So, there is no——

Mr. RUSSO. We have no insight as to whether or not they were compliant or not.

Mr. GUTHRIE. You can't assess whether they were meeting the standards or not.

Mr. RUSSO. Absolutely not.

Mr. GUTHRIE. So that is something to look at. So, one of the other previous panelists said basically, I can't remember the word, was retailers or business, but in essence she said in her testimony to get serious, it is time to get serious about this. You said you spent hundreds of millions of dollars, you spent tens of millions of dollars.

How much do you think this incident in December and then January, first with Target, I know you are the CFO. I know you as the information officer, you may not know, but what do you think this has cost your bills in terms of dollars? Not on customer loyalty, customer anything, but just in terms of dollars.

Mr. MULLIGAN. We don't have insight into that yet. We disclosed publicly, probably 3 weeks ago, that the losses as a result of this incident would be material to Target. I don't have visibility. The

primary driver here is fraud. I don't have visibility of that from the majority of the financial institutions, but what I can tell you is this: of the 40 million accounts that were taken, 6-and-a-half million of them or 15 percent were Target cards, and what we have seen is on our Target Red Card, the proprietary card, our Target debit card, there has been no additional fraud, and on our Target Visa card, which is a Visa card just like any other, we have seen very low levels of fraud. So, we will have more information as we go through the process.

Mr. GUTHRIE. So Neiman Marcus, what kind of expense or cost has this been to your business?

Mr. KINGSTON. We are still in the midst of our investigation, so you know, I don't have visibility to that yet.

Mr. GUTHRIE. And then, Mr. Smith, we are hearing from two Fortune 500 companies, very sophisticated companies, that have sophisticated systems in place, it appears, and they are still breached by very sophisticated criminals. So what about the small guy? I know that is the kind of the area you look at, if you are, where I get gasoline and gas at the pump and a small locally-owned station, what processes are in place for these guys?

Mr. SMITH. Well, again, the PCI standards are across the board for any store who transmits or processes data. You know, the smaller merchants have a smaller platform to be attacked, right, so they are able to defend their smaller presence on the Internet. There are lots of, as Mr. Russo alluded to, basic security principles that they can put in place, relatively cheap to protect their network and their data. And there is a lot of information out there including on our Web site for the small merchants to, what technologies, what they should be putting out there.

Mr. RUSSO. If I can interject.

Mr. GUTHRIE. Sure.

Mr. RUSSO. Being a small merchant is a very tough thing these days. You not only have to worry about shoplifting and somebody breaking into your store, but you now have to worry about data security.

In an effort to make that a little bit easier, as Mr. Smith indicated, on our Web site we certify different solutions that they can go and choose. Not only do we certify different solutions in the form of payment applications, as well as POS devices that are secured and certified to be PCI compliant, but also, we train installers throughout the Nation so that a small merchant, as opposed to using his brother-in-law, to help install a piece of software can actually go out and pick somebody off this list to securely install this information for them.

So we make it easier for the smaller merchant, but again, the small merchant area is a very, very big problem.

Mr. GUTHRIE. Because they would be a portal into a whole——

Mr. RUSSO. Absolutely.

Mr. GUTHRIE. So one of the other panelists also said that there is a list of different things people can do and they will do some, but they won't do the others. Is that the case with your, did you look back and say, wow, there was something we should have known to do that we didn't do? Or is it, this was so sophisticated

that it went around a very sophisticated system that you had. I guess I am out of time, I'm sorry.

But one of the panelists earlier basically said that. Not necessarily your situation, but situations that there could have been a check box and they decided not to check because it cost money. I mean, that is what she said. Not word for word, but is that what you all found to be the case, or has it been so sophisticated that you had everything in place and you say, wow, I can't believe they can get around that? Or did you find something obviously you should have found.

Mr. TERRY. Go ahead. But then you are done, Brett.

Mr. GUTHRIE. OK.

Mr. MULLIGAN. Congressman, as I said, we invested hundreds of millions of dollars in technology and assessment. Part of the ongoing end-to-end review of our systems will provide facts when that is complete and there will be learning, certainly, and we will respond to those learnings.

Mr. GUTHRIE. But there wasn't something obvious you didn't do that led to this?

Mr. TERRY. Brett?

Mr. Kingston, answer.

Mr. KINGSTON. I think at Neiman Marcus, we felt, and feel very good about the high standards of security that we had in place, and that we continue to have in place.

Obviously, there will be lessons learned out of this, and certainly one of the takeaways so far, this is a very highly sophisticated attack.

Mr. TERRY. Mr. Johnson, you are recognized for 5 minutes.

Mr. JOHNSON. Well, thank you very much, Mr. Chairman.

And I, as I mentioned to the first panel, I spent my entire professional career as an IT professional. One of those stents was as the director of the CIO staff for U.S. Special Operations Command, and you don't have an environment that is any more concerned about network and computer security than our national security. I mean, that is paramount.

So I understand the complexities that you folks have to deal with on a daily basis to address this and I can empathize with the struggles that you have.

Just real quickly, just a few questions. Mr. Mulligan, why hasn't Target joined the financial services ISAC, the Information Sharing and Analysis Center?

Mr. MULLIGAN. I don't know the answer to that specifically, Congressman. I can tell you we have a long history of sharing information with law enforcement as it relates to these type of threats, and we certainly believe that information sharing, a shared responsibility across all industries is essential to dealing with this type of evolving threat.

Mr. JOHNSON. Is this most recent incident, has that given you thought to consider joining?

Mr. MULLIGAN. Certainly, Congressman, and in fact, as I stated earlier, we have implemented at least one step of that with retailers for information sharing, but yours is another that we are absolutely open to.

Mr. JOHNSON. What about large retailers like you folks? Do you think it is time for large retailers like you guys to consider having your own ISAC?

Mr. MULLIGAN. We absolutely believe that information sharing is important, Congressman, absolutely.

Mr. JOHNSON. OK, what about empowering law enforcement to share information with the private sector with respect to ongoing threats and attacks? Do you think that is important also?

Mr. MULLIGAN. We do. We have had an ongoing relationship with law enforcement at many levels and have enjoyed a great relationship with them historically, and certainly during this period of time as well.

Mr. JOHNSON. OK. Mr. Kingston, what are the systems that you had in place to guard against a data breach, and why did they fail in this case?

Mr. KINGSTON. So Congressman, we had a multi-layered security approach and architecture in place, and I will just highlight some of the controls and different technologies. So we had network behavioral analysis and monitoring technology in place. We had network segmentation with the use of firewalls and controlled intrusion detection systems, two-factor authentication for remote access. We also deploy encryption technologies, and we also utilize tokenization as a method to protect and secure consumer information that is stored in our system.

Mr. JOHNSON. So, and that sounds pretty robust. I mean, it is the traditional kinds of things that folks do to provide network and data security. Why do you think those things failed, just the sophistication of the attack?

Mr. KINGSTON. So you know, with what we have learned so far, and again, there are still some important questions that we haven't answered in our investigation, but with what we have learned so far, it really points back to the malware being so sophisticated and customized to specifically evade those different technologies and detections. Just to give you an example, this particular malware was able to inject itself into known point-of-sale programs, so that it could disguise itself and continue to operate as if it was a normal program.

And then it was able to delete itself and clean up its tracks, so very, very complex, very difficult to detect.

Mr. JOHNSON. Yes, yes. You have emphasized the sophistication of the attack. You just talked about that, even customizing the malware so it wouldn't be detected by today's current antivirus programs. Can the criminals always stay one step ahead of us like they appear to be doing in this case? Is that a battle we are going to face?

Mr. KINGSTON. Clearly, it is going to be difficult for us, both public and private sector. I certainly hope one day we get to a point where we can at least be on par, if not ahead of the criminals.

Mr. JOHNSON. OK. Does your recent experience equip you to try some different techniques? Have you guys started thinking about how do we make sure that they can't get through, and then once they get through, that we can detect them?

Mr. KINGSTON. I think, undoubtedly, with the things that we are learning through this investigation with the help of our forensic

teams and with the help of law enforcement, there are definitely going to be things that we can consider to help even further strengthen the security that we have in place today.

Mr. JOHNSON. Sure. Well, I have a gazillion questions, Mr. Chairman, and I don't think you are going to give me a time to ask them so I will yield back.

Mr. TERRY. Not a gazillion, no, but we will let you have one more after everyone else if you want to stay.

Mr. TERRY. Mr. Bilirakis, you are now recognized for 5 minutes.

Mr. BILIRAKIS. Thank you, Mr. Chairman, I appreciate it very much.

And I appreciate the panel's testimony today. And thanks for your patience as well.

Mr. Mulligan, thank you again for testifying. In your testimony, you note that December 16th and December 17th, you began notifying the payment processors and card networks, and on December 19th, made a public announcement regarding the breach; and is that true?

Mr. MULLIGAN. That is accurate.

Mr. BILIRAKIS. OK, all right. Given that 47 states as well as the U.S. and the U.S. territories have developed data breach notification laws, often with different requirements, standards of harm, and definitions of personally identifiable information, did you or your company find it difficult to navigate through these different standards?

Mr. MULLIGAN. Our focus, once we realized the malware was on the system, we had two parallel tracks that we were pursuing. The first was to shut down the malware, and then assess what it was doing, and once we verify that it was taking payment card information, we wanted to notify the processors, and the brand so that they could begin their fraud deduction and fire up their fraud detection policy.

The second path was on providing public notice as soon as we had the scope, we had actionable information for our guests, and had built the resources to respond what we knew invariably would be a significant call volume.

Mr. BILIRAKIS. Well, again, I want to ask the question: Was it difficult to navigate this process since, what is it, 47 different States have different laws, and I know you are everywhere around the U.S.

Mr. MULLIGAN. It is my understanding that the majority of those States' statutes provide for broad public disclosure. We provided broad public disclosure on the 19th. As I am sure you know, we were on the front page of every newspaper on December 20th, and so that was our approach. We also provided notice to 17 million guests by email for the guests that we had.

Mr. BILIRAKIS. OK, should there be, in your opinion, a National standard with regard to notification, notifying customers?

Mr. MULLIGAN. Certainly, one standard would be easier to follow than 47, but we complied with all 47 state statutes.

Mr. BILIRAKIS. Thank you.

Mr. Kingston, the same question, should there be a National standard as far as notifying customers?

Mr. KINGSTON. I mean, I don't have an opinion on whether there should be a National standard. I would say that it is important that there be flexibility within whatever legislation standard you have, because I do think, as was noted in the first panel, these investigations, these events are different, and on a case-by-case basis, need to be handled differently.

Mr. BILIRAKIS. Anyone else on the panel wish to comment on that? Should there be a national standard?

Mr. RUSSO. Outside the purview of the counsel.

Mr. BILIRAKIS. OK. Next question, in 2015, liability for fraud losses will be to shift from card issuers to merchants. Mr. Mulligan, you said you are accelerating chip technology for Target's red cards. Do you believe the switch to chip-and-PIN can save money in the long run?

Mr. MULLIGAN. We have been advocates to moving to chip-enabled technology, and chip-and-PIN technology over a long period of time, and while it certainly doesn't resolve all of the issues, it is a significant step forward for our industry in ensuring that that data is safe. So we have been proponents. We are in the middle of rolling it out. We have 300 stores already deployed with guest payment devices, what we call, where you read the cards. We will finish that by the fourth quarter of this year, and early next year all of our credit products, the payment products we offer will also have chips embedded on them.

Mr. BILIRAKIS. Very good. Will it save money in the long run?

Mr. MULLIGAN. We believe so.

Mr. BILIRAKIS. All right, very good, Mr. Kingston.

Mr. KINGSTON. Sir, we are actively evaluating PIN-chip technology at Neiman Marcus, and we will certainly, if consumers are issued cards with PIN-chip in them, be ready and able to support those transactions.

In addition, we are also looking at other technologies that can also protect Neiman Marcus consumers that shop online. We have a very robust online business which PIN chip doesn't necessarily address, as well as the growing trend for mobile payment transactions. So we believe that while PIN chip technology is certainly going to enhance security, that there are other solutions out there that we also will evaluate.

Mr. BILIRAKIS. Thank you.

Again, for Mr. Smith, do you believe it will save money in the long run? You know, the switch to chip and PIN?

Mr. SMITH. I can't really comment on the savings, but you know, any security technologies that can be deployed to protect cardholder data, you know, we would be supportive of.

Mr. BILIRAKIS. Mr. Russo?

Mr. RUSSO. I agree with Mr. Smith. Certainly, it will be yet another level of security that is important.

Mr. BILIRAKIS. And that is our priority.

Thank you very much, I appreciate it. Thanks for your question. I yield back.

Mr. TERRY. Thank you, Mr. Bilirakis. Now, you may think this is over, but we have agreed between us to have a second round. It is just that everybody has left but us two. So the lucky part is that you are only going to get two extra questions.

So my question to you is going to be to Mr. Mulligan and Mr. Kingston, on specifics about audits and when they are done, and when you last did them before the breaches were discovered.

Mr. Smith, I want you to answer it more not Neiman Marcus, or Target-specific, but what is appropriate for audits and when they should be done, and how frequently pursuant to your expertise and professional opinions.

So with that, as I understand, the process or norms are that you do audits throughout the year on your security systems. So how often do you do those and when was the last time an audit was done on your security before you discovered the current hacks and malware that brings you before us today?

And also, do those audits include password integrity and possible phishing, procedural process, or process deficiencies.

Mr. Mulligan?

Mr. MULLIGAN. We have a robust audit plan or assessment plan, I would call it more broadly. Certainly it starts with PCI assessment, which is done annually. It takes 9 months. We have that performed by a third party. That is one step.

But beyond that, we have ongoing assessments, Congressman, penetration testing, assessing our technology, the people, the processes, the controls we have in place. It would be all-encompassing. And we have a multiple of those every year.

We had a third-party global firm assess us against Fortune 100 retailers just last year and we were at or better than the technology deployed in those retailers. So it is an ongoing part of our data security program.

Mr. TERRY. So the other two parts of that, though, was when was the last one done, and does that also include password integrity?

Mr. MULLIGAN. I am not sure. I can't give you the exact date of our last one. It would include password protection because it looks broadly at all of our processes. I am happy to get you a date.

Mr. TERRY. All right, thank you. Mr. Kingston.

Mr. KINGSTON. Chairman, I will answer the last part of the question first. Our audits do address password integrity, but we have several different forms which we audit and assess our security controls, so I will start with periodic audits of IT general controls, which include password strength and controls. We also do a quarterly scan, a penetration scan of the perimeter to see what potential vulnerabilities or risks are coming into the networks as well as the internal networks. And then the last part of the assessment that I point out is under PCI.

Mr. TERRY. All right. Mr. Smith?

Mr. SMITH. You know, we conduct annual assessments under PCI for our clients all the time. In addition to that, working with our clients as partners, we do active penetration testing, active testing all the time depending on if there is an incident or if there is a security issue, or there is an area that they want tested. We are constantly going in and out of organizations, you know, frequently to test their systems.

Mr. TERRY. How often?

Mr. SMITH. I think it is going to depend on a PCI compliance. It is an annual testing.

Mr. TERRY. All right.

Mr. SMITH. But as part of that, we do frequent, you know, vulnerability scanning.

Mr. TERRY. OK.

Mr. SMITH. But again, if you are looking at beyond that, we are actively involved with many of our clients doing active penetration testing on an ongoing basis——

Mr. TERRY. All right.

Mr. SMITH [continuing]. Through all of their applications.

Mr. TERRY. Thank you. Ms. Schakowsky, you are recognized.

Ms. SCHAKOWSKY. Thank you.

I really do want to thank the gentlemen representing Target and Neiman Marcus for your patience today and for coming here, as the chairman said, willingly, and sitting through a long hearing. So I think that should be noted, and for your openness and willingness to cooperate. But I have been disturbed, not necessarily by what you have done, but there have been some efforts in the courts to undermine the ability of government to actually act in the area of data security.

Since 2002 the Federal Trade Commission has applied its enforcement authority under Section 5 of the FTC act to the area of data security by bringing legal actions against companies that fail to reasonably protect customer data. Last week the FTC announced its 50th data security settlement.

But in the court, there is a case FTC versus Wyndham that is currently pending in the U.S. District Court for the District of New Jersey, and Wyndham is challenging the FTC's use of its unfairness authority to insist that companies have minimum data security standards in place. And an amicus brief has been filed by the Retail Litigation Center, an arm of the Retail Industry Leaders Association, which I know at the very least that Target is a member of, together with the U.S. Chamber of Commerce, the American Hotel and Lodging Association, and the National Federation of Independent Businesses, which are in support of that position.

So I am just wondering from both of you, if you are part of those amicus briefs through these associations, and whether your companies agree with the position taken by Wyndham and that the FTC lacks authority to enforce reasonable data security measures. Mr. Mulligan?

Mr. MULLIGAN. I can begin. I should first note, Mr. Chairman, to your question about the last assessment. We were found PCI-compliant on September 20th of 2013.

To your question, I am not familiar with that. What I can tell you is that we are committed to making this right, and we are committed to engaging on this topic. And we are willing to do so independent of RILA. Target is willing to engage on this topic.

Ms. SCHAKOWSKY. Thank you, Mr. Kingston.

Mr. KINGSTON. So I am not intimately familiar with that legislation or those issues either, but——

Ms. SCHAKOWSKY. This is a court case.

Mr. KINGSTON. And I apologize, I am not familiar with it. But I will tell you that Neiman Marcus supports having standards in place for data security and which is why we are actively a participant in the PCI standards and assessment process, and will often look to not only meet those, but exceed them.

Ms. SCHAKOWSKY. Let me just finish in saying I hope both of you would just talk with your companies and see if you are part of something that would undermine the ability of the FTC to protect consumers in cases of data security breaches. Thank you.

I yield back.

Mr. TERRY. And that does conclude all of our questions.

You can start wrapping up, but we will probably submit questions, or at least every one of us have the right to send you questions. We will try and get those to you if there are any to you individually within 14 days, and ask the same amount of time to return an answer.

Now, just some general business here. I ask unanimous consent to include the hearing record statements from the following four organizations: Credit Union National Association, Independent Community Bankers of America, National Retail Federation, Retail Industry Leaders Association. All of these have been shared with the minority, without any objection?

Ms. SCHAKOWSKY. No.

Mr. TERRY. Hearing none, so ordered. Now, we are adjourned. Thank you gentlemen.

[Whereupon, at 12:51 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

CUNA
Credit Union National Association

Bill Cheney
President & CEO

February 5, 2014

The Honorable Lee Terry
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade
Committee on Energy and Commerce
United State House of Representatives
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce,
Manufacturing, and Trade
Committee on Energy and Commerce
United State House of Representatives
Washington, DC 20515

Dear Chairman Terry and Ranking Member Schakowsky:

On behalf of the Credit Union National Association (CUNA) and America's credit unions, I am writing today to thank you for holding today's hearing entitled "Protecting Consumer Information: Can Data Breaches Be Prevented?" CUNA is the largest credit union advocacy organization in the United States, representing America's 6,700 state and federally chartered credit unions and their 99 million members.

This hearing is an important and timely response to recent merchant data breaches affecting millions of Americans and their financial institutions. We appreciate the Subcommittee's focus on safeguarding consumer data, and we look forward to today's testimony and discussion of what should be done to ensure an appropriate response to not only these data breaches, but data breaches that may occur next week, next month, or next year.

We encourage Congress to take a holistic approach to this issue. In the years to come, consumers will use many payment methods, including magnetic (mag) stripe cards, chip and PIN cards (EMV), cloud-based mobile payments, tokenization, and other methods we can only imagine at this point in time. Focusing on one payment method as the absolute answer to solving data security breaches is both shortsighted and distracts from the greater need of a federal data security framework for all entities. Instead, Congress should take a broad look at how consumer data is secured and the improvements that are necessary to prevent future breaches from taking place.

Data breaches occur, in part, because merchants are not required to adhere to the same statutory data security standards that credit unions and other financial institutions must follow, and merchants are rarely held accountable for the costs others incur as a result of the breaches. All participants in the payment process have a shared responsibility to protect consumer data, but the law and the incentive structure today allows merchants to abdicate that responsibility, making consumers vulnerable.

Since the initial reporting of the Target data breach, credit unions have focused on protecting their members from harm, to the extent they can. They have taken many steps including, but not limited to, notifying their members that a breach had occurred, reissuing new debit and

credit cards to affected members, and increasing staff at call centers to account for additional member inquiries.

The impact of merchant data breach related costs is far reaching; for not-for-profit credit unions operating on already thin margins, these costs make a significant difference in their ability to offer services to their members. CUNA recently conducted a survey of credit unions regarding the costs they are incurring to help their members respond and recover from the recent breach at Target. Preliminary data indicates that credit unions are incurring a cost of approximately $5.10 per affected card and that the system has incurred a total estimated cost of between $25-30 million as a result of this breach. This figure will continue to increase because this data does not include fraud costs which may develop in the near future.

In addition to the actual costs credit unions must bear as result of the breach, they also face reputational damage because they have an obligation to notify their members that their account has been compromised but are often limited in their ability to disclose the name of the merchant where the breach occurred. So, when members are notified that their account has been compromised, the credit union is unable to tell them where the compromise occurred and some members assume the problem was with the credit union.

As Congress considers legislative remedies, credit unions support three basic principles:

1. All participants in the payments system should be responsible and be held to comparable levels of data security requirements.

Under current federal law, credit unions and other financial institutions are held to high standards of data security for consumer information under the *Gramm-Leach-Bliley Act*. There is no comparable federal data security responsibility for a national merchant holding consumer data. This represents a weak link in the chain and it needs to be addressed. We support legislation, such as S. 1927, the *Data Security Act of 2014*, introduced by Senators Carper and Blunt, that would provide a national standard for businesses to protect sensitive consumer information, rather than a myriad of differing state laws and regulations.

2. Those responsible for the data breach should be responsible for the costs of helping consumers.

It has been said by merchants that consumers will not be responsible for any financial loss in their accounts. That is true, but not because the merchant will reimburse affected consumers. It happens because the consumer's financial institution pays for the costs related to a merchant data breach involving accounts held at that institution. Under current law, the merchant is not obligated to reimburse financial institutions for any costs incurred as a result of the breach. In other words, even though the breach happened on the merchant's watch, retailers have no responsibility for the costs of the breach because financial institutions take care of their members and customers.

When a merchant data breach occurs, credit unions are there to help their members. Whether it is increased staffing to handle additional member questions, notifying members, reissuing cards, tracking possible fraudulent activity, or reimbursing a member for fraudulent charges

caused by a third party, credit unions bear the costs even though the merchant was responsible for the breach. We support legislation to address this problem and make it easier for credit unions to recoup the costs they incur. We believe that if Congress sets strong merchant data security standards and those standards are not met by a merchant whose data is breached, the merchant should be held responsible for the credit union's costs associated with that breach.

3. Consumers should know where their information was breached.

Credit unions also support legislation that requires merchants to provide notice to those consumers affected by a data breach, and permits credit unions to disclose where a breach occurs when notifying members that their account has been compromised.

When it comes to bad news like a data breach, it is easy to "blame the messenger." In today's world, the credit union is the messenger and, depending on the state, may not be permitted to identify the breach source to the consumer member. Consumers need transparency and knowledge to understand where their data has been put at risk. S. 1927 addresses this priority as well.

In conclusion, we look forward to the Subcommittee's dialogue regarding data security. It is a complicated and dynamic issue. As these latest merchant breaches have demonstrated, millions of consumers, and their respective credit unions, are affected. We believe the best answer is a federal comprehensive approach to data security.

On behalf of America's credit unions and their 99 million members, thank you for your attention to this very critical matter and your consideration of our views.

Best regards,

Bill Cheney
President & CEO

February 5, 2014

Protecting Consumer Information: Can Data Breaches Be Prevented?

On behalf of the nearly 7,000 community banks represented by the Independent Community Bankers of America (ICBA), thank you for convening today's hearing titled: "Protecting Consumer Information: Can Data Breaches Be Prevented?" Community bankers and their customers are deeply alarmed by recent, wide-scale data breaches at prominent, national retail chains. These breaches have the potential to jeopardize consumers' financial integrity and confidence in the payments system. This confidence is vital to sustaining consumer spending necessary for the economic recovery. It is critical we determine what happened, identify the weakest links in the payments processing chain, and implement targeted changes to enhance consumer financial data security. We appreciate the opportunity to offer the community bank perspective on this important issue.

Making Customers Whole

While all the facts of these breaches are not yet known, community banks are taking actionable steps to make credit and debit customers whole. Consumers are protected by a policy of zero-liability coverage with regard to any fraud losses. This coverage is primarily provided by community banks and other financial institutions. Financial institutions are required to provide this protection in order to issue Visa and MasterCard debit and credit cards.

With a vital stake in containing the damage caused by breaches and restoring consumer confidence, community banks absorb the upfront costs of reissuing cards, responding to customer concerns and inquiries, protecting against fraud and any other expenses. These costs may be significant depending on the scope of the breach. For smaller institutions, the cost of reissuing a single credit or debit card ranges from $10 to $15. In a wide-scale breach even a community bank may have to reissue thousands of payment cards. Community banks absorb these costs upfront because their primary concern is to accommodate their customers. However, we strongly believe that these costs should ultimately be borne by the party that experiences the breach. This is critical to aligning incentives to maximize data security by all parties that store consumer data.

While our current focus is on making customers whole, it is appropriate to begin to consider changes in policy, business practice, and technology that will strengthen payment system security and curb the risk of future breaches.

More Comprehensive Data Security Standards Are Needed

Since 1999, financial institutions have been subject to rigorous data protection standards under the Gramm-Leach-Bliley Act (GLBA). These standards have been effective in securing consumer data at financial institutions. To adequately protect consumers and the payments system, **all** participants in the payments system should be subject to GLBA-like standards. Under current law, merchants and other parties that process or store consumer financial data are not

1615 L Street NW, Suite 900, Washington, DC 20036 ▪ 202-659-8111 ▪ Fax 202-659-9216 ▪ www.icba.org

subject to federal data security standards. Securing financial data at banks is of limited value if it remains exposed at the point-of-sale and other processing points

Liability Should Be Used To Align Incentives

To maximize data security, the party that experiences a breach should bear responsibility for all costs associated with the breach. This change would better align incentives to keep consumer data safe and foster good business practices. As described above, when payment card information is compromised, mitigation costs are significant. If the party that experiences the breach does not bear these costs, they have little incentive to improve their data security.

New Technologies Will Reduce Risk But There Is No Universal Remedy

Community banks are already investing in technologies that will better secure transaction processing and thwart criminals. In particular, community banks are joining other financial institutions in the orderly migration to chip technology for debit and credit cards. Chip technology may not have prevented the recent retailer breaches but it would have reduced the market value of the card data as it would be far more difficult for criminals to make counterfeit cards. Using chip technology will not protect against fraud in "card-not-present" transactions, such as online purchases. Criminals will continue to try to find weakness regardless of the technology so it is crucial that the marketplace continues to have the flexibility to innovate.

Thank you again for convening this hearing. ICBA looks forward to working with this Committee to craft targeted solutions to enhance the security of consumer financial data.

National Retail Federation®
The Voice of Retail Worldwide

Statement
On Behalf of

The National Retail Federation,
The National Council of Chain Restaurants,
and Shop.org

For

The House of Representatives Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade's

Hearing on

"Protecting Consumer Information:
Can Data Breaches Be Prevented?"

February 5, 2014

Prepared by
Mallory Duncan
General Counsel and
Senior Vice President

National Retail Federation
325 7th Street, N.W., Suite 1100
Washington, D.C. 20004
(202) 783 –7971
www.nrf.com

Chairman Terry, Ranking Member Schakowsky and members of the Committee, thank you for holding a hearing examining data breaches and cyber crime. The National Retail Federation (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 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.

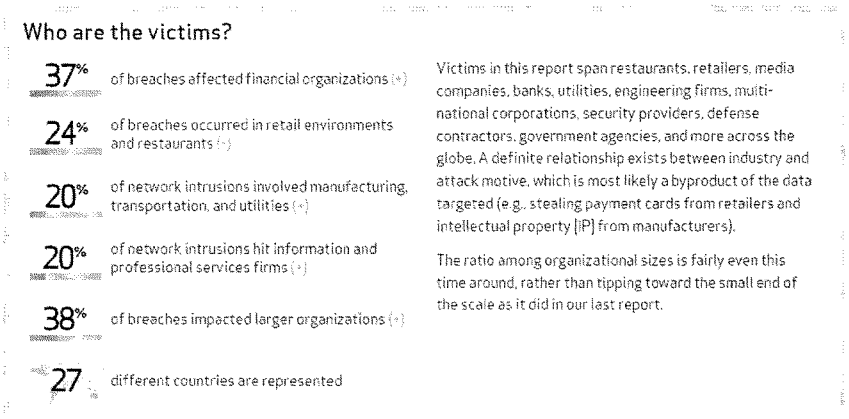
With that in mind, this testimony is designed to provide some background on data breaches and on fraud, explain how these events interact with our payments system, discuss some of the technological advancements that could improve the current situation, raise some ways to achieve those improvements, and 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% of breaches happened at financial institutions; 24% happened at retail; 20% happened at manufacturing, transportation and utility companies; and 20% 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% 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.

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

[1] 2013 Data Breach Investigations Report, Verizon.
[2] "Countries with the most card fraud: U.S. and Mexico," *Forbes* by Halah Touryalai, Oct. 22, 2012.

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]

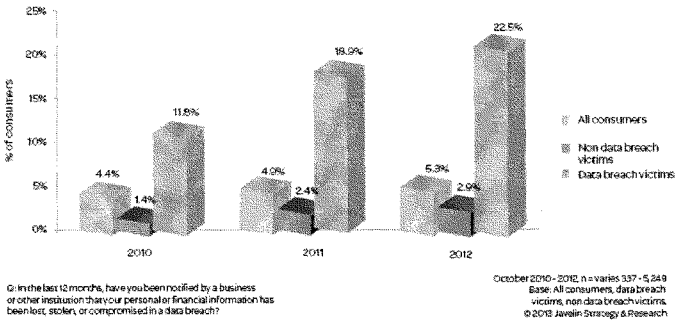
Fraud is particularly devastating for retailers in the United States. LexisNexis and Javelin Strategy & Research have published an annual report on the "True Cost of Fraud" each year for the last several years. The 2009 report found, for example, that retailers suffer fraud losses that are 10 times higher 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]

---

[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

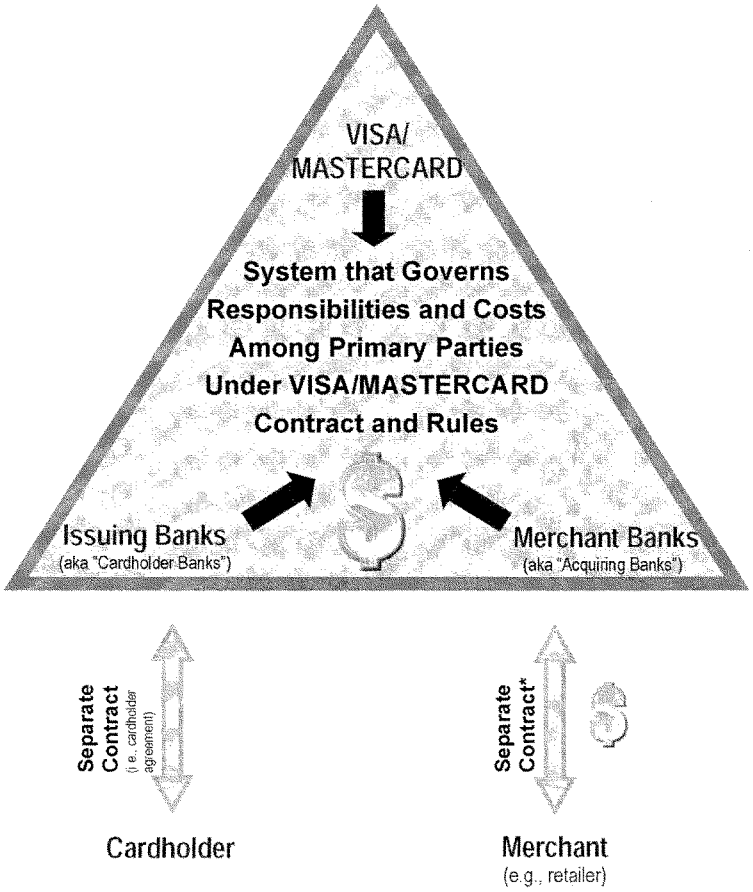
These numbers provide insights as to how to get to the right solutions of better safeguarding consumer and cardholder data and the need to improve authentication of transactions to protect against fraud. But before delving into those areas, some background on our payments system could be helpful.

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 recently, "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

[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/.

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-

[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.

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 directly 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.

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. That is a good next step for the United States. 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.[17] 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 1990's technology (chips) with a 1960's 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.

---

[17] 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.

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."[18]

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."

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.[19]

And, 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, I 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

[18] The Nilson Report, Issue 934, Sept. 2009 at 7.
[19] 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.

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, 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.

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.

RETAIL INDUSTRY LEADERS ASSOCIATION
Educate. Innovate. Advocate.

1700 NORTH MOORE STREET
SUITE 2250
ARLINGTON, VA 22209
T (703) 841-2300 F (703) 841-1184
WWW.RILA.ORG

February 5, 2014

Representative Lee Terry
Chairman
Subcommittee on Commerce, Manufacturing and Trade
House Energy & Commerce Committee
United States House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

Representative Jan Schakowsky
Ranking Member
Subcommittee on Commerce, Manufacturing and Trade
House Energy & Commerce Committee
United States House of Representatives
2322A Rayburn House Office Building
Washington, D.C. 20515

Dear Subcommittee Chairman Terry and Representative Schakowsky:

On behalf of the Retail Industry Leaders Association (RILA), I welcome the opportunity to offer our comments on the record relevant to the subcommittee's hearing, "Protecting Consumer Information: Can Data Breaches Be Prevented." 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 cyber-attacks nearly every day, unfortunately some attacks are successful and the resulting incidents can affect millions of our American 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.

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. Retailers 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. On January 27, RILA launched its Cybersecurity and Data Privacy Initiative which focuses on strengthening overall cybersecurity. As part of this initiative, RILA is forming the Retail Cybersecurity Leaders Council (RCLC) and calling for the development of both federal data breach notification legislation and federal cybersecurity 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.

In the weeks ahead, this Committee and others are likely to consider a range of legislative solutions to cybersecurity threats. RILA will engage with federal lawmakers and other stakeholders to develop sound and effective data breach notification and federal cybersecurity legislation that sets a national baseline to preempt the current patchwork of state laws and supports information sharing between the public- and private sectors.

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, actions with 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 and because of 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.

Also as part RILA's Initiative, RILA called for collaboration among retailers, banks and card networks to advance improved payments security. 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 the 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 have little doubt that all parties share the goals of protecting consumers and maintaining confidence in in our industry's cybersecurity. In order to accomplish these goals, the perpetual adversaries that make up the payments ecosystem must work together. That is why RILA is reaching out to representatives across the merchant community, as well as those representing the card networks and financial institutions of all sizes, in an effort to work together to identify near- and long-term solutions.

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 look forward to working with the Committee and request that these comments be included in the record.

Sincerely,

William Hughes
Senior Vice President, Government Affairs
Retail Industry Leaders Association

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

June 18, 2014

The Honorable Edith Ramirez
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue N.W.
Washington, D.C. 20580

Dear Chairwoman Ramirez,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, February 5, 2014 to testify at the hearing entitled "Protecting Consumer Information: Can Data Breaches Be Prevented?"

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday July 2, 2014. Your responses should be e-mailed to the Legislative Clerk in Word format at **Kirby.Howard@mail.house.gov** and mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Lee Terry
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade
Attachment

Additional Questions for the Record
Subcommittee on Commerce, Manufacturing, and Trade
"Protecting Consumer Information: Can Breaches Be Prevented?"
February 5, 2014

The Honorable Lee Terry

1. You testified that legislation would "strengthen [FTC's] existing authority governing data security standards." If you already have the authority to pursue data security enforcement actions now, why do you need a new law? What would change with such a law?

   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 over 50 data security cases.

   The Commission supports federal legislation that would (1) strengthen its existing tools to address companies' inadequate practices for securing consumers' data and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach. Such legislation is important for a number of reasons. First, we currently lack authority under Section 5 to obtain civil penalties, an important remedy for deterring violations. Second, enabling the FTC to bring cases against non-profits would help ensure that whenever personal information is collected from consumers, the entities that maintain such data take reasonable measures to protect it. Finally, rulemaking authority under the Administrative Procedure Act would enable the FTC to respond to changes in technology when implementing the legislation.

2. You testified that "although most states have breach notification laws in place, having a strong and consistent national requirement would simplify compliance by businesses while ensuring…consumers are protected." Does that mean you believe preemption is appropriate in this area?

   The Commission has expressed support for 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, the Commission would not support the law.

3. You testify the Commission supports a Federal law that requires companies "in appropriate circumstances," to provide notification to consumers. Can you describe what "appropriate" circumstances are? Are there occasions where notification could cause unnecessary problems for consumers and should not occur (e.g., cancelling a credit card when no account information was compromised)?

   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 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.

The following standard strikes the right balance: When an entity discovers a breach of security, the entity should be required to notify every consumer whose personal information was, or there is a reasonable basis to conclude was, accessed by an unauthorized person, unless the entity can demonstrate that there is no reasonable risk of identity theft, fraud, or other harm. (Of course, breach notification would only be triggered if specified categories of personal information have been the subject of a breach.) This standard balances the need for consumers to know when their information has been breached against the threat of over-notification for breaches that have no reasonable risk of harm.

4. You testify the Commission has settled 50 cases against businesses that it charged with failure to provide reasonable and appropriate protections for consumers' personal information. That does not include non-profits because the FTC's jurisdiction does not extend to those entities. With regard to data security, should the Commission have authority over non-profits? We have heard of universities and colleges suffering data breaches. Are they a common source of data breaches?

Yes, the Commission believes it should have jurisdiction over non-profits in this area. A substantial number of reported breaches have involved non-profit universities and health systems. Enabling the FTC to bring cases against non-profits would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it.

5. Has the Commission pursued any data security cases that resulted in litigation instead of a settlement?

Most companies have chosen to settle the Commission's data security claims. However, the Commission currently has two data security cases in active litigation. *FTC v. Wyndham Worldwide Corp.* is pending in the federal district court in the District of New Jersey.[1] The Commission also approved the filing of a case in the FTC's administrative court, *In the Matter of LabMD*.[2]

6. How does the FTC enforce its "unfairness" standard? What principles guide the FTC so that businesses know when they might run afoul of the unfairness standard?

A company's practices are unfair if they 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.[3] In the Commission's data security cases, reasonableness is the lynchpin. In determining whether a company's

---

[1] *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-JAD (D.N.J.).
[2] *LabMD, Inc.*, No. C-9357 (F.T.C. compl. filed Aug. 28, 2013), *available at* http://www.ftc.gov/os/adjpro/d9357/130829labmdpart3.pdf.
[3] *See* 15 U.S.C. § 45(n); Federal Trade Commission Policy Statement on Unfairness, *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

data security practices are reasonable the Commission considers: the sensitivity and volume of consumer information a business holds; the size and complexity of its data operations; and the cost of available tools to improve security and reduce vulnerabilities. The reasonableness test is designed to be flexible; reasonable data security safeguards should be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

In addition to the more than 50 data security consent orders, which provide guidance to businesses about what constitutes reasonable security, the Commission also has published business guidance and educational materials about good data security practices for companies. We have emphasized a process-based approach that includes: designating a person to be responsible for data security; conducting risk assessments; designing a program to address the risks identified, including training, security and incident response; and monitoring the program and updating it as necessary.

7. Has the FTC ever suffered a data breach?

We are not aware of any successful intrusions or infiltrations into the FTC network. Like other federal agencies and companies in the private sector, we are constantly under attack, and we use defense-in-depth (meaning multiple layers of security controls, such as firewalls, anti-virus and anti-spam tools, internet filters), continuous monitoring, and other methods to protect our information systems and the data they contain.

8. You mentioned that more than 16 million Americans have been victims of identity theft. What counts as identity theft for this purpose? Does it include cases where someone else uses your credit card number even if you end up without any financial loss?

The figure cited in the Commission's written testimony is from the Bureau of Justice Statistics report, "Victims of Identity Theft, 2012," which is the most recent BJS study of identity theft victims.[4] For the purposes of that report, identity theft victims are defined as persons age 16 or older who experienced one or more of the following incidents in 2012: unauthorized use or attempted use of an existing account, such as a credit or debit card, checking, savings, telephone, online, or insurance account (referred to as fraud or misuse of an existing account); unauthorized use or attempted use of personal information to open a new account, such as a credit or debit card, telephone, checking, savings, loan, or mortgage account (referred to as fraud or misuse of a new account); or misuse of personal information for a fraudulent purpose, such as getting medical care, a job, or government benefits; renting an apartment or house; or providing false information to law enforcement when charged with a crime or traffic violation (referred to as fraud or misuse of personal information). According to the report, direct and indirect identity theft losses amounted to approximately $24.7 billion in 2012.

Fraud detection programs are not perfect, so consumers are not reimbursed for all fraudulent charges placed on their accounts. Even when victims are ultimately reimbursed for out-of-pocket financial losses from a breach, this does not mean that they did not experience other, non-compensated harms from the breach. Consumers affected by breaches should constantly monitor their financial accounts for unauthorized charges. If consumers discover such charges, they must notify their credit and debit card issuers, close accounts, cancel cards, and wait for new cards to arrive. For those consumers with automatic bill pay, they must alert companies about the new account numbers to prevent late fees and other charges. Victims of identity theft can spend months reporting instances of fraud to creditors and reporting bureaus to restore their credit. Victims are not compensated for the economic cost from these expenditures of time.

The Honorable Jan Schakowsky

1. On January 10, 2014, Target announced that certain customer information – separate from the payment card data already revealed to have been stolen – had also been taken during the breach of its network systems in November and December 2013. This information included names, mailing addresses, phone numbers or email addresses for up to 70 million individuals.

    a. What are the top risks to consumers whose names and contact information are stolen, including those Target customers who are among the 70 million? Please list them.

Personal information that is non-financial still requires protection, because it can be used to perpetuate fraud and identity theft. For instance, bad actors can use email addresses to perpetrate phishing attacks, send spam, or target users for malware, the latter of which can be used to install keyloggers or other technology to capture even more personal information. Moreover, targeted fraud becomes increasingly effective

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

the more personal information a criminal has about a consumer. For example, many consumers still use their email address as a user name on accounts. That, along with access to other personal information, may increase the danger of a criminal being able to ascertain a password and access a financial or other account or to perpetrate identity theft.

b. Members and witnesses at recent congressional hearings on commercial data breaches have discussed at length potential enhancements to payment card security technology, such as the implementation of chip-and-PIN systems. At the Subcommittee hearing on February 5, 2014 – while stressing that the Commission does not recommend any particular technology – you indicated that "we would support any steps that are taken at the payment card system end to protect or better protect consumer information." I believe it is important for retailers, issuers, and the payment card industry to urgently work together to improve card security. However, even if all the stakeholders involved agree to make payment card data as secure as possible, am I correct to understand that it is your position that that Congress should still separately address the overall security of personal data, including non-financial data, collected or stored by commercial entities?

That is correct. The Commission is aware of this developing technology, and according to some reports, it should be a positive step toward strengthening payment card security. However, this technology does not protect other information, such as health information, location information, or SSNs.

All companies that collect and handle consumer information should be required to implement reasonable data security measures. 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.

The Commission reiterates our call for data security and breach notification legislation that would: (1) give us the authority to obtain civil penalties, an important remedy for deterring violations; (2) enable the FTC to bring cases against non-profits, such as hospitals and educational institutions, where many breaches occur; and (3) providing rulemaking authority under the Administrative Procedure Act, enabling the FTC to respond to changes in technology when implementing the legislation.

I believe the breach of marketing data can be a serious threat to consumers. As I said in response to questioning at the Subcommittee's hearing, names and contact information can be used in phishing and social engineering schemes to try to perpetrate identity theft – and while harm from payment card breaches tends to be acute, harm from non-financial breaches tends to linger. In short, identity theft lasts; with chronic effects on consumers that can cost them everything they own.

c. Do you agree that a breach of names and contact information can have a serious long-term impact on consumers, if used to trick them to give up sensitive identity data? Please explain your answer.

Yes. As discussed above, such information can be used to perpetrate fraud and identity theft, which can have lasting impacts on consumers' credit scores, in addition to the economic value of time lost and possible financial loss.

2. On January 31, 2014, the FTC announced the 50th data security settlement in its program of enforcement against those who fail to reasonably protect consumers' personal information. These settlements have been used to protect millions of consumers from unfair or deceptive practices that leave at risk sensitive information like usernames and passwords, Social Security numbers, and health, financial, and children's data. I commend your dedication to this issue.

   Yet, during questioning at the Senate Banking Committee hearing on this topic on February 3, 2014, a Senator pointed out that with so many data breaches each year, 50 cases since 2002 may be commendable, but it may not be enough.

   a. Of course, all breaches do not rise to the level of FTC action, but can you please illustrate how the FTC uses its current legal framework to help with general deterrence, and how authorization to the FTC of new authorities, such as rulemaking authority under the Administrative Procedure Act and broader civil penalty authority, would increase the FTC's ability to deter unfair or deceptive data security practices?

Since 2002, the FTC has brought a steady stream of data security cases – resulting in more than 50 consent orders, and we have also issued extensive consumer and business education materials. During much of this time, we have been the only federal agency sending the message to a wide range of businesses, both small and large, across many sectors, of the need to maintain reasonable security to protect consumer data. Our complaints provide examples of data security practices that did not meet our flexible reasonableness test, and our consent orders serve as templates for best practices for companies setting up and implementing successful information security programs. In addition, we issue extensive guidance for consumers and businesses – especially small businesses – about how to safeguard consumer data. I believe that collectively the FTC's work in this area has helped promote appropriate investment in infrastructure and personnel to address the security of consumer data.

But, plainly, more needs to be done, and a unanimous Commission has concluded that the time has come for Congress to enact strong federal data security and breach notification legislation. We currently lack authority under Section 5 to obtain civil penalties, which are critical to appropriate deterrence of lax security practices. Likewise, enabling the FTC to bring cases against non-profits, over which we presently lack authority, would help ensure that whenever personal information is collected from consumers, the entities that maintain such data take reasonable measures to protect it. Finally, APA rulemaking would give us flexibility in implementing the statute by

making changes where appropriate – for example, to the definitions – to respond to changes in technology and changing threats.

b. Recent newspaper commentary has suggested that by seeking to strengthen its data security authority, the FTC is acknowledging that it currently lacks the authority to police companies' data security practices. How do you respond to such an assertion?

The Commission principally 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 over 50 data security cases to date. In fact, a federal district court recently affirmed the FTC's authority to use Section 5 in the data security area.[5]

The Commission has called for data security legislation that would strengthen its existing tools and authority to help us in this endeavor, namely, civil penalty authority, jurisdiction over non-profits, a nationwide breach notice requirement to be enforced by the FTC and the states, and APA rulemaking to ensure we have adequate flexibility to respond to new technology and threats in implementing the statute.

The Honorable Jerry McNerney

1. Thank you for your leadership within the FTC, especially with regards to the work that is being done on privacy issues. What sort of authority does the Commission have or need from Congress to institute nationwide breach notification processes?

The FTC has authority to investigate breaches and bring civil enforcement actions under Section 5 of the FTC Act for deceptive or unfair acts or practices – such as deceptively claiming to reasonably safeguard consumer data. We have authority to seek equitable remedies for violations of Section 5, which does not include civil penalties.[6] The FTC also generally lacks authority to require companies to issue notification to affected consumers to alert them to a breach of their personal information (with the exception of our narrow scope of authority under the HI-TECH Act). We similarly lack authority over non-profits, which have been the source of a number of breaches. To remedy these gaps, a unanimous Commission has called on Congress to enact legislation to pass a nationwide breach notification law to apply to all companies under the FTC's jurisdiction – expanding that jurisdiction to include non-profits –and to give the Commission civil penalty authority and authority to flexibly respond to changes in technology in implementing the law via APA rulemaking.

2. Businesses are understandably leery of the idea of additional regulations, but many people that I have talked with agree that a national standard is easier to deal with than varying state standards when it comes to data breach notification rules. In your opinion, how can the FTC

[5] *See F.T.C. v. Wyndham Worldwide Corp*, No. 2:13-cv-01887-ES-JAD, 2014 WL 1349019 (D.N.J. Apr. 7, 2014), *petition for leave to appeal filed* (3d Cir. July 3, 2014).

[6] By contrast, the FTC has civil penalty authority under the Fair Credit Reporting Act for security violations by "consumer reporting agencies," such as the national credit bureaus.

and Congress best work together to come up with a national standard that doesn't impose unfairly upon states' rights?

Breach notification and data security standards at the federal level, with appropriate preemption of state law as discussed below, would extend notifications to all citizens nationwide and create a level playing field so that businesses operating in numerous states can apply one standard. A federal law would create uniform protections for all American consumers. However, our support for a federal law that would preempt state law has been conditioned on both a standard that is sufficiently strong and on giving states the ability to enforce the law, an important role for state Attorneys General.

The Honorable Peter Welch

1. We've seen the FTC take a strong leadership position on many issues, not only bringing enforcement actions but also convening experts from industry and academia at workshops. These workshops have been valuable opportunities for the FTC to write reports on what it learns, including guidance to companies when appropriate. It seems to me like an annual workshop and report on data security would be valuable given the recent problems companies have been having -- can we expect the FTC to have such a workshop soon?

Thank you for your recognition of the FTC's leadership on many issues and the value of our use of enforcement actions and public workshops. As you may know, emerging areas in privacy and security are frequent subjects of FTC workshops, studies, and reports. For instance, in June of last year, we held a workshop on threats to mobile security, in which we convened a group of leading experts to discuss mobile malware, the role of platforms in security, and ways to improve security in the mobile ecosystem.[7] Earlier this year, the FTC hosted a "Spring Privacy Series" to examine the privacy and security implications of a number of new technologies in the marketplace, including mobile device tracking, alternative scoring products, and apps and devices that collect consumer-generated health data.[8] At the Commission's November 2013 conference on the Internet of Things, much of the discussion focused on security challenges presented by "smart" devices.[9]

Moreover, the FTC just published its first annual "Privacy and Data Security Update," which is an overview of the FTC's enforcement, policy initiatives, and consumer

---

[7] *See* Mobile Security: Potential Threats and Solutions (June 4, 2013), *available at* http://www.ftc.gov/news-events/events-calendar/2013/06/mobile-security-potential-threats-solutions.

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

[9] *See* Internet of Things - Privacy and Security in a Connected World (Nov. 19, 2013), *available at* http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

outreach and business guidance in the areas of privacy and data security from January 2013-March 2014.[10] We expect to update this document every year.

[10] Federal Trade Commission Staff, 2014 Privacy and Security Update (June 2014), *available at* http://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

June 18, 2014

The Honorable Lisa Madigan
Attorney General
State of Illinois
100 West Randolph Street
Chicago, IL 60601

Dear Attorney General Madigan,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, February 5, 2014 to testify at the hearing entitled "Protecting Consumer Information: Can Data Breaches Be Prevented?"

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday, July 2, 2014. Your responses should be e-mailed to the Legislative Clerk in Word format at **Kirby.Howard@mail.house.gov** and mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Lee Terry
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade
Attachment

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

June 18, 2014

Mr. William Noonan
Deputy Special Agent in Charge
Criminal Investigation Division
Cyber Operations
United States Secret Service
950 H Street N.W.
Washington, D.C. 20223

Dear Mr. Noonan,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, February 5, 2014 to testify at the hearing entitled "Protecting Consumer Information: Can Data Breaches Be Prevented?"

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday July 2, 2014. Your responses should be e-mailed to the Legislative Clerk in Word format at **Kirby.Howard@mail.house.gov** and mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Lee Terry
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade
Attachment

Secret Service Response to the
Post-Hearing Questions for the Record
Submitted to William Noonan
From Chairman Lee Terry

"Protecting Consumer Information: Can Data Breaches Be Prevented?"
February 5, 2014

---

1) **You testified that Secret Service cyber crime investigations have resulted in the prevention of over $11 billion in potential fraud losses. How do you calculate this number?**

The Secret Service is focused on minimizing the financial losses associated with the criminal violations under its investigative jurisdiction. Accordingly, the Secret Service tracks the actual and potential fraud losses associated with the criminal cases it investigates. The prevention of over $11 billion in potential fraud losses from cyber crime, referenced in my testimony, was the total measure of the potential fraud losses associated with Secret service cyber-crime arrests over the period October 1, 2009 to September 30, 2013.

Cyber criminals commonly target payment card data, which are a type of access device, due to the ease with which this information can be monetized through various frauds. Fraudulent use, trafficking in, and counterfeiting of access devices are federal violations of 18 U.S.C. § 1029, which, since it was established as a criminal violation in 1984, has been assigned to Secret Service investigative jurisdiction. Title 18 U.S.C. § 1029(e)(1) defines access devices as "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)."

As part of its criminal investigations, the Secret Service measures the actual and potential fraud losses associated with criminal violations of 18 U.S.C. § 1029. If the actual fraud loss inflicted by a criminal can be discerned by examining financial records associated with an access device, the actual loss is included in the prevented fraud loss calculation. However, if the actual fraud loss cannot be discerned, the potential loss associated with an access device is estimated at a fixed amount of $500. For example, if a stolen credit card was seized and it can be determined that $25,000 in illegal transactions were made with that card, $25,000 will be reported in the measured results. If the dollar amount of illegal transactions cannot be associated with that credit card, an estimated loss of $500 will be attributed to that credit card and reported in the measured results. This estimate of potential fraud losses is based on industry standards and established in the Federal Sentencing Guidelines, which state: "In a case involving any counterfeit access device or unauthorized access device, loss includes any unauthorized charges made with the counterfeit access device or unauthorized access device and shall be not less than $500 per access device."

In July 2012, the Department of Homeland Security coordinated an independent verification and validation of one of the Secret Service's performance measures using this calculation methodology. The audit concluded that the potential fraud loss measure is valid, complete, consistent, accurate, timely, and based on good data quality.

But to the extent that the measure differs from the actual economic losses occasioned by cyber crime, the measure is likely to be lower. Considering that most credit cards have greater than $500 limits, and that this measure does not include all stolen access devices but only those that the Secret Service successfully detected, the Secret Service considers this measure to be an underestimate of the total potential fraud losses associated with the cases it investigates. Moreover, the total economic harm from cyber criminal activity is greater than the criminal revenue or potential fraud losses when the damage to victim companies and cost of remediation is considered.

2) You opined that "legislative action could help to improve the Nation's cybersecurity, reduce regulatory costs on US companies." How so?

Legislative action could help to improve the Nation's cybersecurity, while reducing regulatory costs on US companies by, among other actions, making modest incremental changes to criminal laws related to computer hacking, and establishing a uniform Federal standard requiring certain types of businesses to report data breaches and thefts of electronic personally identifiable information.

The Secret Service supports amending the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, to clarify several existing criminal offenses relating to attacks on computers and computer networks and enhance their penalties. Also, given the growth of transnational organized cyber crime, the Secret Service assesses that adding the offenses under the CFAA to the list of offenses in the Racketeering Influenced and Corrupt Organizations Act (RICO) at 18 U.S.C. § 1961(1) would provide an important enhancement to our ability to disrupt and dismantle organized cyber crime. These and other related criminal law changes would likely not impose any regulatory costs on US companies, while improving our Nation's cybersecurity through enhanced law enforcement action to defeat cyber threats.

The Secret Service also supports establishing a uniform Federal standard for data breach notification. Currently 47 States have data breach notification laws that set various standards for data breach notification. A uniform Federal standard for data breach notification would reduce the regulatory and compliance costs on businesses that currently have to comply with multiple state laws. A uniform national data breach notification standard should also include provisions for notification to appropriate law enforcement agencies with jurisdiction, and allow such agencies to delay any required notice to effected individuals (e.g., customers whose information was stolen) if such notification would impede a criminal investigation.

These legislative proposals, among others, are detailed in the Administration's May 2011 legislative proposal regarding cybersecurity. Acting Assistant Attorney General Mythili Raman recently re-

emphasized the need for changes like these in her February 4, 2014 testimony before the Senate Committee on the Judiciary.

3) **In your opinion, how are the big companies – the ones that seem to be in the cross-hairs of hackers – doing on the cyber protection front? How involved are they with your information sharing efforts?**

The Secret Service is encouraged by several improvements in the private sector's cyber protection efforts. The financial service sector has, in partnership with DHS and Treasury, created a robust and highly effective information sharing organization—the FS-ISAC. This year the retail sector has also moved to create more robust information sharing programs. The Secret Service believes information sharing programs like these perform an important role in developing understanding of sector specific cyber threats and effective mitigation steps. The Secret Service has met with leaders in the retail sector and is supporting their efforts to establish effective information sharing programs.

The Secret Service supports a wide variety of information sharing efforts. As the Secret Service identifies malware and the methods of cyber criminals through its investigation, it quickly provides this information to the DHS NCCIC for broad dissemination through the various information sharing organizations, while protecting grand jury information, the integrity of ongoing criminal investigations, and the victims' privacy. The Secret Service also partners with industry to publish reports on cybersecurity trends, for example through the annual Verizon Data Breach Investigations Report and the annual Trustwave Global Security Report. The Secret Service also uses its network of Electronic Crimes Task Forces (ECTFs) to bring together partners to discuss trends in cyber crime and effective mitigation strategies. All of these information sharing efforts, among others, are mutually complementary.

4) **Is it possible for any entity to be impervious to criminal hacks? And if it is possible, is it practical or realistic?**

Any entity that uses computers is at risk of falling victim to criminal computer hacking. This is why the Secret Service emphasizes the importance of deterring cyber crime and cyber incident response planning. Just as companies do with other security risks, they need to holistically approach the challenge of cyber crime and not define the challenge of cybersecurity narrowly as an "IT problem." Designing business processes that reduce a company's possession and handling of commonly-targeted sensitive data, like payment card data and sensitive personally identifiable information, is often the most cost-effective way for a company to reduce its cyber crime risk.

The Secret Service is often the first to notify companies that they have been the victim of cybercrime. In working with victim companies the Secret Service has found the organizations best able to respond to a data breach have developed a cyber incident response plan and pre-identified a cyber incident response team that includes in-house legal counsel, human resource personnel, corporate security, IT security, technical professionals, and a senior public relations or communications expert to coordinate messaging. Effective and efficient response to a data breach can greatly reduce the costs to the victim company.

Finally, cyber-crime is a systemic threat to US companies, and it is important that companies have developed programs to effectively engage with law enforcement in our efforts to apprehend cyber criminals. Investments in logging and detection of potentially malicious cyber criminal activity, rather than narrowly focusing on static defense, enables companies to more quickly identify criminal activity taking place, and, by working with law enforcement, to apprehend and prosecute those responsible.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

June 18, 2014

Mr. John J. Mulligan
Interim President
and Chief Executive Officer
Target Corporation
1000 Nicollet Mall
TPS 2676
Minneapolis, MN 55403

Dear Mr. Mulligan,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, February 5, 2014 to testify at the hearing entitled "Protecting Consumer Information: Can Data Breaches Be Prevented?"

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday July 2, 2014. Your responses should be e-mailed to the Legislative Clerk in Word format at **Kirby.Howard@mail.house.gov** and mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Lee Terry
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade
Attachment

Target Responses to Additional Questions for the Record

House Energy and Commerce Committee; Subcommittee on Commerce, Manufacturing, and Trade
"Protecting Consumer Information: Can Data Breaches Be Prevented?"
John J. Mulligan, Chief Financial Officer, Target
February 5, 2014

The Honorable Lee Terry

1. **We have seen a number of breaches occur. Target provided notice within 4 days of learning of the breach. How was Target able to provide notice so quickly? What lessons did you learn as you went through the process of complying with the state notification requirements? Given your experience with this breach, is there anything you would do differently if such an unfortunate event were to occur again?**

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 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, email, prominent notices on our website, and social media. Target sought to comply with all existing state notification laws. Specifically, we provided notice by (1) posting notice on our website; (2) providing notice by e-mail to each relevant guest for whom we had an e-mail address; and (3) providing notice to nationwide and state media.

2. **In your response to Mr. Waxman's, Ms. Schakowsky's, and Ms. DeGette's letter you stated that you annually update your security plan. Do you ever update the security plan more frequently based on emerging threats? You also stated that the malware captured "some strongly encrypted PIN data." Do you know if these PINs were compromised through de-encryption?**

Target annually updates its internal information security plan to reflect a wide variety of threats. Target also continually monitors emerging network and organizational threats to identify threats that require specific action by the Company, including updates to its information security practices as appropriate.

Target is not aware that any encrypted PIN data captured by memory-scraping malware during the cyber-attack was decrypted.

3. **Of the 40 million consumers whose payment card data was involved in your breach, for how many did you have contact information? What was your approach to get the word out to others whose contact data you didn't have?**

Of the approximately 40 million consumers whose payment card data Target believed may have been involved in the breach, we had approximately 17 million valid emails, and we provided notice by e-mail to each such individual. In addition, we included written notification in our Target REDcard holder statements, mailed monthly. We also posted notice on our website and provided notice to nationwide and state media.

4. What is the primary source of fraud - online or at point of sale?

The primary source of fraudulent transactions at Target is counterfeit cards used at point of sale in stores.

5. How would implementing chip-and-PIN technology address the massive amount of fraud and vulnerability associated with internet-based transactions?

Chip-and-PIN is an in-store "card present" solution, and does not directly address internet-based fraud. However, indirectly, the way Target is implementing chip-and-PIN combined with point-to-point encryption will help protect card data and keep it from being stolen and used fraudulently elsewhere, which will reduce fraud both in stores and on the internet.

6. If chip technology is broadly implemented, why does it matter if a customer uses a signature or PIN to authenticate his or her identity?

Chip technology authenticates the card and prevents the card from being counterfeited. The PIN is used to verify the cardholder, because only the cardholder knows the PIN. Therefore, the PIN protects against the fraudulent use of valid cards that have been lost or stolen. The PIN is verified by the system so it is more secure than a signature, which is only verified manually. The PIN is an objective set of numbers that is the same for each transaction and must be verified by a computer system. A signature can have a great amount of variance depending on the signing method and it can be difficult to verify a signature because of the inconsistency of an individual's handwriting.

According to Federal Reserve data, debit card transactions that use a PIN are 700% more secure than those that simply require a signature for cardholder verification. (Federal Reserve. "2011 Interchange Fee Revenue, Covered Issuer Costs, and Covered Issuer and Merchant Fraud Losses Related to Debit Card Transactions." March 5, 2013.) According to Visa and MasterCard, "It is much more difficult for a fraud perpetrator to ascertain a PIN than to forge a signature. Accordingly, one of the most effective ways of combating fraud is to make the use of PIN for customer verification compulsory." (Visa Worldwide Pte Limited and Visa AP (Australia) Pty Ltd and MasterCard Asia/Pacific Pte Ltd Submission to the Australian Competition and Consumer Commission in support of Application for Authorization. July 4, 2013.)

According to the Federal Reserve Bank of Kansas City, many countries that use chip-enabled cards do not allow cardholder authentication with signatures because they are not as secure as PIN transactions. Furthermore, the study recommended that all cards (chip/EMV, credit, debit and pre-paid cards) should be issued with a corresponding PIN number for point of sale purchase in order to help combat cyber theft. (Sullivan, Richard J. "The U.S. Adoption of Computer-Chip

Payment Cards: Implications for Payment Fraud." Federal Reserve Bank of Kansas City, First Quarter 2013.)

7. If the payment card data from a chip-enabled card is somehow stolen, and a card is duplicated, would the inclusion of a PIN in the transaction create one more piece of information for thieves to steal?

Target is implementing industry best practices to encrypt the PIN at the payment device, which is designed to minimize any risk that the PIN can be stolen.

The PIN is not part of the card data that is stored on the magnetic stripe. The PIN may or may not be included in the chip itself, depending on how the issuing bank chooses to process PIN transactions. If the issuing bank processes PIN "online," the cardholder enters the PIN at the payment device, where it is encrypted and routed through the payment processor to the issuing bank to be verified. If the issuing bank processes PIN "offline," industry best practice would be for the PIN information to be contained in a secure area of the chip on the card, so when the cardholder enters the PIN at the payment device, it is encrypted and verified against the PIN stored on the chip. In both cases, the PIN is encrypted at the payment device, and that encryption is very difficult to break.

PINs are used successfully today to enhance security for ATM transactions and for a significant share of in-store payment transactions, and have been widely adopted outside the US in regions where chip-and-PIN has already been implemented.

8. Is there foolproof technology that would keep thieves from gaining access to a customer's PIN number?

The encryption processes and technology that Target had in place at the time of the breach were effective in preventing the intruders from accessing unencrypted PIN numbers.

9. If chip-enabled card data is stolen, is the thief then armed with a customer's card number, personal information, and PIN number? If so, how do we prevent the thief from withdrawing a customer's funds directly out of their account at an ATM?

Target is implementing industry best practices to encrypt the PIN at the payment device, which is designed to minimize any risk that the PIN can be stolen.

The PIN is not part of the card data that is stored on the magnetic stripe. The PIN may or may not be included in the chip itself, depending on how the issuing bank chooses to process PIN transactions. If the issuing bank processes PIN "online," the cardholder enters the PIN at the payment device, where it is encrypted and routed through the payment processor to the issuing bank to be verified. If the issuing bank processes PIN "offline," industry best practice would be for the PIN information to be contained in a secure area of the chip on the card, so when the cardholder enters the PIN at the payment device, it is encrypted and verified against the PIN stored on the chip. In both cases, the PIN is encrypted at the payment device, and that encryption is very difficult to break.

PINs are used successfully today to enhance security for ATM transactions and for a significant share of in-store payment transactions, and have been widely adopted outside the US in regions where chip-and-PIN has already been implemented.

10. What is the percentage of retailers currently equipped to process chip-and-PIN transactions? How long would it take and how expensive would it be for retailers to adapt their POS terminals to read chip-and-PIN cards?

While Target does not have visibility into chip-and-PIN adoption for the entire retail industry, Target is accelerating our $100 million investment in the adoption of chip technology. We have already installed approximately 38,000 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 system.

The Honorable Jan Schakowsky

1. **Last April and August, Visa issued data security alerts, notifying Target, Neiman Marcus, and other retailers of "an increase in network intrusions" involving memory-parsing malware – the class of malicious software that was reportedly deployed in recent attacks on retailers. These alerts also provided recommendations on strategies to mitigate the impact of attacks involving this kind of malware. I understand that all retailers, especially large ones such as Target, receive a truly immense number of security alerts – but I would like to better understand how retailers respond to such warnings.**

    a. **Were the April and August 2013 Visa warnings relevant to the malware that caused the November-December 2013 breach?**

In its April and August 2013 alerts, Visa noted that it had seen an increase in cyber criminals installing "memory parser malware" on Microsoft Windows based cash register systems to steal payment card track data. According to Visa, hackers were taking advantage of the few milliseconds in time when track data is unencrypted to steal track data before the processing and re-encryption of such data. VISA's alerts offered general threat intelligence and nothing specific to the attack on Target.

    b. **Which, if any, of Visa's mitigation strategies (related to network security, cash register and point-of-sale security, administrative access, network segregation, and incident response) did Target implement in response to the aforementioned, or similar, security warnings? If it did not implement any of these mitigation strategies, please explain why not.**

In the fall of 2013, Target analyzed currently available information regarding malware aimed at point-of-sale (POS) systems that was capable of capturing payment card data prior to the encryption of the data by the POS system—including Visa's April and August 2013 alerts. Target believed that its various security protocols would limit access to POS systems to install memory-scraping malware (or any other malware, for that matter). As added security, Target also implemented a plan to continue to monitor the POS malware threat landscape. Target also addressed other risks posed by cyber-criminals generally by implementing new defenses, such as an advanced threat detection appliance, FireEye.

    c. **What, if any, security measures were implemented during 2013 to specifically address the threat of memory-parsing malware?**

Target monitors emerging network and organizational threats on an ongoing basis, including the threat of memory-scraping, or memory-parsing, malware. As noted, Target believed that its existing security protocols would limit access to POS systems to install malware. Target also addressed other risks posed by cyber-criminals generally by implementing new defenses, such as an advanced threat detection appliance, FireEye. Target began incorporating FireEye in 2013 as part of its security strategy to incorporate a non-signature-based malware detection solution.

FireEye provides an additional layer of protection beyond industry-standard antivirus protection, intrusion prevention and detection tools and firewalls, and other network defenses; however, FireEye was not yet fully integrated at the time of the breach.

2. **Security breaches like those that affected Target and Neiman Marcus are not a new problem. In 2005, hackers accessed ChoicePoint's database of consumer information. Between 2005 and 2008, prior to their apprehension, a group of criminal cyber thieves including Albert Gonzalez stole 90 million pieces of credit and debit card information from a number of high-profile retailers, including TJ Maxx, Office Max, Dave & Buster's, Barnes & Noble, and even Target.**

   Despite Target's previous experience with a breach of payment card information, Target's security systems suffered a major breach a second time.

   a. **What changes did Target make to its security systems based on what it learned from that earlier breach?**

The 2007 attack differed from the 2013 attack both in terms of scope and the type of attack. In 2007, a limited number of guest credit and debit card numbers were involved. The 2007 attack also involved a different mode of attack than the 2013 attack. Nonetheless, Target took a number of steps to modify its network security posture in response to the 2007 incident, including, for example, upgrading wireless network encryption.

   b. **According to your forensic investigations of the 2013 breach, why do you believe such a major breach occurred at Target in November and December 2013, while, to date, no similar November and December 2013 breach is reported to have occurred at the other largest U.S. brick-and-mortar retailers?**

According to published news reports, Target is not the only retailer to have experienced a breach relating to payment card data in late 2013. Neiman Marcus reportedly suffered a breach from July 16 to October 30, 2013, which it disclosed in January 2014. Michaels Stores also reportedly suffered a breach from May 8, 2013, to January 27, 2014, which it disclosed in April 2014.

3. **The *New York Times* has reported that Target's systems were "astonishingly open" and lacked adequate firewalls and traffic monitoring. In your February 4, 2014, testimony to the Senate Judiciary Committee, you disputed the *Times'* characterization of Target's security, noting that the company had spent hundreds of millions of dollars on detection, firewalls, benchmarking, and penetration and compliance testing. I would like to gain a fuller understanding of Target's security measures and how the breach took place.**

   a. **In Fiscal Year 2013, what were the funds spent and persons employed on the network security of systems serving Target stores, and were additional funds spent or additional network security personnel hired to protect the integrity of systems serving Target stores during the holiday season? How did the**

resources expended on security in Fiscal Year 2013 and additionally in the holiday season of 2013 compare to previous years?

Target has invested significant capital and resources in security technology, personnel and processes. As indicated in our testimony, Target has invested hundreds of millions of dollars on all facets of network security, from technical defenses to testing to personnel. Target's spending on dedicated information security teams and core security infrastructure increased in Fiscal Year 2013 over Fiscal Year 2012.

b. In the February 4, 2014, Senate Judiciary Committee hearing on data breaches, Fran Rosch of Symantec noted several behavioral security measures companies should adopt, such as monitoring for unrecognized files and new transmissions of data. Prior to November 27, 2013, did Target have strategies to monitor the movement of data around its network for irregularities and the outgoing transfer of data from its servers? If so, please discuss these strategies in detail.

Target deployed numerous physical, administrative, and technical safeguards to protect its network prior to November 27, 2013. These measures included intrusion detection and prevention appliances, vulnerability scans, data loss prevention tools, advanced threat detection technology, state of the art encryption, multi-factor access controls, and a full-time security operations center staffed twenty-four hours a day, 365 days a year. Target's suite of security tools included Symantec's Enterprise Data Loss Prevention tool, which was used throughout Target's network to scan data at rest and in motion.

c. Prior to November 27, 2013, did Target have strategies to protect its point-of-sale systems from threats posed by memory-parsing malware? If so, please discuss these strategies in detail.

Target has had a comprehensive security strategy in place to protect its entire network, including its payment processing systems. Components of this strategy include:

- Compliance with the Payment Card Industry Data Security Standards ("PCI DSS");
- Symantec antivirus software for registers;
- Security policies designed to limit user access to registers;
- File Integrity Monitoring;
- Password controls and security event monitoring for register;
- Physical controls, such as tamper-proof payment devices (e.g., card readers); and
- Policy restrictions on access to registers, such that users cannot, for example, access anything other than the register application, which is launched when the machine is turned on.

d. In testimony, you stated that "we were found PCI compliant on September 20th of 2013." Through forensic investigations of the breach, have you determined if Target met the PCI standards for which it was certified on the

particular days when its network was (i) initially breached and (ii) extensively compromised?

Trustwave, Target's third-party Qualified Security Assessor ("QSA"), certified Target as PCI DSS compliant in September 2013. Nothing Target has found in its investigation of the breach leads Target to alter Trustwave's conclusion that Target was PCI DSS compliant. Nevertheless, Target is taking additional measures post-breach to enhance its overall security posture.

e. Did Target make any material changes to security practices or procedures between September 20, 2013 – when deemed compliant with PCI standards – and the time the breach occurred? If so, what were they?

The changes Target made to its security policies and procedures between September 20, 2013 and December 15, 2013, were intended to enhance its security posture. Target enhanced its security practices in the fall of 2013 by implementing a plan to continue to monitor the POS malware threat landscape, and by commencing its deployment of an advanced malware detection utility called FireEye.

f. Among PCI standards for which the company is assessed annually, did Target meet the most stringent versions published at the time of the breach?

Target was deemed compliant with PCI DSS on September 20, 2013. Trustwave, Target's QSA, completed the PCI Report on Compliance using the version of PCI DSS in effect at the time, the same version in effect at the time of the attack.

g. What is Target's position on the question of how its payment systems could be so severely compromised while at the same time it held a current certification of compliance with PCI DSS? Following the breach, do you believe that companies threatened by malware attacks on their payment systems and their customers would be better served if the baseline security requirements of PCI DSS were more stringent?

Unfortunately, the attack on Target shows that a cyber-attack can occur despite a company's efforts to prevent such attacks—even when its efforts include adherence to PCI DSS.

h. Prior to November 27, 2013, did Target endeavor to implement point-to-point encryption of payment card data, in which such data is immediately encrypted when swiped at the point-of-interaction device? If so, please explain these efforts in detail, and address why the company did not fully implement this kind of encryption.

Prior to November 27, 2013, Target was in the process of implementing newer versions of certain components of its register systems, including card readers and registers. Target was also in the process of upgrading the operating systems used by the registers. These upgrades, which are still in progress, will enable Target to accept chip-and-PIN payment cards and to deploy software capable of encrypting payment card information on the payment device. The upgrades

were being implemented on a pre-existing schedule and had not been fully implemented by the time of the cyber-attack.

i. Does Target have a plan to comply with PCI DSS 3.0 requirements and to upgrade its point-of-interaction devices to those compliant with the newest PCI PTS standards? If so, please explain that plan in detail.

The PCI PIN Transaction Security standard is aimed at the manufacturers of point-of-interaction devices. As the PCI Security Standards Council has indicated, "The PCI PIN Transaction Security (PTS) POI standard enables vendors to develop and bring to market devices that offer protection against such attacks." Target is on track to upgrade to chip-enabled devices by September 2014. Approximately 38,000 of these devices have already been rolled out and are fully compliant with the new PCI PTS standards.

j. Does Target have a plan to upgrade its electronic cash registers? If so, please explain that plan in detail.

Target is in the process of completing the implementation of an updated operating system on all of our registers in 2014.

k. Target's January 31, 2014, response to a letter from Ranking Members Waxman, DeGette, and me explained that payment card data was taken by malware installed on Target's point-of-sale networks. However, it did not explain how other personal data – including mailing addresses, phone numbers, and email addresses – of up to 70 million individuals was stolen. How was this information taken?

The guest contact information was stolen from Target's guest services database. The cyber criminals removed guest contact information from that database. The cyber criminals aggregated the removed data, encrypted it, and stole it by transmitting it to a server controlled by the cyber criminals.

l. Do Target's internal networks link any database containing stored non-financial personal information about customers with sensitive payment card data? If so, what security measures does Target employ to protect its customers' personal data during the company's linkage of payment card data with a database or databases of non-financial personal information about customers?

No, Target's network does not directly link databases containing information such as name, mailing addresses, email addresses, and phone numbers with a database containing payment card data.

4. In written testimony you submitted for the Subcommittee's February 5, 2014, hearing, you stated that "the intruder stole a vendor's credentials to access [Target's] system." Press reports from security blogger Brian Krebs and others indicate that this vendor

was Fazio Mechanical Services, a provider of refrigeration and HVAC services, which has confirmed its link to the Target data breach. According to Fazio Mechanical, the company "does not perform remote monitoring of or control of heating, cooling and refrigeration systems for Target" and its "data connection with Target was exclusively for electronic billing, contract submission and project management, and Target is the only customer for whom we manage these processes on a remote basis." Press reports from security blogger Brian Krebs and others also indicate that Fazio Mechanical's credentials for the Target network appear to have been stolen "with a malware-laced email phishing attack."

a. Why did Fazio Mechanical have external access credentials to Target's network? To what parts of the Target network did Fazio Mechanical have access?

Fazio Mechanical Services access was limited. More specifically, Fazio Mechanical Services had access to Target's external-facing Citrix platform in order to access an application used for construction project management, invoicing, change order management, and other property development related functions.

b. According to a January 21, 2014, *Wall Street Journal* report, "Target Corp. shut down remote access to two websites used by employees and suppliers in a move to tighten security following a massive breach of customer data over the holidays. One system is a human resources website for employees called eHR. The other is a database called Info Retriever that suppliers use to access sales data for their products in Target."

i. Did the vendor whose credentials were stolen have access to eHR or Info Retriever, and if so, which ones?

No, Fazio Mechanical Services did not have access to either eHR or Info Retriever.

ii. Did access to either eHR or Info Retriever, or both, by the intruder or intruders play a role in facilitating the installation of malicious software on Target's systems or the compromise of computers, servers, or other devices?

Target does not believe that the attackers accessed eHR or Info Retriever.

5. A February 14, 2014, *Wall Street Journal* report raises several questions about the vulnerability of Target's network systems to attacks.

a. According to "people familiar with large corporate networks" reached by the *Journal*, "[t]here shouldn't have been a route between a network for an outside contractor and the one for payment data." How did the criminal intruders move undetected from whichever system they initially accessed

within the Target network to electronic cash registers, where it was possible for them to access payment card data?

The cyber criminals accessed a segmented Citrix platform using stolen vendor credentials belonging to Fazio Mechanical Services. The cyber criminals then circumvented several firewalls and other access control technologies in order to deploy memory-scraping malware to Target POS registers.

b. The *Journal* reported that "[s]o-called segmentation issues, where computer systems that shouldn't be connected for security reasons are in fact linked, are a problem at a number of retailers, a person familiar with retail breaches said." However, in a meeting prior to the hearing with Democratic staff of the Committee, Target officials claimed that the company's networks were properly segmented at the time of the breach. If that were the case, how were intruders able to move so extensively through Target's systems?

The cyber criminals accessed a segmented Citrix platform using stolen vendor credentials belonging to Fazio Mechanical Services. The cyber criminals then circumvented several firewalls and other access control technologies in order to deploy memory-scraping malware to Target POS registers.

c. The *Journal* also reported that a February 2014 memo to retailers from the Federal Bureau of Investigation "said it may be a 'vulnerability' to connect credit and debit card readers to remote management software, which makes it easier to manage and monitor internal networks from afar, when combined with weak password selection." At the time of the breach, were credit and debit card readers at Target Stores connected to remote management software? If so, why?

The card readers in Target stores were not accessed using the compromised vendor credentials, and Target did not deploy, use, or allow direct remote access to registers, payment-processing pads, or other in-store POS platforms.

d. Furthermore, the *Journal* reported that "several members of Target's cybersecurity team left the company in the months before the hack, according to people familiar with the matter and a search of social media profiles." Please respond to this report, detailing: (i) any vacant supervisory-level security positions at Target at the time of the breach; and (ii) the number of supervisory-level security positions at Target out of the total number of supervisory-level security positions at Target in which an employee had been in their position for less than six months.

While Target had supervisory-level security positions it was seeking to fill at the time of the incident, other supervisors were fulfilling the responsibilities of those positions on an interim basis.

e. **Lastly, the *Journal* reported that "Target Corp.'s computer security staff raised concerns about vulnerabilities in the retailer's payment card system at least two months before hackers stole 40 million credit and debit card numbers from its servers" and that "at least one analyst at the Minneapolis-based retailer wanted to do a more thorough security review of its payment system, a request that at least initially was brushed off." The *Journal* reported, paraphrasing a former Target employee, that this request "followed memos distributed last spring and summer by the federal government and private research firms on the emergence of new types of malicious computer code targeting payment terminals."**

   i. **Are these reports accurate? If not, please provide additional detail on internal staff discussions on the security of payment card systems in the months preceding the breach.**

   ii. **Did Target security staff raise concerns about the company's payment card system? If so, to whom were these concerns brought, and what were the specific concerns?**

   iii. **Did Target conduct the requested review prior to November 27, 2013? If so, what were the results of the review? If not, why not?**

   iv. **What changes does Target plan to make in order to more quickly and completely respond to the concerns and requests of its security staff? Please discuss these plans in detail.**

Target is not aware of the particular concerns cited by the analyst in the article quoted above. As previously stated, however, in the fall of 2013, Target analyzed currently available information regarding POS malware that was capable of capturing payment card data prior to the encryption of the data by the POS system—including Visa's April and August 2013 alerts. Target concluded that its various security protocols would limit access to POS systems to install memory-scraping malware (or any other malware, for that matter). As added security, Target also implemented a plan to continue to monitor the POS malware threat landscape.

6. **As a part of the January 10, 2014, announcement that up to 70 million customers' non-financial personal information may have been stolen, Target announced that it would be offering one year of free credit monitoring to all Target guests who shopped at U.S. stores. I understand from your testimony on the November and December 2013 data breach that according to Target, "consumers have no liability for any fraud which occurs on their cards as a result of this breach" and that "a part of the package that we offered... is identity theft protection, identity theft insurance, and access to a frauds protection specialist." The day after our hearing, Consumer Reports published an analysis of Target's free credit monitoring offer. It found that – while the offer initially appears "to live up to Target's famous value proposition: Expect more, pay less" – upon signing up, "the offer actually delivers less and pushes consumers to pay up to $74 more," and runs the risk of giving consumers "a false sense of security." While I**

appreciate that Target has done much to communicate with customers and provide them with resources following the breach, I would like to ask about several aspects of the free credit-monitoring offer.

a. According to Consumer Reports, Experian "gives companies the choice of paying for one- or three-bureau credit monitoring" and "Target bought and offered the less-expensive one-bureau monitoring." Why did Target determine that the credit monitoring it would offer, provided through Experian's ProtectMyID service, would only watch the Experian credit report and not those of Equifax and TransUnion, even though information on each credit report can, in the words of Experian, "be very different"?

Our actions leading up to the public announcement of the data breach and subsequent actions have been guided by the principle of serving our guests. Target decided to offer the free credit monitoring to all guests who have ever shopped at Target. Experian had previous experience, an established product, and had the capacity and resources to implement a large-scale program quickly.

b. Is Target aware that upon accessing the Experian site – after signing up for the credit monitoring service that Target has offered – its customers are presented with advertising that suggests that to receive their "total credit picture" they should sign up for an additional Experian service for $14.95? Additionally, is Target aware that Experian is also telling these Target customers that they should "[a]dd Triple Alert credit monitoring" for $4.95 per month and "add [their] credit score" for $7.95? Consumer Reports, which estimates that a worried Target customer might be led to spend up to $74.35 on products of limited utility, has classified these practices as an "upsell." Having chosen to work with Experian on its offer of free credit monitoring, does Target believe these are appropriate business practices for Experian to use against Target's own concerned customers? On its credit monitoring FAQ, Target writes "your trust is important to us." Does Target believe that its customers' experience with these Experian advertisements is likely to improve customers' trust that Target has their best interests in mind?

We wanted to protect our guests from unwanted advertising while also not restricting their access to the same services that are available to other Experian customers. Target's contract prohibits Experian from using information about Target guests enrolling for free credit monitoring to market to those guests unless a guest specifically opts in. We also limited Experian's efforts to solicit Target enrollees to renew the service when the free year expires. The other services that Experian advertises on its site are not limited to fraud protection and identity theft.

c. Many fraud experts believe that one of the most important tools for victims of identity theft is the security freeze. Yet according to Consumer Reports, "Target gave only passing mention of security freezes... in its website breach notice and in some e-mails to consumers." Given the likelihood that some of

the Target customers affected by the breach will become victims of identity theft, why didn't Target more strongly emphasize to consumers the option of seeking a security freeze?

Security freezes primarily protect a consumer from having a criminal fraudulently open a new account in the consumer's name. The theft of Target guest data did not include the type of identifying information that is generally necessary to open a new account, such as social security number and date of birth.

7. **At the Subcommittee hearing on February 5, 2014, I asked you to comment on the email messages sent from Target to customers in mid-January that originated from TargetNews@target.bfi0.com, after describing the confusion – reported by Forbes – that some consumers felt when they could not readily identify the owner of the bfi0.com domain and verify that the message was truly from Target. While I appreciate that in your response to my question you noted that Target previously and concurrently communicated to customers that "there was a single source of truth on our corporate Target.com website," I still believe that Target could have taken some simple steps to ensure that it did not further alarm its already-concerned customers by making sure that the source of its email communication was more readily verifiable.**

    a. **Why were some messages from Target sent from the bfi0.com domain as opposed to a target.com domain?**

Our actions leading up to the public announcement on December 19 and since, have been guided by serving our guests. We wanted to ensure that communications were accurate and actionable. Given the number of people who Target needed to notify, bulk emails were sent with the bfio.com domain as it is recognized by the domain name system and therefore has a higher delivery rate in bulk mail. When sending individual or unique messages to an individual, Target is able to use "target.com" domain as it has a higher likelihood of being successfully delivered without delay.

    b. **What company owns the bfi0.com domain and what is Target's relationship with that company?**

Epsilon owns this email domain. Target used Epsilon to help manage and distribute email to impacted Guests.

    c. **Why didn't Target ensure that email messages from Target received by Target customers arrived from a sender with a "target.com" domain, or take other steps to ensure that email messages from the company could not be misinterpreted to be phishing or other types of scams (which have been prevalent in the wake of the breach)? What will Target do to minimize this potential for confusion in the future?**

We heard from our Guests and consumers that they were confused and concerned about the automated response. As a result, we made the change to ensure a target.com domain was in the

response. We also established our website (https://corporate.target.com/about/payment-card-issue.aspx) as the single source of truth to verify communications from Target. In addition, after making the breach public, Target monitored more than 100 new domain name registrations and active websites for potential phishing and scam operations seeking to take advantage of the incident. Target monitored the proliferation of new domain name registrations that included the word "Target" to determine if those registrations became active websites. Where Target identified active websites that may have been intended to conduct phishing or scam operations or that were otherwise infringing Target's copyrights or trademarks, we promptly sent take-down letters, succeeding in suspending or removing infringing content from all of them. Target informed law enforcement of these efforts.

8. **One topic of discussion at the Subcommittee hearing on February 5, 2014, was the *FTC v. Wyndham* case, currently pending before the U.S. District Court for the District of New Jersey. During questioning, I asked you about a brief of *amici curiae* filed in support of the Wyndham position, which is that the FTC lacks the authority to enforce reasonable data security measures on the basis of the FTC Act's Section 5 prohibition on unfair acts or practices. This brief, which is enclosed for your review, represents four business associations, including the Retail Litigation Center, an arm of the Retail Industry Leaders Association (RILA). I asked you at the hearing if your company was a part of this brief through these associations, and whether your company agrees with the position taken by Wyndham. At the time, you indicated that you were not familiar with the case, but that "we are committed to making this right, and we are committed to engaging on this topic. And we are willing to do so independent of RILA. Target is willing to engage on this topic."**

    a. **Yes or no, should Congress pass a law establishing federal data security standards, applicable to commercial entities including retailers and which would cover sensitive financial and non-financial personal information? If so, which agency do you believe should enforce the law? If not, why not – and what do you propose as alternative measures to enhance safeguards for consumers' personal information?**

Target supports federal data security standards so long as they are reasonable, flexible enough to encompass developments in technology, and do not hinder our ability to serve our Guests. Target believes that Congress has the responsibility to review and determine which agency or agencies should enforce various consumer protection laws and standards. Target seeks to comply with federal laws, regardless of which agencies enforce them.

Following your response, I encouraged you to verify whether or not your company is part of an association that has supported the Wyndham position in the aforementioned brief.

    b. **Is Target a member of RILA?**

Yes.

c. Does Target agree with the position taken by Wyndham and the entities that filed the brief of *amici curiae* that the FTC lacks authority under the FTC Act's Section 5 to enforce reasonable data security measures? If so, what agency do you suppose should make sure that companies adequately protect consumers' personal data and are accountable to the public?

The authority of the Federal Trade Commission under Section 5 is being discussed by policymakers and elected officials. Target believes that Congress has the responsibility to review and determine if agencies have appropriate authority to enforce various consumer protection laws and standards. Target seeks to comply with federal laws, regardless of which agencies enforce them.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225–2927
Minority (202) 225–3641

June 18, 2014

Mr. Michael Kingston
Senior Vice President
& Chief Information Officer
The Neiman Marcus Group
111 Customer Way
Irving, TX 75039

Dear Mr. Kingston,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, February 5, 2014 to testify at the hearing entitled "Protecting Consumer Information: Can Data Breaches Be Prevented?"

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday, July 2, 2014. Your responses should be e-mailed to the Legislative Clerk in Word format at **Kirby.Howard@mail.house.gov** and mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Lee Terry
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade
Attachment

Neiman Marcus | Group

Michael R. Kingston
Senior Vice President
Chief Information Officer

July 2, 2014

The Honorable Lee Terry
Chairman
Subcommittee on Commerce, Manufacturing and Trade
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Terry:

Thank you for the opportunity to testify at your hearing on February 5, 2014 entitled "Protecting Consumer Information: Can Data Breaches be Prevented?" I have attached responses to the written questions that Congresswoman Schakowsky and you posed following the hearing. The Neiman Marcus Group appreciates your interest and attention to this issue.

Sincerely,

Michael R. Kingston

CC: The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce, Manufacturing and Trade

Additional Questions for the Record

The Honorable Lee Terry

1. You testify you called a forensic investigative firm, per protocol required by the payment card brand, after receiving a common point of purchase (CPP) report indicating cards previously used at Neiman Marcus had been compromised and used to commit fraud elsewhere. Have you previously ever had CPP reports indicating a possible problem? If so, were you able to determine the original point of compromise?

   A. Neiman Marcus had not previously received a CPP report; thus the ones we received in December 2013 were the first CPP reports we had received.

2. You describe the reconnaissance efforts the malware conducted earlier in 2013 that enabled it to be customized to your system and further avoid detection. In general, are you able to say when or how the malware originally infiltrated your system?

   A. The earliest evidence of malware in our system according to our ongoing forensic investigation is in March 2013, when so-called reconnaissance malware began operating in our system. The investigation determined that this malware conducted reconnaissance efforts but did not attempt to scrape or obtain any payment-card data. The card-scraping malware operated in our system from July 16 to October 30, 2013, according to our forensic investigation. How the reconnaissance malware infiltrated our system remains unknown at this point, although our investigation is ongoing.

3. You describe how the forensic team created a custom decoder to decrypt the output files the malware had created and encrypted. Does that mean that encryption can be defeated by criminals as well?

   A. Encryption is clearly an important data security tool, and along with other techniques can be deployed to protect sensitive information. However, encryption cannot provide guaranteed protection, as there are ways to defeat it. Criminals commonly attempt to defeat encryption by stealing the encryption algorithm keys. Encryption can also be decoded, although it may be complex and very time-consuming to decode (and therefore decrypt) encrypted files. In our situation, our team of forensic investigators decoded the encrypted files that had been created by the hacker – an important step in order to help determine what the hacker had been attempting to accomplish, and how.

4. You appear to have over-notified customers in an abundance of caution based on what you now know. Has this experience led you to conclude whether or not we need to change current laws to address breach notifications? Are the laws flexible enough to address situations where you are still gathering information and don't know the extent of what happened?

   A. State laws vary in numerous ways regarding the required timing and scope of notification following a data security intrusion. As I discussed during my testimony, once a data intrusion is initially discovered, substantial forensic investigative work may be needed to determine whether malware was actually placed within the system, whether the

malware actually functioned in the system, whether it had the capability to successfully capture card data or other personal information and export it outside the system, and whether the data was successfully exported. Until most or all of these questions are answered, it may be difficult to answer the overall question whether a data breach actually occurred – which also may depend on the definition of "data breach," which varies by state.

I also discussed during my testimony that once a data intrusion is discovered, it is important to take steps to contain the intrusion – steps that may be complex and time-consuming and that require detailed knowledge about the intrusion. Otherwise, if notification is made before the intrusion is contained, there is a significant risk that the attacker might accelerate efforts to obtain captured account numbers, or that other cyber criminals might be encouraged to test the system for vulnerabilities.

While the statutes relating to data breach notification vary, we believe that in determining the appropriate timing of notifications, such statutes should recognize the time it takes for the entity that was the target of the intrusion to answer fundamental questions about the nature and scope of the intrusion, as well as to contain the intrusion.

The Honorable Jan Schakowsky

1. It is critically important that when large thefts of sensitive consumer data are carried out, the public is made aware quickly, both in the interest of transparency and so that those affected can act to prevent fraudulent activity. I am very interested in finding out more about the decision-making process that led to public notification of the Neiman Marcus breach. Some have raised concerns that this notification did not occur in as timely a manner as it could have.

    a. I understand that companies whose network systems are breached would like to have time to "dot the *i*'s and cross the *t*'s" – but for consumers, every hour matters. Please explain why Neiman Marcus disclosed its breach on January 10, 2014, to those customers with known fraudulent charges on their accounts, but waited until January 22, 2014, to notify the additional consumers whose payment card data may have been exposed to the malware. Additionally, why could such a broader notification not have gone out by (at the latest) January 16, 2014, when the company released on its website a public letter to customers?

A. Once Neiman Marcus determined that a data intrusion occurred, we were committed to notifying our customers, including those potentially affected by the intrusion, in a prompt and transparent fashion. In fact, on the very same day that our forensic investigators concluded that the malware had been disabled (January 10), Neiman Marcus announced publicly (including through press announcements and statements on our Twitter account) that we had suffered a data security incident and that some customers' payment card information had been potentially compromised. This announcement was widely disseminated by prominent print and broadcast media as well as social media. We also sent individual notices that same day (by email) and the next day (by letter) to all customers whose payment cards were listed on the then-received

CPP reports (about 2,400) for whom we had email and postal addresses. As I explained above and in my testimony, providing public notification prior to the date of containment would have been imprudent and risked attracting further hacker activity.

On January 16, our CEO Karen Katz issued a public letter, posted on our website with a prominent link from our home page, explaining that we had been the subject of a data security incident, and offering free credit monitoring and identity-theft insurance for one year to any customer who had used any payment card to conduct any transaction during the past year at any Neiman Marcus Group store or website.

These actions make it clear that Neiman Marcus took very strong steps to quickly notify all its customers and the general public about the data intrusion situation. Broad public notification is one important and effective way to provide notice to our customers, especially in situations like this when we still did not know which individual customers were potentially affected by the data intrusion. Initially, the only information we had about individual customers who may have been affected by the data intrusion was from CPP reports, which listed customers who had used their cards at Neiman Marcus and subsequently received fraudulent charges at some point. As I testified, determining how and when the malware had operated (and therefore which customers were potentially affected) was time-consuming, complicated work, even for expert forensic investigators, and included the work necessary to decrypt the malware's encrypted output files and ensure the malware was disabled. The investigators ultimately learned that the malware was highly sophisticated and was different than any other malware they had ever analyzed.

It was around the time of Karen Katz's January 16 letter that the investigators had completed sufficient work to become reasonably confident that the dates during which the card-scraping malware had been active were July 16 to October 30, 2013. This date range allowed us to preliminarily identify the universe of customers who were potentially affected by the data intrusion. Significant work was required to gather the contact information as to those customers for whom we had such information, and to prepare the letters and email notices.

Four business days later, on January 22, we issued an updated public notice on our website explaining the July 16 – October 30 period. The same day, we sent out individual email and letter notices about the incident to not only our customers who shopped at a Neiman Marcus store between these dates (for whom we had contact information) but also a much broader group of customers – any customer who used a payment card at any time in the past year for any Neiman Marcus Group purchase (whether in one of our stores or on our websites) and for whom we had contact information.

Through these acts of public and individual notification, Neiman Marcus acted promptly and appropriately to advise our customers of the situation and to provide them with timely and accurate information.

b. Having just recently gone through the response and public notification activities for the breach, what do you believe Neiman Marcus could have done differently in order to provide the public with more complete information on the breach at an earlier time?

A. As set out above, we provided widespread public notification (using both traditional and social media) on the very same day our forensic investigation concluded that the malware had been fully contained (which was merely four days after the specific nature of the data intrusion became known). Four business days later, our CEO posted an open letter on our website explaining that we had been the subject of a data security incident. Four business days after that, our CEO's public letter was updated based on additional information from the ongoing forensic investigation; information was provided about the apparent beginning and ending dates of the card-scraping malware's operation, and the number of customers potentially affected. We are proud of the prompt and broad manner in which we notified and provided important information to the public and our customers about the data intrusion.

2. At the Subcommittee hearing on February 5, 2014, one topic of discussion was the *FTC v. Wyndham* case, currently pending before the U.S. District Court for the District of New Jersey. During questioning, I asked you about a brief of *amici curiae* filed in support of the Wyndham position, which is that the FTC lacks the authority to enforce reasonable data security measures on the basis of the FTC Act's Section 5 prohibition on unfair acts or practices. This brief, which is enclosed for your review, represents four business associations, including the Retail Litigation Center, an arm of the Retail Industry Leaders Association (RILA). I asked you at the hearing if your company was a part of this brief through these associations, and whether your company agrees with the position taken by Wyndham. At the time, you indicated that you were not familiar with the case, but that "Neiman Marcus supports having standards in place for data security."

a. Yes or no, should Congress pass a law establishing federal data security standards, applicable to commercial entities including retailers and which would cover sensitive financial and non-financial personal information? If so, which agency do you believe should enforce the law? If not, why not – and what do you propose as alternative measures to enhance safeguards for consumers' personal information?

A. Technology evolves rapidly, so electronic data security standards necessarily need to evolve as well. Standards, guidelines, and recommendations are important and can be very helpful to companies seeking to ensure that they are taking all reasonable steps to keep sensitive personal information secure in a quickly-changing world with evolving and sophisticated security threats. Keeping those standards up-to-date, and ensuring that they strike the right balance between not being too vague and not being too inflexible, is a very difficult task for any entity. Whether Congress or another entity is best suited to establish such data security standards is a question beyond our expertise.

Following your response, I encouraged you to verify whether or not your company is part of an association that has supported the Wyndham position in the aforementioned brief.

b. Is Neiman Marcus a member of RILA, or does it have a working partnership with RILA or the Retail Litigation Center?

A. The answer to both questions is no.

c. Does Neiman Marcus agree with the position taken by Wyndham and the entities that filed the brief of *amici curiae* that the FTC lacks authority under the FTC Act's Section 5 to enforce reasonable data security measures? If so, what agency do you suppose should make sure that companies adequately protect consumers' personal data and are accountable to the public?

A. Neiman Marcus did not join the amicus curiae brief in the Wyndham case and has never taken the position that the FTC lacks authority to enforce data security under Section 5 of the FTC Act. We support data security standards and appropriate enforcement in this area.

June 18, 2014

Mr. Bob Russo
General Manager
PCI Security Standards Council
401 Edgewater Place, Suite 600
Wakefield, MA 01880

Dear Mr. Russo,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, February 5, 2014 to testify at the hearing entitled "Protecting Consumer Information: Can Data Breaches Be Prevented?"

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday July 2, 2014. Your responses should be e-mailed to the Legislative Clerk in Word format at **Kirby.Howard@mail.house.gov** and mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Lee Terry
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade
Attachment

PCI Security Standards Council

Payment Card Industry
Security Standards Council, LLC
401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

"Protecting Consumer Information: Can Data Breaches Be Prevented?"

February 5, 2014

QUESTIONS FOR THE RECORD

Mr. Bob Russo
General Manager, Payment Card Industry Security Standards Council, LLC

Questions submitted by Chairman Lee Terry

1. **Would chip-and-PIN technology have made it harder for the criminals responsible for the Target breach to use the card data they accessed?**

The use of EMV chip technology is likely to have reduced the value of the compromised data as it would inhibit the creation of counterfeit cards for in person transactions. However, global adoption of EMV chip technology, including broad deployment in the U.S. market, does not diminish the need for strong data security measures to protect against the loss of cardholder data. Payment cards are used in a variety of 'card-not-present' channels—such as electronic commerce—where today's EMV chip technology is not typically an option for securing payment transactions. Businesses must continue to strengthen data security protections that are designed to prevent the unauthorized access and exfiltration of cardholder data.

There are no silver bullets - one specific technological approach will not address all security challenges. Security requires a multi-layered approach that includes the use of PCI Security Standards. The potential for a breach and damages caused by a breach can be mitigated if the entity has preventative, detective, and incident response controls that employ a combination of people, process, and technology as outlined in the PCI Security Standards. The PCI Security Standards are a critical layer of defense in this battle against cyber criminals.

2. **How does your organization keep PCI data security standards up to date? Do they have to be modified every time a new type of malware appears?**

Since the threat landscape is constantly evolving, the PCI SSC expects its standards to do the same. Confidence that businesses are protecting payment card data is paramount to a healthy economy and payment process—both in person and online. That's why to date, more than one thousand of the world's leading retailers, airlines, banks, hotels, payment processors, government agencies, universities, and technology companies have joined the PCI Council as members and as part of our assessor community to develop security standards that apply across the spectrum of today's global multi-channel and online businesses. Our community members are living on the

front lines of this challenge and are therefore well placed, through the unique forum of the PCI Council, to provide input on threats they are seeing and ideas for how to tackle these threats through the PCI Standards.

The PCI Council develops standards through a defined, published three year lifecycle. Our Participating Organization members told us that three years was the appropriate timeframe to update and deploy security approaches in their organizations. In addition to the formal lifecycle, the Council and the PCI community have the resources to monitor and provide updates through standards, published FAQs, Special Interest Group work, and guidance papers on emerging threats and new ways to improve payment security. Examples include updated wireless guidance and security guidelines for merchants wishing to accept mobile payments.

For example, based on industry feedback, with the release of version 3.0 of the PCI DSS and Payment Application-Data Security Standard (PA-DSS, the standard that covers payment applications), the PCI Council made changes to address emerging threat areas such as third party remote access, POS terminal tampering, and to define vendor accountability. Similarly, our latest versions of security standards for Point of Sale devices requires a default reset every 24 hours that would remove malware from memory and reduce the risk of data being obtained in this way. By responding to these requirements, POS manufacturers are bringing more secure products to market that reflect the standards' development process that incorporates feedback from a broad base of diverse stakeholders in the payment industry.

Updates are aimed at providing the right balance of flexibility, rigor, and consistency to help organizations make payment security part of their "business-as-usual" activity, not something centered on an annual assessment.

Proper implementation and ongoing maintenance are critical to protecting card data, as highlighted by the recently released Verizon 2014 PCI Compliance Report. According to Verizon, researchers "continue to see many organizations viewing PCI compliance as a single annual event, unaware that compliance needs to have a 365 day-a-year focus." Organizations with security controls in place as part of complying with PCI security standards improve their chances both of avoiding a breach in the first place, and of minimizing the resulting damage if they are breached.

To support implementation and maintenance of PCI security controls the PCI Council manages a number of programs and listings of information on our public website. In addition to standards, PCI Council programs include: website listings of lab-tested secure PIN and non-PIN POS terminals and other payment devices; security of payment applications; testing and qualification of assessors performing PCI DSS audits, training and qualification of professionals to install payment equipment and software; and many other programs focused on the integrity of payment systems and third parties that merchants rely on to conduct business.

3. What are the differences between how small businesses comply with PCI versus what PCI requires of big businesses?

As a technical standard setting body, the PCI Council creates security standards, but is not involved in enforcement, compliance validation, or reporting. All organizations that accept, store, process or transmit payment card data are subject to the same PCI Security Standards. The

difference lies in how an organization reports its compliance with the PCI Security Standards to its acquirer and/ or payment card brand.

An organization that accepts a large number of payment card transactions may be subject to an annual physical assessment of its systems by contract with their acquiring bank or payment card brand. A smaller business may be required to complete a self-assessment questionnaire to understand and communicate its security posture with any business partners.

Question submitted by Ranking Member Jan Schakowsky

1. **At the Subcommittee hearing on February 5, 2014, a member of Congress inquired about the difference between chip-and-PIN and chip-and-signature payment cards. I understand, as you indicated in your response, that "the combination of PCI and EMV in any form" would be a "powerful solution for... face-to-face fraud and counterfeit cards." However, recent articles on The Verge and the *Washington Post's* Wonkblog have conveyed, respectively, that "[a] PIN is obviously stronger protection against fraud than a signature, which can be easily forged and is ignored by most cashiers anyway," and that "[c]hip and PIN is the most secure way to conduct a transaction because it prevents a card that's lost or stolen from being used by a thief at the point of sale by signing for the transaction." I would like to return to my colleague's question and ask: from a security standpoint, what is the difference between chip-and-PIN and chip-and-signature, and again, from a security standpoint, which provides stronger protection for consumers?**

From an overall data security perspective, which is the focus of the PCI Council, the strongest protection for consumers is the combination of EMV chip technology and PCI Security Standards.

Rather than focusing on a specific category of payment fraud, as EMV chip does with the face-to-face card present environment, the PCI Data Security Standard (PCI DSS) seeks to protect cardholder data anywhere this data is present within the payment ecosystem. In addition, the latest versions of the PCI Council's standards and programs for secure payment terminals, the PIN Transaction Security (PTS) requirements, requires a default reset every 24 hours that would remove malware from memory. When used together, EMV chip and PCI Security Standards can reduce fraud and enhance the security of the payments ecosystem.

EMV chip technology in any form provides an additional level of authentication at the point-of-sale that helps reduce card present and counterfeit fraud. Use of a PIN provides protection against lost and stolen card fraud. The PCI Council does not manage or develop standards around chip technology or authentication methods. Further information on EMV chip can be found on the website of the industry group responsible for this technology, EMVCo at www.emvco.com

In the case of recent breaches EMV chip technology could not have prevented the unauthorized access, introduction of malware, and subsequent exfiltration of cardholder data. The PCI Security Standards contain numerous security protocols that would prevent the insertion of malware and quickly detect any exfiltration of information, along with our latest PTS requirements that promote development of secure payment terminals. But in such a breach EMV

chip would have ensured that the value of the customer information that was compromised would have been greatly reduced.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

June 18, 2014

Mr. Phillip J. Smith
Senior Vice President
Trustwave Holdings
12127 Longridge Lane
Bowie, MD 20715

Dear Mr. Smith,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, February 5, 2014 to testify at the hearing entitled "Protecting Consumer Information: Can Data Breaches Be Prevented?"

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday July 2, 2014. Your responses should be e-mailed to the Legislative Clerk in Word format at **Kirby.Howard@mail.house.gov** and mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Lee Terry
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade
Attachment

Questions for the Record Response: Phillip J. Smith, Trustwave Holdings

Additional Questions for the Record

The Honorable Lee Terry

1. **How quickly would you imagine that best practices would need to change in order keep up with the changing tactics of cyber criminals? Is it realistic – or even possible - for the private sector to keep up with these sophisticated hackers?**

It's not that best practices necessarily need to change. They just need to expand and be followed. There are still basic best security practices to which businesses are not adhering. For example, according to our 2014 Trustwave Global Security Report, weak passwords opened the door for the initial intrusion in 31 percent of compromises we investigated in 2013 - the most commonly used being "Password1." Our 2014 State of Risk report revealed 63 percent of businesses do not have a fully mature method to control and track sensitive data and 58 percent of businesses use third-parties to manage sensitive data, yet almost half (48 percent) do not have a third party management program in place.

Using strong passwords, tracking sensitive data and creating third party management programs are all standard best practices that, in spite of the recent slew of high profile data breaches, are not being followed. In addition to following the ones that are already known, businesses should also be expanding their best practices due to the increasingly complex threat landscape, abundance of data that needs protection and wide use of consumer-owned devices (i.e. BYOD).

Businesses should create and regularly update BYOD policies, patch management programs, and incident response readiness plans. They should also perform risk assessments regularly and perform vulnerability scanning and penetration testing across all of their networks, applications, databases and devices to help identify and remediate security weaknesses before criminals exploit them.

2. **You referenced a study by Osterman Research that revealed 74 percent of the organizations surveyed were infiltrated by malware. If it is so pervasive, why has the market evolved to develop tools to make discovery easier?**

There are security tools that make malware identification and blocking easier however, from what we have seen, many organizations do not use them at all, use them incorrectly and/or solely rely on one technology instead of looking at the bigger picture.

Data protection requires multiple layers of technology combined with threat intelligence, manpower and expertise. One tool isn't enough. In order to stay ahead of malware attacks, businesses need to continuously be identifying and remediating security weaknesses within their infrastructure; they need to identify where their most valuable data lives and moves and install technologies that protect their attack vectors; they need to feed threat intelligence into those technologies so that they are updated to protect against the latest threats; and they need to monitor their controls 24-7 so that they can flag suspicious behavior and stop a criminal in his tracks. They need all of those elements combined with anti-malware technologies designed to detect and block malware before it reaches the end user.

The technology exists but the manpower and expertise behind it doesn't. A security control is only as effective as the people who manage it. According to our recent Security on the Shelf report, 28 percent of organizations are not getting the full value out of their security-related software investments. Of the $115 per user that organizations spent on security-related software in 2014, 33 dollars of this investment was either underutilized or never used at all. That means that for an organization of just 500 users, more than 16,000 dollars in security-related software investments was either partially or completely wasted.

3. You recommend separating systems that contain payment card data from other systems. Is this expensive? Is it practical for anyone but big companies?

The key is to find a security vendor that offers flexible solutions. Any size business should have the capability to separate their critical data from non-critical data. Vendors that offer flexible solutions, meaning the business only purchases what it really needs, are the best ones to partner with when it comes to data protection. We recommend that businesses turn to a managed security services provider for these kinds of controls. That way they are receiving the technologies, manpower and expertise, all for one subscription price that is paid annually and set for a number of years.

4. If Fortune 500 companies can be breached despite the resources they expend, does that suggest smaller companies with fewer resources are much more vulnerable?

Any business, no matter the size, is a target. However, the businesses that make it more difficult for a criminal to break in have less risk of being breached. Criminals look for the easiest path of resistance. If they encounter too many layers of security they will seek out another victim that's easier to attack.

The more resources businesses can dedicate to security, the better; however they need to make sure they are using those resources properly. Some larger companies may have the resources for security however they may not be using them in the right places. For example, they may be using their security budget to purchase various security technologies but then do not dedicate enough staff with specific security expertise to make sure those technologies are installed, updated and continuously working properly. They may have staff monitoring their behavior logs however those staff members may not be trained to know what to look for. They may have an incident response readiness program in place but they may never test that plan to identify and remediate any weaknesses within it. They may have an IT team and security team but the two may not communicate regularly opening up a potential vulnerability that's easy to avoid.

Smaller companies may have fewer resources but there are ways to fill that resource gap – such as partnering with an outside team of security experts (managed security services provider) – and strengthen their data protection.

5. Will security standards stop data breaches? If not, what is the appropriate response to limit risks of fraud and identity theft?

Security standards can help prevent data breaches but they need to be mandatory and can only go so far. For example, at the recent White House summit on cybersecurity, President Barack Obama focused on the importance of sharing threat intelligence across government agencies, law

enforcement and the private sector and how safe harbor protections for companies that participate should be in place. The remarks were a great beginning and helped bring data protection to the forefront of many business conversations but an Executive Order, which for the most part is voluntary sharing among the private sector, can only go so far. Executive Orders are just one part of the equation. Congressional action is required in order to encourage full cooperation from the private sector by providing protection for sharing data. This information is needed to protect the nation's critical infrastructure and our citizens' privacy. To do this effectively, we need public/private collaboration in creating mandatory requirements surrounding what kind of information must be shared, with whom and in what timeframe.

Security standards must also not be viewed as the be-all-end-all to security. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires all businesses that store, process or transmit payment card data to implement certain security controls. However, too many businesses simply "check the box" assuming compliance with the standard is the only security measure they need to take. Businesses should use the PCI DSS as the baseline to their security programs. It's a good beginning but far from an end. They need to treat compliance as an inherent result of continuously being secure. If they implement security controls based on their specific needs first, compliance should automatically be achieved.

.

6. Your Global Security Report states the average time to detect a breach is 210 days. Why does it take so long?

Oftentimes businesses do not have enough manpower and expertise dedicated to identifying and reporting suspicious activities. They may have the technology to log their activities however the people reading those logs may not understand what they should be looking for and, if they find something suspicious, what they should do next. According to our 2014 State of Risk report, 21 percent of businesses do not have incident response procedures in place and 20 percent of businesses do not have a process that enables the reporting of security incidents. Businesses need to create and regularly test an incident response readiness plan so they know how to flag suspicious behavior and what procedure they should follow if they do suspect a breach. By regularly testing this kind of plan they can identify and remediate any weaknesses in that procedure so that they are always prepared to detect and stop a breach.

7. Are there one or two recommendations you can make for the smaller companies with limited resources that are most effective in limiting vulnerabilities to criminal hacking?

As I mentioned above, smaller companies typically do not have the manpower and expertise dedicated to their security programs. They typically have one IT specialist who serves as a "jack of all trades" and does not have the time or expertise required to protect the organization's data. That is why we recommend smaller companies outsource their security needs to a third party team of experts whose sole responsibility is to install, update, monitor and manage their security enabling the in-house staff to focus on other priorities.

They should also incorporate basic security best practices such as using their point-of-sale systems only for payment transactions, using complex passwords or passphrases to access their applications, networks and databases and making sure their anti-virus is up-to-date and all software is patched.

8. **Trustwave's Global Security Report highlights a 400 % increase in mobile malware in 2012. What does that say about the future of mobile commerce? What are the risks to the average consumer who wants to use a smartphone for purchases or other commercial transactions? When it comes to PCs, we have software that can detect some types of malware. Are there tools consumers can use to scan for or protect themselves against malware on their mobile devices?**

Companies that develop applications for mobile commerce need to incorporate security during the development, production and active phase. This includes continuous scanning and testing of all networks, applications, databases and devices – all of which are key elements of a solid vulnerability management program. They need to make sure security is built in and not bolted on and by doing so they will reduce the risk of a consumer getting breached.

There are gateway technologies designed to detect and block malware that's attempting to infect PCs and mobile devices. These technologies can identify and strip out malware in real-time so that no end user gets infected. Consumers should also follow basic security best practices when using mobile devices. They should avoid accessing any sensitive information like their bank accounts on their devices. They should keep their devices locked when not in use with a pin, password or pattern etc. and treat third party applications with suspicion and skepticism. They should research the application before downloading it to see if someone has shared any feedback online. Some applications are designed specifically for phishing user data, so checking applications' permissions on the device before and after downloading it is critical. Some applications grant themselves access permissions and privileges on the device to secretly steal user sensitive data.

The Honorable Jan Schakowsky

1. **At the Subcommittee hearing on February 5, 2014, a member of Congress inquired about the difference between chip-and-PIN and chip-and-signature payment cards. I understand, as Mr. Russo of the PCI Security Standards Council indicated in his response, that "the combination of PCI and EMV in any form" would be a "powerful solution for... face-to-face fraud and counterfeit cards." However, recent articles on The Verge and the *Washington Post's* Wonkblog have conveyed, respectively, that "[a] PIN is obviously stronger protection against fraud than a signature, which can be easily forged and is ignored by most cashiers anyway," and that "[c]hip and PIN is the most secure way to conduct a transaction because it prevents a card that's lost or stolen from being used by a thief at the point of sale by signing for the transaction." I would like to return to my colleague's question and ask: from a security standpoint, what is the difference between chip-and-PIN and chip-and-signature, and again, from a security standpoint, which provides stronger protection for consumers?**

EMV is primarily an anti-fraud solution that relies on an authentication mechanism and provides tools to prevent counterfeiting of payment cards. It is largely silent on the theft of data from a merchant. It is a step in the right direction but it is not a silver bullet for security. Even with EMV technology businesses are at risk of man-in-the-middle attacks and EMV does not address e-commerce security. According to our 2014 Trustwave Global Security Report, in 2009, e-commerce compromises made up just 11 percent of assets targeted in the breaches we

investigated. In 2011, e-commerce compromises made up 20 percent of assets targeted, and in 2012 that number soared to 48 percent. Last year, the number of e-commerce breaches perched even higher, making up 54 percent of assets targeted. The increase may be partially due to other countries adopting EMV technology.

Since chip and PIN cards are harder to clone, many criminals are shifting their targets, moving from brick and mortar businesses to e-commerce. If they gain access to payment card information on a chip and PIN card, they can still use that information to make purchases online. Each chip-and-PIN payment card contains two different security codes - one on the magnetic stripe, the other on the chip. Existing protections make it near impossible to clone a payment card using the code on the chip however if criminals gain access to cardholders' account numbers and expiration dates, they can use the code on the magnetic stripe to make purchases from e-commerce sites.

Businesses cannot look at EMV as the be-all-end-all to security. They still need multiple layers of security controls in place which include continuously scanning and testing their applications, networks and databases for security weaknesses so they can remediate those holes and making sure they have enough manpower and expertise to monitor and update their security controls so that they can defend against the latest threats.