RPTS KERR

DCMN ROSEN

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, D.C.

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,

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

Mr. Terry. So, good morning everyone, and we have an impressive two panels to testify this morning. Our first are government witnesses. We have the chair from -- 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 that 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 a 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 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.

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 post 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 security 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.

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 we -- 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 prevent -- 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.

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

The Chairman. 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, private industry are doing everything necessary to protect the public from future breaches, and I yield the balance of my time to Mrs. Blackburn.

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, and now I recognize -- but before I officially recognize, say that 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.

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 chairman -- Edith Ramirez, chairwoman, 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:]

******** INSERT 1-1 ********

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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

[The prepared statement of Ms. Madigan follows:]

******** INSERT 1-2 ********

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 for convenience 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:]

******** INSERT 1-3 ********

Mr. Terry. Mr. Zelvin, you are now recognized for you 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 effort -- 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:]

******** INSERT 1-4 ********

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. Have you -- is the Secret Service, or are you involved in a -- in an 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 separate -- 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. Okay. 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. The -- 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 the -- 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 -- 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, you know, 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, you

know, where they are in the process once we are alerted to the fact that there has been -- a breach has taken place, and obviously we are, you know, 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, particularly on the -- 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, you know, 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. Should -- 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 -- you know, 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, you know, situations where literally the information is obtained because documentation with sensitive information is being thrown into a dumpster and people have, you know,

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 response -- 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. Okay. 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. Okay. 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.

RPTS MCCONNELL

DCMN HUMKE

[10:28 a.m.]

Mr. Barton. Okay. 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. Okay.

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? Okay --

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. Okay. 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.

Mr. Terry. [Presiding.] Without objection.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Dingell. 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.

[The information follows:]

******** COMMITTEE INSERT ********

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.

[The information follows:]

******** COMMITTEE INSERT ********

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. Okay, 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 companies 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. Okay, why don't we --

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

Mrs. Blackburn. Okay.

Ms. Ramirez. -- 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. Okay.

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. Okay, 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 -- no, I'm referring to company failures.

Mrs. Blackburn. You are referring to company failures. Okay, 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, you know, 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 could be -- that would enhance security --

Ms. Ramirez. Absolutely.

Mr. Welch. -- 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, you know, not just financial identity theft, but there are many other types of --

Mr. Welch. Right.

Ms. Madigan. -- 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 these systems. Today we have seen the change now, they are going to find -- 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 answers; 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. -- 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, okay, 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, you know, 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 any time 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, you know, 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 proactively 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 -- or 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 also out in the -- 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 company 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, you know, finding the fires and putting them out, but preventing them from happen to go 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. Yeah, 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 of 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 but 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 delayed 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, okay. 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 -- and 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 have 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. Okay, so outside of the United States.

Mr. Noonan. Yes, sir.

Mr. Johnson. Okay. 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 -- and 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 do we have -- 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, you know, 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. Okay, 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. Okay, 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. Okay, 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 working 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 a 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 notification 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. Yeah, I would like to work would 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.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. McKinley. Mr. Noonan, do you know anything about those breach these 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. Okay. 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 reevaluated. And so I think there is some more investigation to be done before reaching conclusions.

RPTS KERR

DCMN HUMKE

[11:30 a.m.]

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, but -- 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. Okay.

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. Okay. 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 INFORMAITON 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:]

******** INSERT 3-1 ********

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 websites 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 websites, 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:]

******** INSERT 3-2 ********

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:]

******** INSERT 3-3 ********

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 multi-national 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 website 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 industry 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. 73 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.

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 websites, 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:]

******** INSERT 3-4 ********

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. -- 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 don'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 compromise 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 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. Okay. 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. Yeah, forensic investigator.

Mr. Terry. Not Mr. Smith.

Ms. Schakowsky. Okay. 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 last.

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 notifying them of a breach of Target customer information and received that message from TargetNews@target.bfi0.com, and scammers use sometimes 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 -- 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 -- we 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 website. 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 forensic 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, you know, the chip-and-PIN technology has been around for a long time. I think, you know, a lot of effort should be put for new technology in securing, you know, 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 as 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. You know, I think we described 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, you know, 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 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. Okay. Well, I yield back. Thank you for your testimony. Yield back, Mr. Chairman.

Mr. Terry. Okay. At this time the Chair recognizes the vice committee of the full committee, and that is -- 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. Okay. 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. Okay.

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. Okay. 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.

[The information follows:]

******** COMMITTEE INSERT ********

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. Okay

Mr. Russo. -- 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. Okay. 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, okay, 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. Okay. 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 for -- 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 real -- in 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.

RPTS MCCONNELL

DCMN HUMKE

[12:27 p.m.]

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, you know, 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 mean, I know that is the kind of the area you look at, if you are -- I mean, 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, you know, 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 Website for the small merchants to, you know, 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 are 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. Okay.

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. Okay, 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. Okay. 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 is still some important questions that we haven't answered in our investigation, but with what we have learned so far, it is 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. Yeah, yeah. 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. Okay. 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, you know, 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. Okay, 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 -- 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. Okay, 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, you know, 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. Okay. 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 Targets' 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 when 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. Okay.

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. -- 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 -- so 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 when we were last -- 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, with -- 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.]