AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 113–305

SAFEGUARDING CONSUMERS' FINANCIAL DATA

HEARING

BEFORE THE

SUBCOMMITTEE ON
NATIONAL SECURITY AND INTERNATIONAL TRADE
AND FINANCE

OF THE

COMMITTEE ON
BANKING, HOUSING, AND URBAN AFFAIRS
UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

ON

EXAMINING THE PROCEDURES FOR OVERSEEING DATA SECURITY AND BREACHES OF DATA SECURITY BY THE UNITED STATES SECRET SERVICE AND THE FEDERAL TRADE COMMISSION

FEBRUARY 3, 2014

Printed for the use of the Committee on Banking, Housing, and Urban Affairs

Available at: http://www.fdsys.gov/

U.S. GOVERNMENT PUBLISHING OFFICE

88–374 PDF WASHINGTON : 2015

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

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

TIM JOHNSON, South Dakota, *Chairman*

JACK REED, Rhode Island
CHARLES E. SCHUMER, New York
ROBERT MENENDEZ, New Jersey
SHERROD BROWN, Ohio
JON TESTER, Montana
MARK R. WARNER, Virginia
JEFF MERKLEY, Oregon
KAY HAGAN, North Carolina
JOE MANCHIN III, West Virginia
ELIZABETH WARREN, Massachusetts
HEIDI HEITKAMP, North Dakota

MIKE CRAPO, Idaho
RICHARD C. SHELBY, Alabama
BOB CORKER, Tennessee
DAVID VITTER, Louisiana
MIKE JOHANNS, Nebraska
PATRICK J. TOOMEY, Pennsylvania
MARK KIRK, Illinois
JERRY MORAN, Kansas
TOM COBURN, Oklahoma
DEAN HELLER, Nevada

CHARLES YI, *Staff Director*
GREGG RICHARD, *Republican Staff Director*

DAWN RATLIFF, *Chief Clerk*
KELLY WISMER, *Hearing Clerk*
SHELVIN SIMMONS, *IT Director*
JIM CROWELL, *Editor*

SUBCOMMITTEE ON NATIONAL SECURITY AND INTERNATIONAL TRADE AND FINANCE

MARK R. WARNER, Virginia, *Chairman*
MARK KIRK, Illinois, *Ranking Republican Member*

SHERROD BROWN, Ohio
JOE MANCHIN III, West Virginia

JERRY MORAN, Kansas

MILAN DILAL, *Subcommittee Staff Director*
LINDSEY JOHNSON, *Republican Subcommittee Staff Director*

C O N T E N T S

MONDAY, FEBRUARY 3, 2014

	Page
Opening statement of Chairman Warner	1
Opening statements, comments, or prepared statements of:	
Senator Kirk	3
Prepared statement	35

WITNESSES

William Noonan, Deputy Special Agent in Charge, Secret Service, Criminal Investigative Division, Cyber Operations Branch	4
Prepared statement	36
Jessica Rich, Director, Bureau of Consumer Protection, Federal Trade Commission	5
Prepared statement	43
Response to written questions of:	
Senator Kirk	75
James A. Reuter, Executive Vice President, FirstBank, on behalf of the American Bankers Association	18
Prepared statement	48
Response to written questions of:	
Senator Kirk	77
Mallory Duncan, General Counsel and Senior Vice President, National Retail Federation	19
Prepared statement	54
Response to written questions of:	
Senator Kirk	79
Edmund Mierzwinski, Consumer Program Director, U.S. PIRG	21
Prepared statement	63
Troy Leach, Chief Technology Officer, PCI Security Standards Council	22
Prepared statement	69
Response to written questions of:	
Senator Kirk	81

Additional Material Supplied for the Record

Letter from the Independent Community Bankers of America	86
Letter from the National Association of Federal Credit Unions	88
Letter from The ClearingHouse	92
Letter from the Credit Union National Association	94

SAFEGUARDING CONSUMERS' FINANCIAL DATA

MONDAY, FEBRUARY 3, 2014

U.S. SENATE, SUBCOMMITTEE ON NATIONAL SECURITY AND INTERNATIONAL TRADE AND FINANCE, COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
Washington, DC.

The Subcommittee met at 3:05 p.m. in room SD–538, Dirksen Senate Office Building, Hon. Mark Warner, Chairman of the Subcommittee, presiding.

OPENING STATEMENT OF SENATOR MARK R. WARNER

Senator WARNER. I call to order this hearing of the National Security and International Trade and Finance Subcommittee titled, "Safeguarding Consumers' Financial Data." I am going to go ahead and introduce the two witnesses now and then make a brief opening statement and see if Senator Kirk is here to make an opening statement. Since we have got two panels, if my colleagues do not mind, we will go straight then to let our witnesses give their presentations because we have got—this is a subject that has generated an enormous amount of interest, and I am very appreciative of both the panels.

In the first panel, we are going to hear from Mr. William "Bill" Noonan, who is the Deputy Special Agent in Charge of Secret Service's Criminal Investigative Division, Cyber Operations. In this position he oversees the Service's cyber portfolio. He has over 20 years of Federal Government experience. Throughout his career he has initiated and managed high-profile transnational fraud investigations which involve network intrusions and the theft of data and intellectual property from financial institutions and Government systems. Welcome, Mr. Noonan.

Ms. Jessica Rich is the Director of the Bureau of Consumer Protection at the FTC. She has held a number of senior positions at the FTC, including Associate Director in charge of the Division of Financial Practices and Assistant Director of the Division of Privacy and Identity Protection. She joined the FTC as a staff attorney more than 20 years ago. Welcome, Ms. Rich.

This is a subject that has garnered a lot of public attention recently, and I think as somebody who spent still a longer career in technology than I have in Government, this is an area that I think is going to—we are going to see an exponential rise in consumer interest, press interest, and others as we try to get our arms around a challenge that is only going to grow in terms of all of our lives.

In recent weeks we have heard of massive data breaches at Target, Neiman Marcus, and other retailers. For example, at Target alone more than 40 million cards were compromised, and up to an additional 70 million consumers' other information was taken. So not only were the cards taken, but people whose cards' data was not taken, their data was compromised as well.

Let me make clear that while we will talk about these particular retailers, this is not a witch hunt, at least from my perspective, about any particular retailers' actions or inactions. Quite honestly, I think we are going to see—and I know from my role in the Intel Committee, this is a crime that happens daily to financial institutions and retailers at a level that, frankly, if most Americans realized, I think would find rather confounding.

I at one point had a much longer statement, but, you know, there are three areas that I think we need to focus on. As we sort through this issue, we need to understand that we do not need another—I do not need, at least—long-term fight between the bankers, the retailers, and the card industry. Many of us up here have gone through the challenges rightfully felt around the interchange battles, but a repeat of that kind of delay in getting a solution serves no one. The hackers in Russia, China, Ukraine, and throughout the world are not waiting for America to get its act together on this issue. They are continuing to strike us every day.

To better protect consumers, our financial institutions, the networks, and merchants should work together to continue to innovate on antifraud technology. As I said, the public cannot afford a year or multiple years of legislative battles like we saw over interchange fees. Every minute of every day the hackers and the cyber thieves are attacking our vulnerabilities.

Second, as somebody who has spent a career in technology, in many ways this is fundamentally a technology problem, and technology can provide part of the solution. We have already seen data that shows that the card protection system used in Europe, the so-called chip-and-PIN system, is much more effective than what we have at present in the United States, in terms of the swipe system, in terms of preventing fraud at point of sale. But we should not assume that any single technology is a silver bullet solution. Technology, as we all know, will continue to evolve on a weekly/monthly basis, and we have to continue to stay ahead. As a matter of fact, we have seen in Europe that while the chip-and-PIN system dramatically decreased, for example, in the U.K. the amount of fraud and cyber theft at point of sale, we saw a dramatic increase then in online fraud and cyber attacks. So I hope we are able to discuss technology solutions, not just chip and PIN, but as we look, for example, on the online issue, I think there is enormous promise in this emerging field of tokenization, which can provide a more encrypted solution set not just for point of sale but for other solution sets.

Let me say again we are not here to endorse any specific technology product or services, but, again, I think this is an area where we need great collaboration.

Third, Government has a role to play. Industry has a role to play. But as consumers, we need to be more vigilant as well. Consumer financial exposure is more limited with credit cards. Here is

industry personal debit. I will try to hold the numbers back a little bit. But I have to tell you, until a few weeks ago I did not realize that my debit card protections are not as great as my credit card products. I will let the record show that I do not show the numbers on the other side. But that even with debit card protections, there are—with this challenge around debit card protections, we have got to see if we can perhaps look at raising those standards to at least equaling credit cards. Debit card use has been growing like mad, transactions tripling since 2003. And, again, I think we look—I think about my kids who have debit cards, and large portions of the underserved community use debit cards. They are going to be a fact of life, and we have to figure out a way to sort that through.

And, finally, I think while we talk about—one of the most frightening things that I heard as I sorted through this and we are thinking about cards and protecting consumer privacy, in many ways we have focused so far on the challenge around protecting credit cards and debit cards, but the real potential exposure we have is if people can actually get into our bank account or online transactions that we all do more and more online banking and other services. That offers an area where there are very few protections at this point and almost unlimited liability for consumers.

So one of the challenges we have is, yes, we have got a role for industry, we have got a role for Government, but we all have a role as Americans to make sure you take that extra protection to occasionally change your PIN number, to make sure you never reveal your bank account information number, that you constantly report if you feel like there has been instances of fraud. This is a role that all Americans are going to have to play a continued increased vigilance in.

With that, I will ask for any opening comments from my friend Senator Kirk, and then we will go to the witnesses.

STATEMENT OF SENATOR MARK KIRK

Senator KIRK. I thank you for having this hearing, Senator. Mr. Chairman, I would just put a face to this crime that we are talking about. Albert Gonzalez—if you could hold that up—was convicted in 2010 of stealing 40 million credit card records that he made so much money off this he even bought his own Italian island off the profits. He is now serving 20 years in prison, and that is in line with the legislation that I will be introducing that calls for a 25-year Federal minimum mandatory for the theft of a million records or more, just to say to whoever would do this in a massive scare, good-bye, you are off to prison for a significant portion of your life. I am looking for bipartisan cosponsors.

Senator WARNER. Well, I think that the question of enforcement has got to be an area that we focus on. I think there will be some bipartisan interest in it.

All right. With that, again, I look forward to an exciting and robust discussion. And, Mr. Noonan, if you want to start, and then we will go to Ms. Rich.

STATEMENT OF WILLIAM NOONAN, DEPUTY SPECIAL AGENT IN CHARGE, SECRET SERVICE, CRIMINAL INVESTIGATIVE DIVISION, CYBER OPERATIONS BRANCH

Mr. NOONAN. Good afternoon, Chairman Warner, Ranking Member Kirk, 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 criminals 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 the recent breaches, and we are confident we will bring these criminals responsible to justice.

However, data breaches like the recent events are part of a long trend. In 1984, Congress recognized the risks posed by increasing use of information technology and established 18 U.S.C. Sections 1029 and 1030 through the Comprehensive Crime Control Act. These statutes defined access device fraud and misuse of computers as Federal crimes and explicitly assigned the Secret Service authorities to investigate these crimes.

In support of the Department of Homeland Security's mission to safeguard cyberspace, the Secret Service investigates cyber crime through the efforts of our highly trained special agents and the work of our growing network of 33 Electronic Crimes Task Forces, which Congress has 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 arrested nearly 5,000 cyber criminals. In total, these criminals were responsible for over $1 billion in fraud losses, and we estimate our investigations prevented over $11 billion in fraud losses.

Data breaches like the recently reported occurrences are just one part of a complex 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 this data; three, distributing or selling the sensitive data to their criminal associates; four, engaging in sophisticated and distributed frauds using the sensitive information 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 our Nation from this threat. We disrupt every step of their five-part criminal scheme through proactive criminal investigations, the defeat of

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

Through the 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 and academia to research cyber threats and publish information on cyber crime trends through reports like the CERT Insider Threat Study, the Verizon Data Breach Investigations Report, 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 payments 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 partnership 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 are looking forward to your questions.

Senator WARNER. Thank you.

Ms Rich.

STATEMENT OF JESSICA RICH, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Ms. RICH. Chairman Warner, Ranking Member Kirk, and Members of this Committee, I am Jessica Rich, Director of the Bureau of Consumer Protection at the Federal Trade Commission. I really appreciate this opportunity to present the Commission's testimony on data security.

In today's interconnected world, personal information is collected from consumers wherever they go. From the workplace to shopping for groceries, from our smartphones to browsing the Web at home, virtually every action we take involves the collection of information, some of it very sensitive. Many of these data uses have clear benefits, but the recent spate of data breaches are a strong reminder that they also create risks for consumers. Hackers and others seek to exploit vulnerabilities to obtain and misuse consumers' personal information. And all of this takes place against the backdrop of the threat of identity theft, a pernicious crime that harms both consumers and businesses.

The Bureau of Justice Statistics estimates that over 16 million people were victims of identity theft in 2012 alone. The FTC is committed to protecting consumer privacy and data security in the private sector. Since our first data security case in 2001, the FTC's data security program has been a strong, bipartisan effort that includes law enforcement, education, and policy initiatives.

The FTC enforces several laws that protect consumer data. Under the FTC Act, the agency can take action against companies that engage in deceptive or unfair practices, including deceptive or unfair data security practices. The FTC also enforces several laws that require special protections in certain business sectors—in the credit reporting industry, among financial institutions, and also among online services for our kids.

In enforcing these laws and investigating patient data security failures, the Commission recognizes that there is no such thing as perfect security and instead examines whether companies have undertaken reasonable procedures to protect consumer data from the risk of identity theft and other misuse.

Since 2001, the FTC has used its authority to obtain settlements with businesses—to obtain 50 settlements with businesses that failed to provide these protections. The FTC's best-known case may be its 2006 action against ChoicePoint, a data broker that allegedly sold sensitive information about more than 160,000 consumers to thieves posing as ChoicePoint clients. The Commission alleged that ChoicePoint failed to use reasonable procedures to screen prospective purchasers of consumer data and ignored obvious security red flags, resulting in at least 800 cases of identity theft.

Before ChoicePoint, the FTC brought actions alleging security failures by such companies as Microsoft, Petco, Guess, BJ's Wholesale, and DSW Shoe Warehouse. And after ChoicePoint, the FTC has brought cases alleging security failures by such companies as TJX, Card Systems Solutions, Lexis/Nexis, LifeLock, CVS, Rite Aid, and HTC. Many of our cases spanning over the course of 14 years allege similar, commonly known vulnerabilities and security failures.

In addition to enforcement, the Commission promotes strong data security through consumer education, business guidance, and policy initiatives. For example, our Web site contained guidance for consumers about what to do in the event of a breach. And perhaps our most important education piece is our guide to businesses about how to develop a strong data security program.

Sitting here today with my colleague from the Secret Service, I want to emphasize that data security is a shared responsibility among many different entities and people, including the different law enforcement agencies that work in this area. The Commission has a long history of working closely with other Federal and State agencies on this important issue. For example, the FTC's LifeLock case was a joint action with 35 State AGs, and the FTC received assistance from 39 State AGs in its case against TJX. We also worked jointly with the Department of Homeland Security in our cases against CVS and Rite Aid.

The FTC also coordinates with criminal enforcement agencies such as the FBI and Secret Service. The goals of the FTC and the criminal agencies are complementary. Criminal actions seek to

punish hackers and other intruders that steal customer data while FTC actions focus on shoring up security protections at companies to prevent intruders from getting inside in the first place.

Let me conclude with a final point on data security legislation. Never has the need been greater. In its testimony, the Commission reiterates its bipartisan support for Federal legislation that would strengthen the FTC's existing authority governing data security and require companies to notify consumers when there has been a security breach.

Thank you for the opportunity to testify here today. The Commission looks forward to continuing to work with Congress on this critical issue.

Senator WARNER. Thank you. Thank you both.

I also should point out that last week I asked a question of DNI Clapper. He had made an estimate that cyber attacks on our economy were in excess of $300 billion worth of damage, and that was a last-year report. I asked him, he says that number is probably dramatically increased, and that was in public testimony last week. Obviously that goes beyond just the question of individual data breach. But this is an issue that, again, I believe is going to grow dramatically.

I also understand, Mr. Noonan, that the Secret Service does not want to weigh in on specific technology solutions, chip-and-PIN, EMV, tokenization. But we are going to need your cooperation at some point and guidance on how working with industry and whatever standards come about that we have got the most cutting-edge technology.

I guess my first question for you, Mr. Noonan, is: Why is it that the Secret Service or even security bloggers are oftentimes the first to know about these attacks? I understand we have got industry PCI standards that are set, but, you know, this news keeps floating out more. The Target breach, to my understanding, originally floated from a blogger, and in one of these blogs, Brian Krebs said that they first identified the malware that was involved in the Target breach back in 2011. Why is it taking us so long to respond? And is that some constraint on you? Or is that not enough aggressive action from industry?

Mr. NOONAN. Sir, first you got into the fact that sometimes the Secret Service knows ahead of time about these breaches and we are able to bring it to the attention of different victims. So the fact that we do that, it is through proactive investigations where we are out sometimes ahead, determining and looking at data as it relates to financial industries. It is through partnerships that we have in the financial industry sector that is able sometimes to bring us data where we are able to go through and parse through that data, be able to find out where information is leaking into the criminal underground from. So, too, is the same way, I believe, that some journalists are able to get hold of some of that information as well.

You also brought up the malware and the fact that it has been around since 2011. I think what we are discussing here is that it is the type of malware. So it is not necessarily that exact type of malware. Malware can be molded and changed per attack. Of course, these attackers are molding malware so it is not picked up through antivirus and through technical means that general IT se-

curity folks would have. So these are very sophisticated criminal actors that are not using just regular malware. They are modifying that malware for each particular high-tech attack when we are talking about an attack of this significance.

Senator WARNER. Well, I guess one of the things that I know my colleagues will want to press on, too—this is both for you and Ms. Rich. How do you get the standard right on when it becomes the duty of the company or the financial institution to report an incursion? You know, particularly since this evolves all the time, and, you know, I know there are standards set, but that has got to be constantly evolutionary. Do we have it right? Do you need more tools? Do we need to do this in—I believe we need to do this in collaboration with industry, setting a regulatory process that would be static in an area that moves this quickly. I would like to get you both quickly to weigh in on this, and then I have got one last quick question for Mr. Noonan. Ms. Rich, do you want to start?

Ms. RICH. Well, the Commission supports Federal standards for both data security and breach notification. Right now there are State laws requiring breach notification, but no standard at the Federal level and no civil penalties. And while we have tools and we are using them to enforce—to address data security failures by companies, it would be extremely helpful to have a Federal law requiring data security, not just notification, with civil penalties.

Senator WARNER. How do you make sure that laws can evolve quickly enough so you do not—if you think about NIST or other standards, it sometimes takes 7 years to evolve. This is a field that changes on a monthly basis.

Ms. RICH. We believe that the legal requirements should require a process for developing appropriate data security so that the specific technical standards can evolve and perhaps be implemented through self-regulation or industry standards. But we do have one regulation in the financial area that is already a model for this called the Gramm-Leach-Bliley safeguards rule that really sets forth a process. You have to put somebody in charge, you know, your chief technology officer. You have to do a formal risk assessment. You have to then implement safeguards in key areas of risk, such as employee training, network and physical security, service providers, *et cetera.* And it sets out a process like that, and we are able to use that as a tool for enforcement without mandating levels of encryption and things that change over time.

Senator WARNER. Mr. Noonan, could you add—and I want to respect all my colleagues' time. Could you also identify for us—we saw in the Target public indications that it might have been from Ukraine, but where some of these criminal activities seem to be generating from? And then we will move to Senator Kirk.

Mr. NOONAN. Sure, sir. Many of these international, transnational cyber criminals are attacking us from Eastern Europe. I do not want to say that it is one country versus another country. What we are seeing is that largely the cyber criminal world is using the Russian-speaking language—I say Russian speaking in the fact that they are using the Russian language as an operational security. So that is the piece that the criminal underworld is using to hide themselves from U.S. law enforcement.

Senator WARNER. Senator Kirk?

Senator KIRK. A real quick question for Mr. Noonan. You describe the general Russian origin of a lot of these attacks. Could you describe your international cooperation with Russian law enforcement on this issue?

Mr. NOONAN. There have been many events where we have worked with the Russian law enforcement to some degree of cooperation. There are times——

Senator KIRK. Vladimir Putin is not exactly our best friend. Could you give a grade to the level of cooperation that we have received for——

Mr. NOONAN. Yes, sir. We do most of our work through the Office of International Affairs and through DOJ's computer hacking—or CCIPS, Computer Crimes and Intellectual Property Section. And, generally, the cooperation that we deal with with the Russian authorities is generally through that mechanism, through the CCIPS 24/7 notification process to get the process taken care of in the Russian Federation.

Senator KIRK. The only quick follow-up I would say, have you had any extraditions from Russia?

Mr. NOONAN. Negative, sir. We have not had any extraditions from Russia.

Senator KIRK. Thank you, Mr. Chairman.

Senator WARNER. Senator Warren.

Senator WARREN. Thank you, Mr. Chairman, Ranking Member. Thank you for holding this hearing.

All of us have constituents who are affected by these data breaches, and I think it is clear that the data protections we have in place now are not enough. In 2012, 16.6 million people, 7 percent of the adult population, in a single year were victims of identity theft. It is a huge number. So I would like to get a better sense of how these laws are enforced.

The FTC has authority to go after companies that engage in either deceptive or unfair practices. I want to break those two out, if I can.

Ms. Rich, can you describe what a company must do with regard to its data security standards for the FTC to bring a claim for deceptive practices?

Ms. RICH. Well, our deception authority focuses on making statements or omitting information that is material, and so our cases in this area generally involve statements that can be express—you know, "We encrypt our data to the highest levels of blah, blah, blah"—or implied, "We really care about your data security, the security of your data, and if you give data to us, nothing bad will come of it." And we look to see if those claims are true by asking a lot of questions, getting data, doing hearings with officials at companies, and consulting with experts to determine whether those claims are true.

Senator WARREN. OK. Ms. Rich, let me just clarify this. If a company's security standards are inadequate but the company says nothing about them, then the FTC is powerless, at least under its authority, to go after deceptive practices. Is that right?

Ms. RICH. We have two prongs of our Section 5 authority, and the other is unfairness.

Senator WARREN. I am going to come to unfairness in just a minute. I just want to find out how helpful "deceptive" is for a company that has totally inadequate data protection standards. And I just want to clarify. I think what you are saying to me is if the company never says they have great data protection standards, then the answer is, under the deceptive prong, the FTC has no authority to go after this company. Is that right?

Ms. RICH. That is absolutely right, and that is one of the reasons that we are supporting general data security legislation. But let me say we do also have unfairness authority and——

Senator WARREN. So I am going to come there.

Ms. RICH.——and we use our deception authority to look at not just what is stated in a privacy policy, but what the company may claim in the context of its interaction with consumers, including implied claims such as a seal.

Senator WARREN. OK. But under your authority to go after deceptive practices, I understand that the FTC has settled about 30 data security cases since 2002. That would be about 3 per year. So I think it is fair to say that is not very many given the number of data breaches that we have seen over the last decade.

Ms. RICH. Well, I would emphasize that there is not strict liability for a breach. When a breach happens, we look at the underlying practices and not whether there was a breach and then we automatically bring a case. And I would also emphasize that we believe our 30 deception cases and our 20 unfairness cases provide very strong general deterrence as well as specific deterrence, especially given the kind of remedies we seek. And we do believe that our work in this area has brought a lot of attention to the need to secure data and has made a difference in raising the stakes. But we do need more tools.

Senator WARREN. Well, so let us talk about that just a little more. In addition to the 30 cases you have brought over the course of a decade under deceptive practices, I just want to ask you about unfair practices. Can you describe what a company must do with regard to data security standards for the FTC to bring a claim for unfair practices?

Ms. RICH. Well, we have a three-prong test that we need to meet to use our unfairness authority, and one of those is substantial injury. But in many of these breach and—well, these data failure cases—again, it is not strict liability for breach—we have met that standard and we, therefore, have brought those cases.

Senator WARNER. So I understand—and if I am understanding this correctly, you are describing a fairly demanding standard since, as you say, it is more than breach, more than the fact that people have been injured, more than the fact that a company had very lax standards. In fact, as I understand it, there is a great deal—there is some question around the FTC's authority in this area, which may be why you have used unfair practices in only 20 cases over 10 years.

I just want to say I think this is a real problem that the FTC's enforcement authority in this area is so limited. The FTC should have the enforcement authority it needs to protect consumers, and it looks like to me it does not have that authority right now. Data security problems are not going to go away on their own, so Con-

gress really needs to consider whether to strengthen the FTC's hand.

Thank you, Mr. Chairman.

Senator WARNER. Thank you, Senator Warren. I think an interesting line of questioning, and I do think, you know, we oftentimes see—you may have a series of players in an industry who are meeting those standards. The challenge is you may have that one weak link, and the whole industry sector could be infected because of the weak link. So I think there should be some more ability to collaborate here.

Senator Johanns.

Senator JOHANNS. Thank you, Mr. Chairman.

Let me start out in the international front, if I could, and maybe follow up on Senator Kirk's questions a little bit. Is there any data available that would illustrate to us what percentage of attacks come from someplace outside of the United States? Is that data available? Either one of you. Go ahead, Mr. Noonan.

Mr. NOONAN. Sure, I am certain that it is. I will have to—if you do not mind, I can respond back to you in writing at some point.

Senator JOHANNS. Yes.

Senator JOHANNS. Just for the purposes of the hearing, would it be the majority of attacks, do you think?

Mr. NOONAN. I would say a majority of the significant attacks, sir, are from outside our borders.

Senator JOHANNS. And to put a finer point on that, would the majority of attacks then be coming out of Eastern Europe that are foreign attacks?

Mr. NOONAN. Yes, sir, that is the belief of the Secret Service.

Senator JOHANNS. Now, in terms of the cooperation that we get out of that part of the world, can you think of any case at all where there has been an extradition from Eastern Europe where a hacker was sent to the United States for prosecution, any case?

Mr. NOONAN. Yes, just recently we had a case out of Romania.

Senator JOHANNS. Romania?

Mr. NOONAN. Yes, sir.

Senator JOHANNS. Is that rare?

Mr. NOONAN. With the Romanian authorities, we are working very, very closely with them at this point. So it is not rare on that occasion. But in other countries within Eastern Europe, potentially it could be rare, yes.

Senator JOHANNS. What I am getting to—and I am not trying to be coy here—is that it looks to me like Eastern Europe or substantial parts of Eastern Europe are a sanctuary if you are a hacker, because the chances of being sent over here to face prosecution and conviction and jail time are probably nonexistent. Would you agree with that statement?

Mr. NOONAN. Yes, I would agree.

Senator JOHANNS. That is kind of a bad deal, no matter how secure you are, because at the end of the day, if those folks are not facing the possibility of prosecution, they are just going to keep going.

Mr. NOONAN. Yes. However, we do have some very strong partnerships within some of the countries over in Eastern Europe, which it is through those collaborative efforts that we are making

gains against a number of the cyber criminals. So to say that we do not have cooperation in Eastern Europe is not 100 percent accurate.

Senator JOHANNS. Sure.

Mr. NOONAN. It is through many of the different law enforcement authorities that we do have a strong collaborative effort in moving toward some of these cyber criminals and identifying who these actors are and learning more about their networks.

Senator JOHANNS. Right. Let me, if I might, focus on breach notification, because I think from the consumer's standpoint, that is critical. You know, as consumers we want to have the ability to trace a hacker to Romania or wherever. But the one thing that we do have is, if we are given notification, that we have the ability to stop using the card or tear it up or notify our creditors. We can be proactive.

Ms. Rich, how important would you say breach notification is in our effort to protect consumers?

Ms. RICH. I think for the very reasons you say, it is extremely important, which is why we support a law at the Federal level with civil penalties.

Senator JOHANNS. How do we do that—and I do not want to get into a sensitive area, but this is a sensitive area. As a former Cabinet member, I can tell you I know we had millions of records from citizens that contain sensitive information: Social Security numbers, data of birth, residence address, on and on and on. And I will also add that oftentimes the Federal Government's security system is not the best. I wish it was, but it is not the best. And it could be the health care law, it could be the VA, it could be the Department of Agriculture, it could be a whole host of things.

What mandate do we have on the Federal Government that if my information, at whatever department, has been compromised, somebody is going to let me know that?

Ms. RICH. You mean what laws govern the Federal Government's collection of information?

Senator JOHANNS. Yes.

Ms. RICH. There are laws that require—a number of laws that require data security among Federal Government agencies as well as breach notification. I am not completely familiar with the details of all of those, but I know, that if any breach happens in my Bureau, who we are supposed to report it to.

Senator JOHANNS. Do you know of any breach notification requirements in the health care law?

Ms. RICH. I am not familiar with all the details of the health care law. But I did want to add, on the point you were making about Eastern Europe, that because there are always going to be criminals and they may be coming from countries where it is very difficult to trace, that is why it is this partnership, this joint effort among different approaches and different agencies. We cannot just count on criminal enforcement. It is very important that companies also shore up their systems as much as they can against attacks. We need to attack this problem from different angles.

Senator JOHANNS. Thank you, Mr. Chairman.

Senator WARNER. Thank you, Senator.

Senator Tester.

Senator TESTER. Thank you, Mr. Chairman. Thank you for holding this hearing.

As long as we are talking about breach, we will flesh it out a little more. The breach I think you were talking about with Senator Johanns was between the financial institution and the card holder. Is there any breach requirements between the retailer and the financial institution or the retailer and your office, Mr. Noonan, or your office, Ms. Rich?

Ms. RICH. There are State laws that require breach notification that may apply to retailers, but there is no Federal breach notification law.

Senator TESTER. OK. So there are no breach requirements across the board, whether it is to the card holder or between the retailer and the banks, or the retailer and the investigative services, or the banks and the investigative services. There is no breach requirements across the board?

Mr. NOONAN. Again, not that I am aware of.

Senator TESTER. Could you tell me when the breach happened on Target?

Mr. NOONAN. The breach at Target is still an ongoing investigation.

Senator TESTER. No, but when did it actually happen? When did the breach happen? Maybe it is an unfair question. When did the actual attack to their database happen? What date?

Mr. NOONAN. Again, it is an active investigation, so we cannot necessarily get into the specifics at this point.

Senator TESTER. So you cannot tell me how much time it was before you found out about it to be able to start your investigation and when the breach actually happened?

Mr. NOONAN. No, I cannot at this point.

Senator TESTER. It was a period of time, though.

Mr. NOONAN. Actually——

Senator TESTER. It was not immediate?

Mr. NOONAN. It is through proactive—I will get back to it in a moment if I can——

Senator TESTER. I do not want to put you on the spot. You can just say you could take the Fifth, if you want. It does not matter.

[Laughter.]

Senator TESTER. OK.

Senator WARNER. Senator, it has been in the public at least from, I think, November 27th to December 15th, and then there was an announcement on December 19th.

Senator TESTER. I got that. My concern is this: there needs to be breach notification across the board so you can get to the bottom of it, because I think time is literally money in this situation. And if there is a breach that happens and that retailer withholds the information, or for some reason the banking institution may want to disclose information—I do not know why, but—I do not know why either one would want to, quite frankly. But you guys need to know about it immediately so you can start finding out where the bad guys are that did it if we are going to get to the bottom of it, right?

Mr. NOONAN. Yes, sir.

Senator TESTER. OK. Mr. Noonan, your testimony focused really on the retail industry as a point of entry for the criminals, and you highlighted investigations of a number of retail networks where cyber criminals were able to install programs to be able to capture information from retailers. And it has been already talked about by the Chairman. There were 40 million cards, 70 million personal—people with personal information that was given out. Could you tell me why a retailer would be storing sensitive payment information on their own networks?

Mr. NOONAN. I do not know if—I do not believe in this case information on the cards were actually being stored on the network.

Senator TESTER. So how did they get them, then? How did they get the information?

Mr. NOONAN. The information was being collected as the data was going through the process.

Senator TESTER. OK. I got you. So how did they get the 70 million?

Mr. NOONAN. It was a heavy period of collection time in which the data was being collected by the criminals.

Senator TESTER. OK. So the fact whether this was encrypted or not makes very little difference. I was under the assumption that this was on a database, the information was not encrypted. The folks that got into that database then encrypted the information and took it out.

Mr. NOONAN. There is more—I think you are getting this from the media perhaps. There is more to the investigation—

Senator TESTER. Of course.

Mr. NOONAN. Correct. Right.

[Laughter.]

Mr. NOONAN. Right, and again, this is an ongoing investigation. I cannot talk about the specifics of exactly how that was being done.

Senator TESTER. OK. Ms. Rich, I want to talk a little bit about the enforcement that you have. Right now, I mean seriously speaking, of all the things you have to deal with, do you have any tools to work with that really work?

Ms. RICH. We are doing a lot in this area. This is one of our areas of priority. We are bringing enforcement. We are doing education. We are using the bully pulpit——

Senator TESTER. I got you. I am not being critical of you. I am being critical of us.

Ms. RICH. Well, we do want more tools. We do want more tools.

Senator TESTER. Yeah, and when was the last time your tools dealing with this issue were dealt with from a policy standpoint? I am talking about has there been a revamp of your tools dealing with data breaches in the last 10, 15, 20, 50 years?

Ms. RICH. We have received some new authority in this area, including we do have a data breach law for a narrow class of health entities, PHRs, personal health records. But for the most part—and Gramm-Leach-Bliley was passed in 1999 or 2000. But it has been awhile.

Senator TESTER. OK. We obviously have some work to do, Mr. Chairman. Thank you.

Senator WARNER. You are ceding back 30 seconds?

Senator TESTER. Efficiency, baby.

[Laughter.]

Senator WARNER. Senator Menendez.

Senator MENENDEZ. Thank you, Mr. Chairman. I appreciate you holding this hearing. When these issues broke in December, Senator Schumer, myself, and yourself signed a letter to the Chairman of the full Committee asking for hearings, and I am glad that your Subcommittee is leading on this. And I understand the Chairman is going to broaden some of his call for hearings and include this topic. So this is extraordinarily important.

Ms. Rich, I have two particular lines that I want to pursue. I think Senator Warren opened the door to something that I think is incredibly important, which is: What role should the FTC and the Federal Government create in standards? It seems to me that whatever high standard exists in the marketplace readily available in technology is one that we would want to have companies follow in order to ensure the security of millions of Americans' private information, critical information to themselves, to their credit histories, to retailers, to banking institutions. And so if a company—if we set a standard that basically says look what is available in the marketplace, we cannot expect a company that gets hacked and was already using the highest standards available in the marketplace to be held responsible. But if, in fact, there was a standard that was available and that company or companies were not using that standard, then we have to question whether or not they made an investment decision not to go ahead and expend the resources for that higher standard.

So it seems to me that part of the question is—and I know that the private sector has largely worked on creating its own standards, but is there a role for the Federal Trade Commission and the Federal Government to set a standard that says, look, whatever is existing in the marketplace that, in fact, can be achieved to give the highest protection available should be the standard. And if you do not pursue that standard, then you are subject to consequences thereof?

Ms. RICH. Well, that is incredibly similar to the way we think about it now when we talk about having reasonable security. So reasonable security means you take into account, you know, what is—what the risks are in your business, what kind of—what the sensitivity of information you collect, how much information you collect, and the cost and availability of measures that are out there in the marketplace. So that is exactly how we analyze it. And the good——

Senator MENENDEZ. The question is: Does the industry understand that they are going to be held to those standards? Because I do not get the sense that there is an obligation per se to be held to that higher standard.

Ms. RICH. Well, one of the limitations we have in our work is we do not have civil penalties or the kind of sanctions that are needed to provide the right incentives to focus on this issue.

Senator MENENDEZ. But if we set a standard—I want to get to civil penalties in a moment, because I sent a letter to your Chairwoman, and she responded to me in that respect. If we set a standard that at least everybody has notice, here is what we expect of

you; if we do not set standard, then we have a more amorphous process of deciding what is the right standard or not. And, of course, we should have industry input into that standard. But it seems to me that we should be setting a standard, because if we set a standard, then we have notice, the essence of due process, notice and opportunity to be heard, and then we go away with a standard. So I would like to pursue with the agency whether or not such a standard is important, Mr. Chairman.

And, secondly, with reference to additional authorities, in my letter to Chairwoman Ramirez asking about the Commission's efforts in the past, I notice that there were never civil penalties, even though there were very large breaches—not as large as this one now, but large for their time. And it seems to me that she agreed that the authority to impose civil penalties would be a helpful tool to have in addition to current authorities like consumer restitution and disgorgement of ill-gotten gains.

I do not think that is something that you want to levy against every company. I think that goes back to the standard. If you have the standard and you are pursuing the standard, you should not be subject to penalty. If you have a standard and you are not pursing the standard, then civil penalties may be an option.

Do you agree with that line of thinking?

Ms. RICH. It is very important to have civil penalties as an available remedy to make sure there is both specific and general deterrence when there has been a failure.

Senator MENENDEZ. OK. And the reason, if I can, Mr. Chairman, finally, you know, your testimony reasserts the Federal Trade Commission's longstanding assertion borne out through case history that Section 5 of the FTC Act covers instances where a company fails to adequately protect consumer data. This assertion is based on the commonsense premise that customers have an understanding that companies will take reasonable steps to protect their data and failure to do so would be an unfair or deceptive practice. However, such companies as LabMD and Wyndham Worldwide have been challenging this assertion.

So I think that if that is the case, that now they are going to challenge that assertion, it seems to me to call for not just voluntary efforts but to create a standard and consequences of that standard that can give Americans the best security that they can hope for. And I look forward to working with the Committee and with the FTC in that regard.

Senator WARNER. Thank you, Senator.

One last comment. I know we probably all have other questions, but we have got a second panel, unless anybody wants to make one comment. Then if anybody has got a burning, burning question, we will go to the second panel. Just, you know, one—following up on Senator Tester's comments, you know, trying to get the notion of your obligation to disclose when you have been breached, I think sorting that through is going to be a challenge, because there are so many attacks every day, and we have got to set a standard somewhere that you cross a threshold, so you do not want to—what I get concerned about is that you do not want to create the old—remember the Homeland Security color code system, which every-

body proceeded to ignore. There has got to be a materiality piece in here somewhere.

Senator TESTER. I agree with you. On the other hand, if a business withholds that information because it is in the heart of Christmas shopping season——

Senator WARNER. Amen.

Senator TESTER.——and it might affect their bottom line——

Senator WARNER. Amen.

Senator TESTER.——they need to be hung out to dry.

Senator WARNER. Amen. Well, the other point, too, following up on Senator Menendez, an earlier point you made to Senator Warren I thought was an interesting one, where companies in the past have, in effect, put a seal or put some kind of Good Housekeeping Seal of Approval that may or may not be valid really troubles me greatly. But I thank both the witnesses, and we will move to the second panel. Thank you both.

[Pause.]

Senator WARNER. If the panel does not mind, I am going to go ahead and start introducing you even as you are in the process of being seated. I am going to start introducing you once my staff gives me your introductions.

Gentlemen, thank you. The first panel was focused on our governmental witnesses. Now we are going to focus more on industry and consumers.

Mr. James Reuter?

Mr. REUTER. Reuter.

Senator WARNER. Reuter, sorry. I should know that, like the news agency. He is Executive Vice President of FirstBank, located in Lakewood, Colorado, where he has been since 1987. He is also President of First Data Corps, which provides all IT and operational support services for more than 110 locations. Welcome, Mr. Reuter.

Mr. Mallory Duncan is Executive Vice President and General Counsel of the National Retail Federation where he is responsible for coordinating strategic, legislative, and regulatory issues involving customer data privacy, bankruptcy, fair credit reporting, truth in lending. He previously worked for J.C. Penney and for the FTC.

Mr. Troy Leach is the Chief—excuse me. Why don't we do Mr. Mierzwinski? Mr. Ed Mierzwinski is the Federal Consumer Program Director and Senior fellow for the U.S. PIRG, Public Interest Research Groups. He has worked in the Federal offices of U.S. PIRG since 1989 and is recognized as an expert in the wide area of consumer issues with an emphasis on financial services, banking, credit cards, credit reports, privacy, and identity theft. Thank you, sir.

And Mr. Troy Leach is the Chief Technology Officer for the PCI Security Standards Council. This is the industry council that is setting the standards right now. In his role, Mr. Leach partners with industry leaders to develop comprehensive standards and strategies to secure payment, credit card data, supporting information. He has a long history in the private sector working on IT issues.

Gentlemen, thank you all very much. You have got a panel that is anxious to ask you questions, so, Mr. Reuter, why don't you start? Then we will just go down the line and get to questions.

STATEMENT OF JAMES A. REUTER, EXECUTIVE VICE PRESIDENT, FIRSTBANK, ON BEHALF OF THE AMERICAN BANKERS ASSOCIATION

Mr. REUTER. Chairman Warner, Ranking Member Kirk, and Members of the Subcommittee, my name is James Reuter, President of Support Services at FirstBank in Lakewood, Colorado. We are a $13 billion institution with over 115 locations and 2,000 employees serving Colorado, Arizona, and California. My operation provides information technology, payment processing services, a 24-hour call center, and electronic banking services for 115 FirstBank locations. I appreciate the opportunity to be here to represent the ABA.

Even with the recent breaches, our payments system remains strong and continues to support the $3 trillion that Americans spend safely and securely each year with their credit and debit cards, and with good reason: Customers can use these cards confidently because their banks protect them by investing in technology to detect and prevent fraud, reissuing cards and absorbing fraud costs.

At the same time, these breaches have reignited the long-running debate over consumer data security policy. The banking industry recognizes the importance of a safe and secure payments system to our Nation and its citizens. We thank the Subcommittee for holding this hearing and welcome the ongoing discussion.

Let me be clear. Protecting customers is the banking industry's first priority. As the stewards of the direct customer relationship, the banking industry's overarching priority in breaches like that of Target's is to protect consumers and make them whole from any loss due to fraud. When a retailer like Target speaks of its customers having "zero liability" from fraudulent transactions, it is because our Nation's banks are making customers whole, not the retailer that suffered the breach. Banks swiftly research and reimburse customers for unauthorized transactions and normally exceed legal requirements by making customers whole within days of the customer alerting them.

Beyond reimbursing customers for fraudulent purchases, banks often must reissue cards to affected customers. For our bank, this cost is $5 per card. In the end, banks receive pennies on the dollar for fraud losses and other costs incurred while protecting their customers. In fact, banks bear over 60 percent of reported fraud losses, yet have accounted for less than 8 percent of reported breaches since 2005.

More needs to be done to stop this kind of fraud in its tracks. Having a national data breach standard is an important step in this direction.

In many instances, the identity of the retailer that suffered the breach is either not known or oftentimes intentionally not revealed by the source. Understandably, a retailer or other entity would rather pass the burden on to the affected consumers' banks rather than taking the reputational hit themselves. In such cases, the bank is put in the position of notifying their customers that their credit or debit card data is at risk without being able to divulge where the breach actually occurred. Often customers, absent better

information, blame the bank for the breach itself and any inconvenience they are now suffering.

Consumers' electronic payments are not confined by borders between States. As such, a national standard for data security and breach notification, as contained in Senate bill 1927, the Data Security Act of 2014, is of paramount importance. It is critical that all players in the payments system, including retailers, must improve their internal security systems as the criminal threat continues to evolve.

Criminal elements are growing increasingly sophisticated in their efforts to breach the payments system. This disturbing evolution, as demonstrated by the Target breach, will require enhanced attention, resources, and diligence on the part of all payments system participants.

Let me make one final point. Protecting the payments system is a shared responsibility. Banks, retailers, processors, and all participants in the payments system must share the responsibility of keeping the system secure. That responsibility should not fall predominantly on the financial services sector. Banks are committed to doing our share, but cannot be the sole bearer of that responsibility.

Policymakers, card networks, and all industry participants have a vital role to play in addressing the regulatory gaps that exist in our payments system, and we stand ready to assist in that effort.

Thank you, and I would be happy to answer any questions you might have.

Senator WARREN. [Presiding.] Mr. Duncan, please.

STATEMENT OF MALLORY DUNCAN, GENERAL COUNSEL AND SENIOR VICE PRESIDENT, NATIONAL RETAIL FEDERATION

Mr. DUNCAN. Thank you, Senator Warren, Ranking Member Kirk, Members of the Subcommittee. Collectively, retailers spend billions of dollars safeguarding consumers' data and fighting fraud. Most of the U.S. data breaches we have seen—whether at retailers you have heard about or at banks and card companies, about which you have heard less—have been perpetrated by criminals. The companies are victims. We need to reduce fraud; that is, we should not be satisfied with deciding what to do after a data breach occurs—who to notify and how to assign liability. Instead, it is important to look at why such breaches occur and what the perpetrators get out of them so that we can find ways to reduce and prevent not only the breaches but the fraudulent activity that is often their goal.

In its comprehensive 2013 data breach report, Verizon revealed that 37 percent of breaches happened at financial institutions, 24 percent at retail, and the remainder at others. It may be surprising to some given recent media coverage that more data breaches occur at financial institutions than at retailers, but that thieves focus on banks because they have the most sensitive financial information. Still, fraud is devastating for retailers in the United States, and it is rising.

In 2012, the United States accounted for nearly 30 percent of credit and debit card charges but 47 percent of all fraud losses. Who bears this cost? Independent studies vary. They say retailers

bear anywhere from 90 percent to 40 percent of the payment card fraud costs. We think a fair assessment is that retailers pay about half.

Why is card fraud increasing? Thieves go where the rewards are plentiful and easiest to obtain. Unfortunately, our card payment system is outdated and rife with opportunities for fraud.

Despite the billions of dollars spent by merchants in hopes of becoming PCI compliant, we still must accept fraud-prone cards that are so attractive to data thieves. Unlike the rest of the world, U.S. cards still use a signature and magnetic stripe for authentication. The fraudsters rely on our system being so porous.

What the card companies effectively say to merchants is that even though this sensitive information is visibly printed on the card, even though security information can be lifted off a magstripe by a reasonably sophisticated 12-year-old, and even though signatures are a virtually worthless form of authentication, it is your responsibility to guard that information at all costs. Retailers work very hard to do it, but the request does not really make sense.

What is needed is for the networks and banks to issue cards that are not so easily compromised. At a minimum, we need to replace the signature with a PIN and the magstripe with a chip. Even that will not be state-of-the-art. After all, it is technology that is three-quarters of a generation old. But fraud dropped 70 percent when it was adopted in Britain, and fraud is growing here because we have not. We must adopt both PIN and chip. The PIN authenticates the card holder and, thus, helps protect her and the merchant. The chip authenticates the card to her bank. Together they greatly reduce fraud.

The banks know this combination is very powerful. They promote it all over the world. Yet here in the United States they are proposing signature and chip cards, "chip and choice," as one of them cutely calls it. It is an ineffective half measure, the locking of the back door while leaving the front door open. Why adopt a halfway measure? Merchants would still need to spend billions to install new equipment to read cards that would combine 1990s technology—chip—with 1960s relic—signature—in the face of 21st century threats. Frankly, if Congress is seriously concerned about protecting our payment card system against fraud, it ought to do oversight of any group that is seriously advancing this absurd solution.

There are additional changes to the system that would be helpful and provide greater security. Point-to-point encryption of data is one, but it relies on banks and networks being able to accept encrypted data, and that has been a challenge.

Chips are more advanced than magstripes, but their sophistication pales in comparison with a smartphone. Today smartphones are mini-computers. They could enable state-of-the-art fraud protection, and if payment platforms are open and competitive, they will only get better.

As to legislative solutions, we lay out a number of proposals in our written testimony. It is important, however, that the Federal law should ensure that all entities handling the same type of sensitive consumer information, such as payment card data, are subject to the same statutory rules and penalties with respect to notifying consumers of a breach affecting that information.

In closing, three brief points are uppermost:

First, retailers take the increasing incidence of payment card fraud very seriously. Merchants already bear at least an equal, or often a greater, cost of fraud than any other participant in the payment card system. We did not design the system; we do not configure the cards; we do not issue the cards. We will work to effectively upgrade the system, but we cannot do it alone.

Second, the vast majority of breaches are criminal activity. No system is invulnerable to the most sophisticated and dedicated of thieves. Consequently, eliminating all fraud is likely to remain an aspiration. Nevertheless, we will do our part to achieve that goal.

And, last, it is long past time for the United States to adopt PIN and chip card technology. If the goal is to secure data and reduce fraud, we must, at a minimum, do both.

Thank you.

Senator WARNER. [Presiding.] Mr. Mierzwinski.

STATEMENT OF EDMUND MIERZWINSKI, CONSUMER PROGRAM DIRECTOR, U.S. PIRG

Mr. MIERZWINSKI. Thank you, Chairman Warner, Senator Kirk, Members of the Committee. I am Ed Mierzwinski. I am a consumer advocate, and I have been working on these issues for some time. And my views I think are somewhat in line with the merchants, but also somewhat not in line with the merchants.

First, the Target breach itself, I want to make one point about that. The breach occurred with information that allows fraud to take place on your existing accounts in the first 40 million consumers who were breached. The additional 70 million, the information that was collected allows phishing attacks to try to obtain more information to commit identity theft. But I think the biggest risk to customers of Target is fraud on existing accounts. So the provision of credit monitoring, which they are giving for free but is normally an overpriced, junky product, really creates a false sense of security. It will not stop fraud on your existing accounts, and it will not stop identity theft. It will simply tell you when your Experian account has changed. It could be because of identity theft, or it could be because of something else. But it will be after the fact. But that is one point I wanted to make about the Target breach.

The thing about Target, again, is that they are not at fault completely. They are maybe in violation—and I have seen different stories on whether they were or they were not in violation—of the current highest PCI standards. We will know that more after they have testified in the next few days. But whether or not they were in violation of the PCI standards, those standards are cobbled on to an obsolete technological platform. It is like they are trying to put disc brakes on a Model T, airbags on an Edsel. I mean, the merchants are being asked constantly to add different bells and whistles to an obsolete system from the mid-20th century. So that is a problem. I think the banks and the card industry have a lot to answer to with these problems.

I want to make a couple of quick points that are all made in my testimony.

First, I was encouraged, Chairman Warner, when you mentioned that debit card protections maybe should be increased. We strongly support that idea. All plastic should be equal. The zero liability promise the banks make is just a promise. It is not the law. I only use credit cards. I never use debit cards. The other problem, of course, with a debit card is you lose money from your account. Until they complete the reinvestigation, you could have other checks bounce.

Second, any reforms should be technology neutral and technology forcing. You really should have a reform that encourages continuous increasing in the uses of better and better technology. And as Mr. Duncan pointed out, it should be on an open platform, and competitors should be allowed to come in. I think today if you look at the networks, the two big ones are a duopoly. They have all the standard characteristics of a duopoly. They seek excess rents. They do not like new technology. They do not like competitors. And that has really been a problem.

I think you should look at the PCI standard-setting body. Do the merchants have adequate input into it? Do the prudential regulators or the FTC have enough review of it? You should not enact any new legislation that preempts State laws. If Congress enacts a good enough law, it does not have to preempt State laws. The States will move on. They will do other things. But if Congress does not enact a good enough law, you need the States as first responders, and my testimony goes into detail. After 2003, when the FACT Act amendments to the Fair Credit Reporting Act did not include adequate identity theft reforms, 46 States passed breach laws; 49 States gave consumers the right to freeze their credit report. And so those were important things that the States did. Whereas, every bill that I have seen to some extent not only preempts any breach law, which is their nominal purpose, but goes further and preempts any right of the States to do anything in the future. And that is really, I think, the wrong way to go.

Another point that we make in our testimony is that if you do enact a breach law, it should be on an acquisition standard. There should not be a harm trigger. The company that did not protect my information should not be allowed to decide whether or not to give me notice.

One point that I do not make in my testimony but I have made in previous testimony before the Commerce Committee is that I strongly support any effort to increase the FTC's authorities, including the right to impose civil penalties for a first violation.

Thank you for the opportunity. I hope to answer any questions you might have.

Senator WARNER. Mr. Leach.

STATEMENT OF TROY LEACH, CHIEF TECHNOLOGY OFFICER, PCI SECURITY STANDARDS COUNCIL

Mr. LEACH. Thank you. My name is Troy Leach. I am the CTO of the PCI Security Standards Council, a global industry initiative focused on securing payment card data. Our approach to an effective security program is people, process, and technology as key parts of data protection.

Our community of over 1,000 of the world's leading businesses tackles security challenges from simple issues—for example, the word "password" still one of the most commonly used passwords—to really complicated issues, such as proper encryption. We understand consumers are upset when their payment card data is put at risk and the harm that is caused by these breaches.

The council was created as a forum for all stakeholders—banks, merchants, manufacturers, and others—to proactively protect consumers' card hold data. Our standards focus on removing card holder data if it is no longer needed. Our mantra is simple: If you do not need it, do not store it. If it is needed, then protect it through a multilayered approach and devalue it through innovative technologies that reduce the incentive for criminals to steal it.

Let me tell you how we do that. The data security standard is built on 12 principles, everything from strong access control, monitoring and testing networks, annual risk assessments, and much more. This standard is updated regularly through feedback from our global community. In addition, we have developed other standards that cover payment software, point-of-sale devices, and the secure manufacturing of cards. And we do much more as well. We develop standards and guidance on emerging technologies like tokenization and point-to-point encryption that remove the amount of card data kept in systems, rendering it useless to cyber criminals. Tokenization and point-to-point encryption work in concert with other PCI standards to offer additional protections.

Now, another technology, EMV chip, has widespread use in Europe and other markets. It is an extremely effective method of reducing card fraud in face-to-face environments. That is why the PCI Council supports the deployment of chip technology.

However, EMV chip is only one piece of the puzzle. Additional controls are needed to protect the integrity of payments online, on the telephone, and in other channels. These controls include encryption, proper access, response from tampering, malware protection, and more. These are all addressed within the PCI standards. Used together, EMV chip and PCI standards can provide strong protections for payment card data.

But effective security requires more than just standards and technology. Without ongoing adherence and supporting programs, these are only tools and not solutions. The council makes it easy for businesses to choose products that have been lab tested and certified as secure. The council's certification and training programs have educated tens of thousands of individuals, including assessors, merchants, technology companies, and government. Finally, we conduct global campaigns to raise awareness of payment card security.

The council welcomes the Committee's attention to this critical issue. The recent compromises underscore the importance of a multilayered approach, and there are clear ways in which the Government can help, for example, by leading strong law enforcement efforts worldwide, particularly because of the global nature of this threat, and by encouraging stiff penalties for these crimes. Promoting information sharing between the public and private sector also merits your attention.

The council is an active collaborate with Government. We work with NIST, DHS, and many other Government entities, and we are ready and willing to do more.

We believe the development of standards to protect payment card data is something that the private sector and PCI specifically is uniquely qualified to do. But global reach, expertise, and flexibility of PCI have made it an extremely effective mechanism for protecting consumers.

Now, the recent breaches underscore the complex nature of payment card security. A multifaceted problem cannot be solved by a single technology, standard, mandate, or regulation. It cannot be solved by a single sector of society. Business, standards bodies, policymakers, and law enforcement must work together to protect the privacy interests of consumers. Today, as this Committee focuses on recent data breaches, we know that criminals are focused on inventing the next attack.

There is no time to waste. The PCI Council and business must continue to provide multilayered security protections while Congress leads efforts to combat global cyber crimes that threaten us all. We thank the Committee for taking a leadership role in seeking solutions to one of the largest security concerns of our time.

Senator WARNER. Thank you all, gentlemen.

I made this comment in my opening statement, but I would like to make it again with you all sitting in front of me. It is my strong hope that as we approach this issue, we recognize, rather than pointing blame at each other, the only way this is going to work to protect consumers and give them the confidence they need is for the banking industry, the retail industry, the card and the industry at large to actually collaborate together. We do not need, I do not believe, another replay of a multiyear legislative battle here when the hackers are not going to take a timeout and American consumers are going to be increasingly at risk.

Mr. Leach, in the spirit of your comments, we are going to do a lightning round here, so I would ask you to keep your comments as close to yes or no as possible, recognizing, of course, that there is not a single technology solution but seeing a dramatic decrease in Europe in terms of fraud at face-to-face transactions when they moved to the chip-and-PIN system. What do each of you think in terms of our country moving to the chip and PIN as one step forward?

Mr. REUTER. We have embraced the chip technology. In fact, the card networks have laid out a timeline that involves a pretty strong incentive for the industry by October 2015 to move there. And so as——

Senator WARNER. Let us get to everybody else. Mr. Duncan?

Mr. DUNCAN. Mr. Chairman, I take to heart your comments about not pointing fingers at each group. As I said in my testimony, if we are actually to have effective protection, it has got to be, as you said, PIN and chip. If you listen to the response that was just given, it only mentioned the chip. And as I said, that is closing the back door and leaving the front door open.

Senator WARNER. So it sounds to me you are saying yes to full chip and PIN.

Mr. DUNCAN. Yes.

Mr. MIERZWINSKI. Yes, absolutely to full chip and PIN, not chip and signature, but do not leave that as the ceiling. Make sure that you can go more.

Senator WARNER. Mr. Leach?

Mr. LEACH. We are supportive of chip technology as well, but keep in mind that information——

Senator WARNER. As I learn this, I might want to make sure I am getting it right. Chip is different than chip and PIN. Are you supportive of chip and PIN?

Mr. LEACH. We are supportive of chip and PIN. Any type of authentication added on to chip technology is an important form of authentication. It is important to keep in mind, though——

Senator WARNER. OK. I got it, and I think that is great progress today, everybody agreeing. I would concur with Mr. Mierzwinski that—and I thought I was a relatively informed consumer. I did not realize my debit card did not have the same protections. And, you know, I think again about the fact that where the growth of debit cards is coming is younger folks and the underbanked community, who potentially are the most vulnerable if they do not have these protections. It would seem to me that equalizing cards on a same standard makes common sense. Give me a reason why not. Anyone?

Mr. REUTER. As a practical matter, we invoke a zero liability policy, so we today, if a transaction—if you did not authorize it, you are not responsible for it.

Senator WARNER. I do not want to get you in trouble with the ABA, but is that an endorsement of equalization in the truth in lending—truth in reporting——

Mr. REUTER. I believe that from a legislation perspective, the way we are all performing as banks, I am not sure additional legislation is needed, because we are adhering to a zero liability policy as a matter of our business practice.

Senator WARNER. Would there be no practical reason why you would not want to have the same standard between different types of plastic?

Mr. REUTER. There would be no practical reason.

Senator WARNER. Mr. Duncan?

Mr. DUNCAN. We believe it is a good idea.

Senator WARNER. Mr. Leach? And you get the last word.

Mr. LEACH. And just to follow up on the point, I just want to emphasize that chip technology is in the clear, so we still need additional security protections to that. We are supportive as well.

Mr. MIERZWINSKI. I would just add, Senator, that the issue here is that the zero liability may not occur in all circumstances. It may only apply to signature transactions, not to PIN-based transactions. That is the question, debit or credit, which confuses consumers at the store. Debit means using a PIN. Credit means it is still a debit card but you are using it on the signature-based credit card network. And, also, I would look at the zero liability contract and say what if I had two violations in a year, do they honor the second one? Because some banks do not.

Senator WARNER. Let me level down. I am interested and I would like to hear more. I guess the last point I want to make—I am not sure I am going to get a question out, but we have focused on the

challenges around the cards. I would make the comment, though, that the cards actually do add an extra layer of protection because of some of the network, because of even the technologies that may not be fully up to snuff at this point, versus what may be our real Achilles heel, which is everybody's movement toward online financial transactions. I think about the fact of how many of us pay our utility bills or I pay college tuition online. In a certain sense, that is, if people can get into that personal data information, that is something that is there are no limits on in terms of an individual's exposure. We are much more, I believe, vulnerable. And, again, my time has expired, but I would simply say chip and PIN, good step forward; equalization of cards, good step forward; but continuing, again, the notion that Mr. Leach said, recognizing tokenization and other abilities that are online transactions, trying to put a level of protection is something that I think needs a lot more study and work.

Senator Kirk?

Senator KIRK. Let me just follow up with Mallory. I agree with you that Parliament has done a much better job than Congress moving to chip and PIN. I was struck by your comment that fraud was reduced in the U.K. by 70 percent by using chip and PIN. For those of us who have lots of friends in the U.K., you will see them pull out a credit or debit card with a chip in it and disparage the technological backwardness of the United States.

Can I just ask you on behalf of the Retail Federation, how much would it cost your members to move to a full U.K.-based chip and PIN?

Mr. DUNCAN. Senator, we would have to replace all of the card readers in the store. There are approximately 3.5 million retailers in the United States. Many of them are just a one-store location, one checkout place; others have a dozen on each floor. So if you multiply that times approximately an average of 1,000 or more per unit, you are talking several billions of dollars in order to replace those, and, of course, some amount of time.

Senator KIRK. And, in general, I took from your testimony that the Retail Federation would support making that move.

Mr. DUNCAN. We absolutely would. In fact, some retailers have already begun to install chip-and-PIN readers in their facilities in hopes that the banks will do the right thing.

Senator KIRK. Mallory, let us identify the heroes. Who was the first who did that?

Mr. DUNCAN. I cannot tell you who the first was, but they tend to be the larger retailers who experience more international clients, so like a Home Depot, for example, or maybe a Best Buy.

Senator KIRK. Thank you.

Senator WARNER. Thank you. I am very supportive of moving toward chip and PIN. I would only point out, as I dug into the data on the U.K., when we saw chip and PIN and face-to-face transaction fraud drop dramatically, it was like squeezing a balloon, and you saw online fraud in the U.K. shoot up, I think something like 30 percent.

Senator Warren?

Senator WARREN. Thank you, Mr. Chairman.

So I will just pick up on the same point about chip and PIN. We understand why chip and PIN works better, and it seems that we are years behind Europe in developing adequate technology, technology we know is out there, but applying adequate technology here in the United States.

So I was interested in your testimony, Mr. Leach. You said that you think that standards are best left to private organizations such as yours. That is what we have done, and we are now way behind in technology and have become the targets for data attacks from around the world. So why should we leave this to organizations like yours?

Mr. LEACH. Well, Senator, it is a very fair question to ask. I think for us we look at standards being people, process, and technology, and recognize that while we have not migrated to chip, we have advanced fraud monitoring tools in the United States, the best in the world, as well as looking at other technologies that are more cost-effective for merchants to move to, like tokenization and point-to-point encryption.

Senator WARREN. I am sorry, Mr. Leach. Let me just make sure I am following you here. I thought I had heard in this conversation that we were uniform in our agreement that the way we should go now is to chip and PIN. And you are telling me we have other things we can do, which I am not disagreeing with, but I am asking the question: Why have we not hit the basic chip-and-PIN standard?

Mr. LEACH. Well, I think, Senator, that question is probably not for a standards body like myself. My role and our role is to actually develop secure standards for what we have today.

Senator WARREN. Well, fair enough, but your testimony was not just we have great standards if someone wants to adopt them. Your testimony, as I understood it, was that the standards should be left to private organizations and not to Government to say you have got to meet the standards put out by other organizations or developed in other ways. And so that is the point I am pushing on. It sounds like to me we may need some pressure from the Government to make sure that the toughest standards are used.

Maybe I could ask the question of Mr. Reuter. Why has chip and PIN not been adopted already in the United States?

Mr. REUTER. Well, I would like to comment on why the rest of the world is ahead of us on chip. The United States has a very robust telecommunications system. Years ago, in other parts of the world, they did not have as robust of a telecommunications system, so as a result, they deployed chip technology to solve that problem. It was not driven by fraud measures. Today, as we have seen more breaches at retailers and different things, we are embracing the chip technology here in the United States.

The reason I keep leaving out PIN is one of my concerns with PIN data is it is a static piece of information. The chip brings the dynamic data to the transaction, which is really what renders the compromised data useless. The PIN is a static element, so I would—I appreciate and support the ongoing debate on chip and signature—but I would hate to delay the deployment of chip technology on this one issue because it has the biggest impact on fraud.

Senator WARREN. Well, let me actually hit both parts of your question to make sure that I fully understand your point. I understand that Europe had reasons to go to chip early on, but are you saying that the banks have just now discovered that chip and PIN would be a more secure system? Or have they had some reason to know that for many, many years now?

Mr. REUTER. You know, we have been working toward putting chip technology in. The card networks laid out the timeline we are working toward in 2011. There are 8 million retailers, 14,000 financial institutions——

Senator WARREN. So was it only in 2011 that the banks figured out that chip and PIN would be a more secure system?

Mr. REUTER. No, there were conversations before that, but that is when the actual timeline was laid out.

Senator WARREN. All right. But the Europeans have done more to protect themselves than we have. Now, as to the question about chip and PIN, why don't I just invite Mr. Duncan to weigh in on that issue about whether or not chip and signature would be a better approach.

Mr. DUNCAN. Well, signature is worthless. I mean, your signature is on the back of your card right now. If you lose it and a thief finds it, there is an exemplar there for them to copy your signature. It is essentially worthless. If you are going to have security, you have to have PIN.

As for the idea that they are slightly different systems and, therefore, we should not use both, imagine putting up a burglar alarm system in your house. You have one sort of protection for the doors when they open and a second sort of protection for the windows. Why would you say, "Well, this one works differently so I am not going to alarm the windows"? If you want security, you have got to have the whole system. It has got to be PIN and chip. And I am just flummoxed as to why anyone thinks otherwise.

Senator WARREN. Thank you.

It sounds like to me, Mr. Chairman, that the banks have delayed, the retailers have delayed, the Government has delayed, and the ones who have paid the price are the consumers whose data are being stolen.

Senator WARNER. Senator Tester.

Senator TESTER. Thank you, Mr. Chairman. I am getting conflicting data here. I have got a bank that employs some of my constituents in Montana that had 7 percent of their debit cards—now, we are not talking credit, just debit—7 percent of their debit cards that were impacted by the recent breach. That was only 12,000 cards. In their particular case, it cost them about 5 bucks a card, $60,000, to replace them. That was just to replace the cards. It did not include any additional costs bearing the cost of monitoring fraud.

When this breach happened, I actually got a call from the credit union that is located in the Hart Building—the credit union that is located in the Hart Building, where we have an account—and it said, "Your account has been breached. We think it would be wise if you issued a new credit card." We were very appreciative of that, and they did. And so I actually visited with somebody from the credit union who said it cost about 30 million bucks, this recent

breach on them. And that does not include any of the fees that were back there, because I asked the credit union, I said, "If this card is used somewhere else by somebody else and they ring up a charge, am I going to have to pay for it?" And they said no, they would take care of it.

So the question is, and this is for you, Mr. Reuter: In this particular case, what do you think the prospects are for a particular bank or credit union in this case will actually get reimbursed for fraud costs?

Mr. REUTER. You know, our bank, we reissued almost 65,000 cards, and that came as a result of us learning more about the breach, but also customer demand. Our call center, we took an extra 30,000 calls over a 3-week period. So the bottom line is we have already invested quite a bit, and at the end, when all the dust settles, we will get, at the most, pennies on the dollar.

Senator TESTER. Now, Target has said that they are going to make sure that—let me see if I can get the right quote here. They are going to make sure that customers are made whole and have zero liability. Who is going to pay the bill? Is it going to be Target, or is it going to be the banks?

Mr. REUTER. We as banks shoulder that responsibility. We are the ones reimbursing——

Senator TESTER. Does Target reimburse you then?

Mr. REUTER. No, they do not.

Senator TESTER. What has been your experience on you recovering fraud costs in other breaches, like the TJX case?

Mr. REUTER. My experience has been we recover very little.

Senator TESTER. Pennies on the dollar again?

Mr. REUTER. Pennies on the dollar.

Senator TESTER. OK. Let us talk about the cards here for a second again. I mean, look, I love to pay in cash. I would even rather pay in checks, but that is not the way it works a lot of times. And so I end up using my credit card a lot. I am like Mr. Mierzwinski—and sorry about the pronunciation of the last name. I use credit cards almost exclusively myself.

If merchants—and this is for you, Mr. Duncan. If they are concerned about fraud, and I think they are concerned about fraud, what is preventing them from doing more identity checks when you go to the checkout line? I have got to tell you, they do not even ask to look at my signature anymore. They do not ask for a credit card. They do not ask for anything. They just take the credit card, they swipe it. And sometimes they do not even take the credit card and swipe it. They say, "You swipe it."

So what are the merchants doing to help prove identity at point of sale?

Mr. DUNCAN. Well, one thing we would like to do is to have a PIN authentication. That would be one thing——

Senator TESTER. OK, but we do not.

Mr. DUNCAN.——that would help. Number two——

Senator TESTER. Just a second. We do not right now. OK? I think we can all agree there, here, we would like to go that way.

Mr. DUNCAN. Right.

Senator TESTER. We had a breach. You guys, everybody at the table said they were concerned about it. Everybody up here is con-

cerned about it. If the retailers are concerned about it, what are they doing to help stop the breach now?

Mr. DUNCAN. Well, as I mentioned in my testimony, we have put—there is a lot in your question. I mentioned in my testimony we have spent billions hardening the system so that the bad guys cannot get in and pull out information.

Senator TESTER. OK.

Mr. DUNCAN. We encrypt the information. In terms of signature at the checkout, the card associations have told us that we are not allowed to ask for information along with that.

Senator TESTER. Oh, really?

Mr. DUNCAN. It is considered—I guess they consider it a hassle of the consumer if we ask for additional identification. Some merchants do it anyway.

Senator TESTER. Yes. Well, they used to do it all the time.

Mr. DUNCAN. Well, unfortunately we are told we are not allowed to do it.

Senator TESTER. That is interesting. I want to talk about the cost with the chip and PIN. Mr. Duncan, you had said $3 billion it would cost the merchants. There are a lot of small merchant folks out there that—I mean, that is probably quite a bit per machine. Who would pay the $3 billion? Is that going to be picked up by the retail association? And does that have any impact on your support for chip and PIN?

Mr. DUNCAN. We would have to pay for that equipment, so it would come out of the retailers' bottom line. We would do it to improve security. And I should clarify my statement. What they have told us is that we may not reject a transaction based on the signature. So looking at a driver's license, the signature does not match, you still cannot reject the transaction. So to be precise, that is what they have told us.

Senator TESTER. OK. That would be interesting to flesh that out some more, too, because that does not sound particularly good to me. But you cannot ask for an opportunity to compare signatures. I think that is where the key is in a card if I lose mine and you pick it up and use it, they are going to know—well, they are probably going to know it is not Jon Tester.

Mr. DUNCAN. But if it is feminine handwriting, they would still have to accept the transaction.

Senator TESTER. I got you. Well, thank you, Mr.——

Senator WARREN. You have not seen his handwriting.

Senator TESTER. Yes, exactly. It is pretty bad. It used to be worse when I was left-handed. Anyway, thank you very much, Mr. Chairman.

Senator WARNER. Before I move to Senator Menendez, just two quick points. One, you mentioned credit unions. We have got lots of interest. We have got testimony from credit unions, independent banks, other organizations who have submitted for the record. And I would also just point out to Senator Tester, you know, that second security check at the checkout, though, think about how many transactions are going where you are automated now.

Senator TESTER. That is what I was talking about.

Senator WARNER. We have got to get a technology—I am not sure that human interaction piece is going to be——

Senator TESTER. Right. I mean, that is what I said. A lot of times they do not even take the card. They just say, "You swipe it."

Senator WARNER. Or you go to the grocery store and you check out without a person.

Senator TESTER. That is true. We do not have a lot of those grocery stores.

Senator WARNER. I am not going to ask you the price of milk.

Senator Menendez?

Senator MENENDEZ. Thank you, Mr. Chairman.

You have had a big discussion here on chip-and-PIN technology, which has been around more than a decade. It is widely used in Western Europe and other areas outside the United States. So I see that several of you in your testimony caution against adopting a similar standard by law that would lock in any specific technology. However, even if we do not adopt a Federal legal standard that favors one technology over another, couldn't we still have a standard based on performance? In other words, at what point should it be considered an unreasonable security risk for a company not to be using chip-and-PIN technology or something that performs equivalently? Mr. Mierzwinski?

Mr. MIERZWINSKI. Well, Senator, I think my testimony, we definitely say we should not adopt a specific standard, but I certainly think, from what I understand—and I am not the world's biggest expert on the tech—that chip and PIN is a higher standard than chip and signature. So if you have a technology-forcing standard, a performance standard, that chip and PIN meets, I think that is a good way to go as long as it is an open standard that encourages more and better technology to come forward.

Senator MENENDEZ. What about the banks and the retailers?

Mr. REUTER. You know, setting a specific technology standard I would agree is not a good idea because of how quickly the fraudsters keep changing and adapting. But as far as setting standards that we all do the best we can with the technology available, I think that that is fine.

Mr. DUNCAN. We would like our partners in this to do the right thing and to adopt PIN-and-chip technology. However, as I mentioned earlier, a number of retailers are already beginning to explore mobile as a possibility, and we want to be careful that Congress would not do something that might slow down that transition to even more secure systems in the future.

Senator MENENDEZ. Yes, well, that is why I am saying not supporting a specific standard. I get the sense everybody is worried about what Congress will do. We are worried about what you all will do. I sit here and listen to the banks say retailers should have more liability. I sit here and listen to the retailers say banks should have more liability. In the interim, the only entity that potentially is getting screwed with all of their financial data and security is consumers. So we have to have a different paradigm as to how we get here. And so it seems to me, as I was posing the questions to the Federal Trade Commission representative before, that creating some type of standard that does not necessarily lock you into a technology that may be in time, you know, a dinosaur but does ultimately create a standard of responsibility is important for both the banks and the retailers at the end of the day.

Now, I know that the industry, the card industry, likes setting its own standards. I understand why. But at some point there is a responsibility here to the consumers and to the economy, because it is not good for retailers, it is not good for banks when we have data breaches at the end of the day. And it is not good for the card companies in terms of the confidence in people who put it on their credit card.

So I would like to hear from Mr. Mierzwinski, you ask in your testimony whether Federal regulators should have a greater role in setting security standards. And, Mr. Reuter, in your testimony you raise the question of whether we should have a national standard that applies by force of law versus simply by the force of contract to all parties in the chain of possession of consumer financial and payments data. Isn't that really part of the goal here so that we can have a standard that then can be applied and that ultimately we can make judgments? Look, if you met that standard and there is a data breach, there is nothing more you could do. I mean, you know, you did all the things that you could. But if you do not have a standard, we never know what is the right engagement by both the banks and the retailers in protection of consumers.

Mr. MIERZWINSKI. Well, Senator, I understand that you are conducting an ongoing series of hearings. On Thursday the regulators are coming in, and I think it is useful to ask them, Should there be a Federal performance standard, as you point out, a Federal performance standard that is enforceable by the regulators? Should the regulators have the authority to look at—and maybe they do already, and maybe they are already doing something here, but they have not told me about it. Shouldn't they have the authority to determine whether any industry standards body, any voluntary industry standards body is performing adequately to protect the safety and soundness of the financial system? So, yes, I agree.

Senator MENENDEZ. Yes, Mr. Reuter?

Mr. REUTER. Senator, we as a banking institution already have to comply with a number of data security standards in the Gramm-Leach-Bliley Act. It is not only something that is written and we have instant response, but we are examined on it on a regular basis. So as an industry, that is why we are not opposed to setting standards. We are already obligated to follow standards today.

Senator MENENDEZ. And that may be different than what the Federal Trade Commission might determine would be the standard more broadly, but I appreciate that in Gramm-Leach-Bliley.

May I have one other question, Mr. Chairman, one final question? And it goes to you, Mr. Mierzwinski, as a consumer advocate here. You know, we have seen an economy that is increasingly data driven in terms of companies collecting, storing, processing even greater quantities of consumer information, often against consumers' wishes or even without their knowledge. The financial service industry, for example, we hear stories about lenders data mining sources like social media to help them form underwriting decisions on consumer loans. Companies aggregate more data. The consequences of a breach or improper use become greater as the risks expand beyond simple fraud to identity theft and other hardships.

Target experienced breaches of at least two kinds of customer information: payment card data and personal information, such as names, email addresses, and phone numbers. What if the next breach involves information like purchase histories or Social Security numbers?

So my question is: Are you concerned about the rise of big data? And what can we do to give consumers greater control over their data, reduce the chances of a breach, and minimize the harm to consumers if a breach occurs? And should we be putting limits on what companies can store without a consumer's affirmative opt-in?

Mr. MIERZWINSKI. Well, Senator, you have raised a question that I could talk about for about an hour, 2 hours.

Senator MENENDEZ. I am sure the Chairman would not want you to do that.

Mr. MIERZWINSKI. I will not. But at the end of my testimony, I refer to a recent Federal Trade Commission comprehensive report on privacy and also to a Law Review paper that I have written on this very subject of big data being used for financial decision-making. And as Mr. Duncan pointed out, much of the big data that has been collected is now starting to be collected in the mobile landscape as well. So in addition to credit card information, in addition to personal information about the kinds of things that you buy with your cards, we also now know where you are and what you are doing at any particular time, and that new locational data is something that I think Congress should look at as well.

But I would be very happy to talk to you about this Internet ecosystem. It used to be that you had a bank and you had a merchant and you had a credit bureau that had information about you. And there were direct marketing companies, to be sure, but they did not have very much information, and they were not connected. There are hundreds of interconnected if not thousands of interconnected business-to-business companies on the Internet buying and selling information about you today and auctioning you off in real time to the highest bidder. Many of them are predatory lenders, the highest bidders. There are companies on the Internet called "lead generator sites" that I would encourage the Committee to just hold a hearing on lead generation. You type, "I want a loan," on the Internet. You are taken to a site that just bids you out to the highest bidder. Not the lowest bidder, the highest bidder.

So there is a lot of work that needs to be done. Consumers need greater rights. There are some bills that address parts of it, and we would be happy to talk further on it.

Senator MENENDEZ. Mr. Chairman, I can see that there can be some value, even to consumers, to have some degree of information. But by the same token, I am increasingly concerned about the degree, the depth, the breadth, and scope of where that information is, and finding the right balance here I think is incredibly important.

I thank the Chair for his indulgence.

Senator WARNER. Well, let me thank the witnesses and thank my colleagues.

A couple of closing comments. One is I do think I would make my point for the third time. You know, we are just the first of what was going to be a series of hearings. The American public is very,

very concerned about this issue, and we can either do it in a collaborative fashion, or we can do it in an adversarial fashion. And I am not even saying so much Congress versus industry and consumer groups, but you all collaborating together is terribly important.

I think we have seen today actually that across the panel there was a sense that we need to move aggressively to chip and PIN. I tend to agree with Mr. Duncan. I cannot imagine chip and PIN versus chip and signature where you have automated systems. It seems like Beta versus VHS. And a little bit of that in the sense that—I think Mr. Leach made this point, and I want to re-emphasize it. As I learn more, chip and PIN is not a declaration of victory. You know, I would point back to the U.K. circumstance where the point-to-point fraud went down, but online fraud went up. And I think we have not seen the potential vulnerability we have all for online transactions. I was a technology guy, but boy, oh, boy, we have no consumer or financial protections at all in that space.

Also, Mr. Mierzwinski, I think you may have gotten a win today since I think they all agreed to increase the Truth in Lending Act to equalize all cards to an equal standard. So maybe we made some small progress as well.

I would just close out my comments with, you know, two points.

One, if we think about this more holistically, I do think—and I am just starting to learn this notion of tokenization and some of these other things so that there is encrypted data regardless of where your transaction takes place, is something that we need to think through. And I am sensitive to Mr. Duncan's members' concerns that, you know, you do not want to go out and buy a terminal that is going to be outdated 6 months or a year from now, so how you keep that in some kind of open system so it cannot be cobbled on is something that makes sense.

An issue we did not even get to—and I think Senator Menendez raised it near the end, kind of not just broadly about folks' access to our data, but whoever has the data, how is it going to be kept secure? Wherever it stands in the financial system or in our system, you know, what are the obligations to keep that information in a secure fashion? Again, a topic that is going to be—that we will come back to.

So I again want to thank my colleagues. I thank both the first panel and the second panel. I go back to General Clapper's comments that this was—his estimate was a $300 billion hit to our economy last year, and it is dramatically going to be higher. We need to get ahead of this, and I look forward to working to find those solutions. Thank you all.

And, again, these letters will be added.

Senator WARNER. The hearing is adjourned.

[Whereupon, at 4:52 p.m., the hearing was adjourned.]

[Prepared statements, responses to written questions, and additional material supplied for the record follow:]

PREPARED STATEMENT OF SENATOR MARK KIRK

I am very pleased to be having this hearing today. There has obviously been considerable attention drawn to the issue of data security recently, with a number of data breaches occurring at several large retailers across the country. I am especially troubled because these breaches have had such a widespread impact—consumers being hit from all sides and with the more recent breaches impacting what is possibly one-third of the U.S. population. I think we have reached an inflection point. In the more recent data breaches, my constituents in Illinois and across the country were targeted at one of the busiest holiday shopping times, necessitating these individuals to replace cards and sign up for additional credit and identity monitoring—not to mention cope with substantial consumer anxiety.

Further, impacts are not only felt by consumers when a merchant is breached, but also by any number of other third parties, including banks whose customers shopped at the retailer. I have had one community banker in Illinois tell me that the recent Target data breach will cost their company roughly $100,000, and another regional bank has told me that they expect to lose millions for card replacement as well as millions for fraud. My bankers in Illinois tell me that nearly every Illinois bank had at least some credit and debit cards compromised by the breach, with about one-third of customers in State experiencing fraudulent account activity. As a result, Illinois banks had to replace large numbers of debit and credit cards, costing thousands in card replacement and fraud costs. While these are substantial, we know that any merchant that experiences a breach also suffers from brand damage, lost revenues, legal fees and other costs.

I do think it is important to view these breaches as criminal attacks and any entity that is breached as victims. It is also well known that these criminal hackers are persistent and when one technique is thwarted or secured against, these criminals will discover and create new and even more cryptic techniques with which to wreak havoc. However, I am hopeful that through this hearing, we can move beyond being "victims" to understand what other safeguards can be taken. We all saw and experienced the massive ramp up in national security reforms post the September 11th terrorist attacks. While our country is not completely without susceptibility, the United States has become much safer over the past decade and continues to constantly evolve in its security efforts to keep harm at bay.

While similar security efforts have been made in the cyber space, I don't believe it has been quite as extensive—and there is most definitely cause for considering whether we need to broaden the sphere of those responsible for greater cyber security.

According to the Identify Theft Resource Center, more than 4,200 breaches have occurred since 2005 exposing more than 600 million records, and in 2013 there were more than 600 reported breaches—an increase of 30 percent over 2012 and the highest number of recorded breaches since 2005.

In reviewing the spike in breaches, it is notable that the highest number of breaches occurred in the healthcare sector, at 43 percent and the business sector, which includes merchants, which accounted for roughly 34 percent of the reported breaches. Banks, credit and the financial sector accounted for only 4 percent of all breaches and less than 2 percent of all breached records.

After some of the more recent data breaches at retailers, there were claims made and questions asked whether the banks should have updated their technologies—specifically through the use of "chip and pin". While I look forward to hearing from the witnesses about these and other protective measures industry can undertake to make the system safer and more sound, I also understand that in several of the most recent cases, chip and pin technology likely would not have prevented these breaches. Just as with national security, this is a shared responsibility of a number of parties and it is critical that all parties that handle this sensitive personal information take all possible steps to ensure that information is kept safe.

Through the Gramm-Leach-Bliley Act, Reg. E, the Fair Credit and Reporting Act (FCRA) and a number of other regulatory requirements, some of the Nation's most vulnerable institutions—namely banks and financial institutions that house valuable and sensitive information—have taken extraordinary measures to keep up with the ever present and ever changing threats in the cyber security world. In addition to heightened standards, banks also face penalties, such as prompt corrective action, fines and other penalties often before a breach has occurred—just for being noncompliant.

I think all of these heightened standards and oversight is the right approach—financial institutions should have some of the highest cyber security measures in place to protect American consumers and the financial system. However, I think it is also appropriate to consider if other entities that either store or handle the same

type of sensitive information should come under the same scrutiny and oversight to protect consumers.

I hope to explore whether we should expand this "sphere" of scrutiny and bring greater oversight and accountability to other businesses and entities that have access to and in some instances store large amounts of consumer data. Some of these considerations might include whether the Federal Trade Commission (FTC) needs additional regulatory authorities, including the ability to require heightened standards as new threats emerge, additional oversight authority and the authority to utilize penalties for those entities found noncompliant. I also would like to explore whether our witnesses believe that creating a merchant/retailer ISAC (Information Sharing and Analysis Center) would help in preventing these breaches or, at a minimum, if an ISAC could effectively prevent the spreading of these threats to other merchants.

Finally, while industry must be vigilant and constantly evolve to protect itself and U.S. consumers, we also must look at the role of law enforcement in cyber security to see what else our Nation's law enforcement community needs to effectively combat these threats. Part of this may mean exploring what the Administration, Congress and Federal agencies can do to incite international cooperation, especially in areas where these criminal cells seem to exist. We also need to ensure that our criminal statutes are updated to bring stiff sentences to those engaging in these cyber crimes. Thank you again and I look forward to hearing from our witnesses.

PREPARED STATEMENT OF WILLIAM NOONAN

DEPUTY SPECIAL AGENT IN CHARGE, UNITED STATES SECRET SERVICE
CRIMINAL INVESTIGATIVE DIVISION, CYBER OPERATIONS BRANCH

FEBRUARY 3, 2014

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

The Role of the Secret Service

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

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

Secret Service investigations have resulted in the arrest and successful prosecution of cyber criminals involved in the largest known data breaches, including those

---

[1] Beginning in 1970, and over the course of 3 years, the chief teller at the Park Avenue branch of New York's Union Dime Savings Bank manipulated the account information on the bank's computer system to embezzle over $1.5 million from hundreds of customer accounts. This early example of cyber crime not only illustrates the long history of cyber crime, but the difficulty companies have in identifying and stopping cyber criminals in a timely manner—a trend that continues today.

[2] *See* 18 USC § 1030.

[3] *See* 18 USC § 1029.

[4] *See* 18 USC § 1029(e)(1).

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

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

The Transnational Cyber Crime Threat

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

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

The Secret Service has successfully investigated many underground cyber criminal marketplaces. In one such infiltration, the Secret Service initiated and conducted a 3-year investigation that led to the indictment of 11 perpetrators allegedly involved in hacking nine major U.S. retailers and the theft and sale of more than 40 million credit and debit card numbers. The investigation revealed that defendants from the United States, Estonia, China and Belarus successfully obtained credit and debit card numbers by hacking into the wireless computer networks of major retailers—including TJ Maxx, BJ's Wholesale Club, Office Max, Boston Market, Barnes & Noble, Sports Authority and Dave & Buster's. Once inside the networks, these cyber criminals installed "sniffer" programs[6] that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks. After the data was collected, the conspirators concealed the information in encrypted computer servers that they controlled in the United States and Eastern Europe. The credit and debit card numbers were then sold through online transactions to other criminals in the United States and Eastern Europe. The stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The defendants then used these fraudulent cards to withdraw tens of thousands of dollars at a time from ATMs. The defendants were able to conceal and launder their illegal proceeds by using anonymous Internet-based digital currencies within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe.[7]

In data breaches like these the effects of the criminal acts extended well beyond the companies compromised, potentially affecting millions of individual card holders. Proactive and swift law enforcement action protects consumers by preventing and limiting the fraudulent use of payment card data, identity theft, or both. Cyber crime directly impacts the U.S. economy by requiring additional investment in im-

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

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

plementing enhanced security measures, inflicting reputational damage on U.S. firms, and direct financial losses from fraud—all costs that are ultimately passed on to consumers.

Secret Service Strategy for Combating This Threat

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

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

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

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

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

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

Liberty Reserve was identified as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act, effectively cutting it off from the U.S. financial system.

Collaboration With Other Federal Agencies and International Law Enforcement

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

One example of the Secret Service's success in these investigations is the case involving Heartland Payment Systems. As described in the August 2009 indictment, a transnational organized criminal group allegedly used various network intrusion techniques to breach security and navigate the credit card processing environment. Once inside the networks, they installed "sniffer" programs to capture card numbers, as well as password and account information. The Secret Service investigation, the largest and most complex data breach investigation ever prosecuted in the United States, revealed that data from more than 130 million credit card accounts were at risk of being compromised and exfiltrated to a command and control server operated by an international group directly related to other ongoing Secret Service investigations. During the course of the investigation, the Secret Service uncovered that this international group committed other intrusions into multiple corporate networks to steal credit and debit card data. The Secret Service relied on various investigative methods, including subpoenas, search warrants, and Mutual Legal Assistance Treaty (MLAT) requests through our foreign law enforcement partners to identify three main suspects. As a result of the investigation, these primary suspects were indicted for various computer-related crimes. The lead defendant in the indictment pled guilty and was sentenced to twenty years in Federal prison. This investigation is ongoing with over 100 additional victim companies identified.

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

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

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

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

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

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

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

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

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

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

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

Secret Service Framework

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

Electronic Crimes Task Forces

In 1995, the Secret Service New York Field Office established the New York Electronic Crimes Task Force (ECTF) to combine the resources of academia, the private

sector, and local, State and Federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructures. In 2001, Congress directed the Secret Service to establish a nationwide network of ECTFs to "prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."[9]

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

Cyber Intelligence Section

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

Electronic Crimes Special Agent Program

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

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

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

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

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

National Computer Forensics Institute

The National Computer Forensics Institute (NCFI) initiative is the result of a partnership between the Secret Service, NPPD, the State of Alabama, and the Alabama District Attorney's Association. The goal of this facility is to provide a national standard of training for a variety of electronic crimes investigations. The program

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

offers State and local law enforcement officers, prosecutors, and judges the training necessary to conduct computer forensics examinations. Investigators are trained to respond to network intrusion incidents and to conduct electronic crimes investigations. Since opening in 2008, the institute has held over 110 cyber and digital forensics courses in 13 separate subjects and trained and equipped more than 2,500 State and local officials, including more than 1,600 police investigators, 570 prosecutors and 180 judges from all 50 States and three U.S. territories. These NCFI graduates represent more than 1,000 agencies nationwide.

Partnerships with Academia

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

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

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

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

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

Legislative Action to Combat Data Breaches

While there is no single solution to prevent data breaches of U.S. customer information, legislative action could help to improve the Nation's cybersecurity, reduce regulatory costs on U.S. companies, and strengthen law enforcement's ability to conduct effective investigations. The Administration previously proposed law enforcement provisions related to computer security through a letter from OMB Director Lew to Congress on May 12, 2011, highlighting the importance of additional tools to combat emerging criminal practices. We continue to support changes like these that will keep up with rapidly evolving technologies and uses.

Conclusion

The Secret Service is committed to safeguarding the Nation's financial payment systems by investigating and dismantling criminal organizations involved in cyber crime. Responding to the growth in these types of crimes and the level of sophistication these criminals employ requires significant resources and greater collaboration

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

among law enforcement and its public and private sector partners. Accordingly, the Secret Service dedicates significant resources to improving investigative techniques, providing training for law enforcement partners, and raising public awareness. The Secret Service will continue to be innovative in its approach to cyber crime and cyber security and is pleased that the Committee recognizes the magnitude of these issues and the evolving nature of these crimes.

PREPARED STATEMENT OF JESSICA RICH

DIRECTOR OF THE BUREAU OF CONSUMER PROTECTION
FEDERAL TRADE COMMISSION

FEBRUARY 3, 2014

I. INTRODUCTION

Chairman Warner, Ranking Member Kirk, and Members of the Subcommittee, I am Jessica Rich, Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's testimony on data security.

As recent publicly announced data breaches remind us,[2] consumers' information is subject to a variety of risks. Hackers and others seek to exploit vulnerabilities, obtain unauthorized access to consumers' sensitive information, and potentially misuse it in ways that can cause serious harms to consumers as well as businesses. And in this increasingly interconnected economy, all of this takes place against the background of the threat of identity theft, a pernicious crime that harms both consumers and financial institutions. The Bureau of Justice Statistics estimates that 16.6 million persons—or 7 percent of all U.S. residents ages 16 and older—were victims of identity theft in 2012.[3]

As the Nation's leading privacy enforcement agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector and has settled 50 law enforcement actions against businesses that we alleged failed to protect consumers' personal information appropriately. Data security is of critical importance to consumers. If companies do not protect the personal information they collect and store, that information could fall into the wrong hands, resulting in fraud and other harm, along with a potential loss of consumer confidence in particular business sectors or entities, payment methods, or types of transactions. Accordingly, the Commission has undertaken substantial efforts for over a decade to promote data security in the private sector through civil law enforcement, education, and policy initiatives.

This testimony offers an overview of the Commission's recent efforts in the enforcement, education, and policy areas. It then describes the FTC's cooperation with Federal and State agencies on issues of privacy and data security. Finally, while the testimony does not offer views on any particular legislation, the Commission reiterates its bipartisan support for Congress to enact data security legislation that would (1) strengthen its existing authority governing data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.[4]

---

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

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

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

[4] The Commission has long supported data security and breach notification legislation. *See, e.g.,* Prepared Statement of the Federal Trade Commission, "Privacy and Data Security: Protecting Consumers in the Modern World," Before the Senate Committee on Commerce, Science, and Transportation, 112th Cong., June 29, 2011, *available at http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-tradecommission-privacy-and-data-security-protecting-consumers-modern/110629privacytestimonybrill.pdf;* Prepared Statement of the Federal Trade Commission, "Data Security," Before Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce, 112th Cong., June 15, 2011, *available at http://www.ftc.gov/sites/default/files/documents/pub-*

Continued

II. THE COMMISSION'S DATA SECURITY PROGRAM

A. Law Enforcement

To promote data security, the Commission enforces several statutes and rules that impose obligations upon businesses that collect and maintain consumer data. The Commission's Safeguards Rule, which implements the Gramm-Leach-Bliley Act ("GLB Act"), for example, provides data security requirements for nonbank financial institutions.[5] The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,[6] and imposes safe disposal obligations on entities that maintain consumer report information.[7] The Children's Online Privacy Protection Act (COPPA) requires reasonable security for children's information collected online.[8]

In addition, the Commission enforces the proscription against unfair or deceptive acts or practices in Section 5 of the FTC Act.[9] If a company makes materially misleading statements or omissions about a matter, including data security, and such statements or omissions are likely to mislead reasonable consumers, they can be found to be deceptive in violation of Section 5.[10] Using its deception authority, the Commission has settled more than 30 matters challenging companies' express and implied claims that they provide reasonable security for consumers' personal data. Further, if a company's data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition, those practices can be found to be unfair and violate Section 5.[11] The Commission has settled more than 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice.[12]

In the data security context, the FTC conducts its investigations with a focus on reasonableness—a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.[13] In each investigation, the Commission examines such factors as whether the risks at issue were well known or reasonably foreseeable, the costs and benefits of implementing various protections, and the tools that are currently available and used in the marketplace.

Since 2001, the Commission has used its authority to settle 50 cases against businesses that it charged with failing to provide reasonable protections for consumers' personal information.[14] In each of these cases, the Commission has examined a company's practices as a whole and challenged alleged data security failures that were multiple and systemic. Through these settlements, the Commission has made clear that reasonable and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; that the Commission does not require perfect security; and that the mere fact that a breach occurred does not mean that a company has violated the law.

In its most recent case, the FTC entered into a settlement with GMR Transcription Services, Inc., a company that provides audio file transcription services for

---

lic__statements/preparedstatement-federal-trade-commission-data-security/110615datasecurity house.pdf; FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), *available at http://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf;* President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), *available at http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf.*

[5] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).

[6] 15 U.S.C. § 1681e.

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

[8] 15 U.S.C. §§ 6501–6506; *see also* 16 C.F.R. Part 312 ("COPPA Rule").

[9] 15 U.S.C. § 45(a).

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

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

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

[13] In many of the FTC's data security cases based on deception, the company has made an express or implied claim that its information security practices are reasonable, which is analyzed through the same lens.

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

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

The FTC also recently announced a case against TRENDnet, which involved a video camera designed to allow consumers to monitor their homes remotely.[16] The complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from baby monitoring to home security. Although TRENDnet claimed that the cameras were "secure," they had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet address. This resulted in hackers posting 700 consumers' live feeds on the Internet. Under the FTC settlement, TRENDnet must maintain a comprehensive security program, obtain outside audits, notify consumers about the security issues and the availability of software updates to correct them, and provide affected customers with free technical support for the next 2 years.

Finally, one of the best-known FTC data security cases is the 2006 action against ChoicePoint, Inc., a data broker that allegedly sold sensitive information (including Social Security numbers in some instances) concerning more than 160,000 consumers to data thieves posing as ChoicePoint clients.[17] In many instances, the thieves used that information to steal the consumers' identities. The Commission alleged that ChoicePoint failed to use reasonable procedures to screen prospective purchasers of the consumers' information and ignored obvious security red flags. For example, the FTC alleged that the company approved as purchasers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from public commercial photocopying facilities. In settling the case, ChoicePoint agreed to pay $10 million in civil penalties for violations of the FCRA and $5 million in consumer redress for identity theft victims, and agreed to undertake comprehensive data security measures.[18]

B. Policy Initiatives

The Commission also undertakes policy initiatives to promote privacy and data security. For example, through its reports, the FTC has encouraged companies to provide reasonable security for consumer data by following certain key principles.[19] First, companies should know what consumer information they have and what personnel or third parties have, or could have, access to it. Understanding how information moves into, through, and out of a business is essential to assessing its security vulnerabilities. Second, companies should limit the information they collect and retain based on their legitimate business needs, so that needless storage of data does not create unnecessary risks of unauthorized access to the data. Third, businesses should protect the information they maintain by assessing risks and implementing protections in certain key areas—physical security, electronic security, employee training, and oversight of service providers. Fourth, companies should prop-

---

[15] *In the Matter of GMR Transcription Servs., Inc., et al.,* Matter No. 112–3120 (Dec. 16, 2013), *available at http://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it.*

[16] *In the Matter of TRENDnet, Inc.,* Matter No. 122–3090 (Sept. 4, 2013), *available at http://www.ftc.gov/opa/2013/09/trendnet.shtm.*

[17] *United States v. ChoicePoint, Inc.,* No. 106–CV–0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006), *available at http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2010/09/choicepoint-inc.*

[18] In 2009, the Commission charged that the company violated the earlier court order and obtained a stipulated modified order under which ChoicePoint agreed to expand its data security obligations and pay monetary relief in the amount of $275,000. *United States v. ChoicePoint, Inc.,* No. 1:06–CV–0198–JTC (N.D. Ga. 2009) (settlement entered on Oct. 14, 2009).

[19] FTC Report, *Protecting Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), *available at http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.*

erly dispose of information that they no longer need. Finally, companies should have a plan in place to respond to security incidents, should they occur.[20]

The FTC also hosts workshops on business practices and technologies affecting consumer data. For example, in November, the FTC held a workshop on the phenomenon known as the "Internet of Things"—*i.e.,* Internet-connected refrigerators, thermostats, cars, and other products and services that can communicate with each other and/or consumers.[21] The workshop brought together academics, industry representatives, and consumer advocates to explore the security and privacy issues from increased connectivity in everyday devices, in areas as diverse as smart homes, connected health and fitness devices, and connected cars. Also, last June, the Commission hosted a public forum on mobile security issues, including potential threats to U.S. consumers and possible solutions to them.[22] The forum brought together technology researchers, industry members and academics to explore the security of existing and developing mobile technologies and the roles various members of the mobile ecosystem can play in protecting consumers from potential security threats.

The Commission has also hosted programs on emerging forms of identity theft, such as child identity theft and senior identity theft. In these programs, the Commission discussed unique challenges facing children and seniors, and worked with stakeholders to develop outreach for these two communities. Since the workshops took place, the Commission has continued to engage in such tailored outreach.

C. Consumer Education and Business Guidance

The Commission is also committed to promoting better data security practices through consumer education and business guidance. On the consumer education front, the Commission sponsors OnGuard Online, a Web site designed to educate consumers about basic computer security.[23] OnGuard Online and its Spanish-language counterpart, *Alerta en Linea,*[24] average more than 2.2 million unique visits per year. Also, as part of its efforts to educate consumers about identity theft, Commission staff have worked with Members of Congress to host numerous town hall meetings on identity theft in order to educate their constituents. And, for consumers who may have been affected by the recent Target and other breaches, the FTC posted information online about steps they should take to protect themselves.[25]

The Commission directs its outreach to businesses as well. The FTC widely disseminates its business guide on data security,[26] along with an online tutorial based on the guide.[27] These resources are designed to provide a variety of businesses—and especially small businesses—with practical, concrete advice as they develop data security programs and plans for their companies.

The Commission has also released articles directed toward a nonlegal audience regarding basic data security issues for businesses.[28] For example, because mobile applications ("apps") and devices often rely on consumer data, the FTC has developed specific security guidance for mobile app developers as they create, release, and monitor their apps.[29] The FTC also creates business educational materials on specific topics—such as the risks associated with peer-to-peer ("P2P") file-sharing programs and companies' obligations to protect consumer and employee information

---

[20] *Id.* at 24–32.

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

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

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

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

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

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

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

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

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

from these risks[30] and how to properly secure and dispose of information on digital copiers.[31]

III. COOPERATION WITH STATE AND FEDERAL AGENCIES

The Commission has a long history of working closely with Federal and State agencies, as well as the private sector, to further its mission of promoting privacy and data security. State, Federal, and private sector entities each have served a unique role in data security: States have innovated by passing data breach notification laws; Federal banking agencies have protected consumers' security in the banking sector; the FTC has protected the security of consumers' information in retail, technology, and other sectors; Federal criminal law enforcement agencies have prosecuted identity thieves; credit reporting agencies have provided credit monitoring services to consumers in the event of a breach; and trade associations sponsor educational seminars and publish guidance to help their members understand their legal obligations.

In terms of cooperation with States, the FTC works closely with State Attorneys General to ensure that we coordinate our investigations and leverage our resources most effectively. For example, in one of the largest FTC-State coordinated settlements on record, LifeLock, Inc. agreed to pay $11 million to the FTC and $1 million to 35 State Attorneys General to settle charges that the company used false claims to promote its identity theft protection services.[32] As part of the settlement, LifeLock and its principals are barred from making deceptive claims and required to take more stringent measures to safeguard the personal information they collect from customers. The FTC also coordinated with the State AGs on cases such as TJX[33] and ChoicePoint.[34]

In terms of Federal enforcement cooperation, the FTC has worked with criminal law enforcement agencies such as the Federal Bureau of Investigation and Secret Service. The goals of FTC and Federal criminal law enforcement agencies are complementary: FTC actions send a message that businesses need to protect their customers' data on the front end, and criminal law enforcement actions send a message to identity thieves, fraudsters, and other criminals that their efforts to victimize consumers will be punished.

The FTC also works closely with State and Federal agencies to educate consumers and businesses on issues involving data security and privacy. For example, identity theft has been the top consumer complaint to the FTC for 13 consecutive years, and tax identity theft—which often begins by thieves obtaining Social Security numbers and other personal information from consumers in order to obtain their tax refund—has been an increasing share of the Commission's identity theft complaints.[35] Just last month, the FTC hosted 16 events across the country, along with a series of national Webinars and Twitter chats as part of Tax Identity Theft Awareness Week.[36] The events, which included representatives of the Internal Revenue Service, the American Association of Retired Persons, and local U.S. Attorney's offices, were de-

---

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

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

[32] *FTC v. LifeLock, Inc., et al.,* No. 2:10-cv-00530–NVW (D. Ariz.) (filed Mar. 9, 2010), *available at http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2010/11/lifelock-inc-corporation.*

[33] *In the Matter of The TJX Cos., Inc.,* No. C–4227 (F.T.C. July 29, 2008), *available at http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2008/08/tjx-companies-inc-matter; see* also Press Release, Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisent for Failing to Provide Adequate Security for Consumers' Data (Mar. 27, 2008), *available at http://www.ftc.gov/news-events/press-releases/2008/03/agency-announces-settlement-separate-actions-against-retailer-tjx* (citing the Commission's coordination with 39 State Attorneys General).

[34] *United States v. ChoicePoint, Inc., supra* note 17; *see also* Press Release, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress* (Jan. 26, 2006), *available at http://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million* (mentioning the FTC's cooperation with the Department of Justice and Securities and Exchange Commission).

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

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

signed to raise awareness about tax identity theft and provide consumers with tips on how to protect themselves, and what to do if they become victims.

IV. CONCLUSION

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

PREPARED STATEMENT OF JAMES A. REUTER

EXECUTIVE VICE PRESIDENT, FIRSTBANK,
ON BEHALF OF THE AMERICAN BANKERS ASSOCIATION

FEBRUARY 3, 2014

Chairman Warner, Ranking Member Kirk, and Members of the Subcommittee, my name is James A. Reuter, Executive Vice President, FirstBank, based in Lakewood, Colorado. Founded in 1963, FirstBank currently has over $13 billion in assets, over 115 locations and 2,000 employees serving Colorado, Arizona, and California. I serve as President of FirstBank Support Services, which provides information technology, payment processing services, 24 hour call center, and electronic banking services for 115 FirstBank locations. In addition, I serve on the American Bankers Association's (ABA) Payments Systems Administrative Committee, which focuses on emerging technologies that affect the payments system and assesses the implications for the financial services industry.

I appreciate the opportunity to be here to represent the ABA and discuss the recent Target and other data security breaches. The ABA represents banks of all sizes and charters and is the voice for the Nation's $14 trillion banking industry and its two million employees.

Notwithstanding these recent breaches, our payment system remains strong and functional. No security breach seems to stop the $3 trillion that Americans spend safely and securely each year with their credit and debit cards. And with good reason: Customers can use these cards confidently because their banks protect them from losses by investing in technology to detect and prevent fraud, reissuing cards and absorbing fraud costs.

At the same time, these breaches have reignited the long-running debate over consumer data security policy. ABA and the thousands of community, mid-size, regional, and large banks we represent recognize the paramount importance of a safe and secure payments system to our Nation and its citizens. We thank the Subcommittee for holding this hearing and welcome the ongoing discussion. From ABA's perspective, Congress should examine the specific circumstances of the Target breach and the broader data security issues involved, and we stand ready as a resource to assist in your efforts.

In my testimony I will focus on four main points:

- **Protecting consumers is the banking industry's first priority.** As the stewards of the direct customer relationship, the banking industry's overarching priority in breaches like that of Target's is to protect consumers and make them whole from any loss due to fraud.
- **A National data breach standard is essential.** Consumers' electronic payments are not confined by borders between States. As such, a national standard for data security and breach notification is of paramount importance, and we strongly support S. 1927, the Data Security Act of 2014.
- **All players in the payments systems, including retailers, must significantly improve their internal security systems as the criminal threat continues to evolve.**
- **Protecting the Payments System is a Shared Responsibility.** Banks, retailers, processors, and all of the participants in the payments system must share the responsibility of keeping the system secure, reliable, and functioning in order to preserve consumer trust. That responsibility should not fall predominantly on the financial services sector.

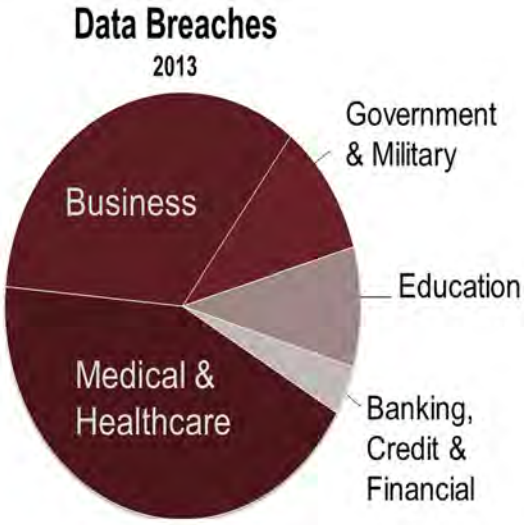
Before addressing each of these points in detail, it is important to understand the data security vulnerabilities in our system. The numbers are telling and point to the need for shared responsibility to fight off the continual attacks on data.

I. Data Security: Where are the Vulnerabilities?

It is a sobering fact that, since January 2005, a total of over 4,200 breaches exposing almost 600 million records have occurred nationwide. (Source: Identity Theft Re-

source Center) There were over 600 reported data breaches during 2013 alone, an increase of 30 percent over 2012 and the third highest number of breaches over the last 9 years. The two sectors reporting the highest number of breaches were the healthcare sector at 43 percent of reported breaches and the business sector, including merchants, which accounted for nearly 34 percent of reported breaches.

Moreover, the business sector, because of the Target breach, accounted for almost 82 percent of 2013's breached records. The Banking, Credit and Financial sector accounted for only 4 percent of all breaches and less than 2 percent of all breached records.[1] However, in spite of the small percentage of actual data breaches, the Banking, Credit and Financial sector bears a disproportionate share of breach recovery and fraud expenses. This is a consistent trend since 2005, where over this 9-year period our sector accounted for approximately 8 percent of all reported breaches. The business sector accounted for approximately 36 percent and health care sector approximately 23 percent of all breaches over the same time period.



Source: Identity Theft Resource Center

These numbers point to the central challenge associated with breaches of financial account data or personally identifiable information: while the preponderance of data breaches occur at entities far removed from the banking sector, it is the bank's customer potentially at the end of the line who must be protected.

II. Protecting Consumers is Our First Priority

While the facts of the Target breach remain fluid, the company has acknowledged that the breach occurred within its internal systems, affecting nearly 40 million credit and debit card accounts while also revealing the personally identifiable information (*e.g.,* name, address, email, telephone number) of potentially 70 million people. *On average, the Target breach has affected 10 percent of every bank's credit and debit card customer base.*

Paying for Fraud

When a retailer like Target speaks of its customers having "zero liability" from fraudulent transactions, it is because our Nation's banks are making customers whole, not the retailer that suffered the breach. Banks are required to swiftly research and reimburse customers for unauthorized transactions, and normally exceed legal requirements by making customers whole within days of the customer alerting the bank of the fraud, if not immediately.[2]

[1] *2013 Data Breach Category Summary,* Identity Theft Resource Center, January 1, 2014, *available at: http://www.idtheftcenter.org/images/breach/2013/BreachStatsReportSummary2013.pdf*

[2] With traditional card payments, the rights and obligations of all parties are well-defined by Federal statute when an unauthorized transaction occurs. For example, Regulation E describes

Continued

After the bank has reimbursed a customer for the fraudulent transaction, it can then attempt to "charge-back" the retailer where the transaction occurred. Unfortunately, and certainly in my experience, the majority of these attempts are unsuccessful, with the bank ultimately shouldering the vast majority of fraud loss and other costs associated with the breach. Overall, for 2009, 62 percent of reported debit card fraud losses were borne by banks, while 38 percent were borne by merchants.[3]

It is an unfortunate truth that, in the end (and often well after the breach has occurred and the banks have made customers whole) banks generally receive *pennies for each dollar* of fraud losses and other costs that were incurred by banks in protecting their customers. This minor level of reimbursement, when taken in concert with the fact that banks bear over 60 percent of reported fraud losses yet have accounted for less than 8 percent of reported breaches since 2005 is clearly inequitable. We believe banks should be fully reimbursed for the costs they bear for breaches that occur elsewhere.

Reissuing and Ongoing Monitoring

Each bank makes its own decision as to when and whether to reissue cards, which in the case of our bank costs $5 per card. In the case of the Target breach, the decision of whether to reissue cards was made even more difficult considering the inconvenience this can cause during the holiday season: breach or no breach, many consumers would not have wanted their cards shut down leading up to Christmas. Those cards that have not been reissued are being closely monitored for fraudulent transactions. In some instances, banks gave customers an option of keeping their cards open through the holidays until they could reissue all cards in January or, if they were concerned, to shut their card down and be reissued a new card immediately.

The Target compromise was also unique in terms of the high awareness of the "Target" name, the sheer number of people affected, and the media coverage of the event. In addition to proactively communicating with customers about the breach, bank call centers and branches have handled millions of calls and in-person inquiries regarding the card compromise. Many smaller and community banks have increased staffing to meet consumer demand. At the end of the day, consumers expect answers and to be protected by their bank, which is why they call us, not Target or whoever actually suffered the breach.

We also remain vigilant to the potential for fraud to occur in the future as a result of the Target breach. Standard fraud mitigation methods banks use on an ongoing basis include monitoring transactions, reissuing cards, and blocking certain merchant or types of transactions, for instance, based on the location of the merchant or a transaction unusual for the customer. Most of us are familiar with that call from a card issuer rightfully questioning a transaction and having a card canceled as a result. In many cases, however, the lifespan of compromised consumer data extends well beyond the weeks immediately following the breach itself. Just because the headlines fade away does not mean that banks can afford to relax their ongoing fraud protection and screening efforts. In addition there are ongoing customer support issues as customers setup new card numbers for recurring transactions related to health club memberships, online stores such as iTunes, *etc.*

III. A National Data Breach Standard is Essential

In many instances, the identity of the entity that suffered the breach is either not known or, oftentimes, intentionally not revealed as there is no requirement to do so. Understandably, a retailer or other entity would rather pass the burden on to the affected consumers' banks rather than taking the reputational hit themselves. In such cases, the bank is put in the position of notifying their customers that their credit or debit card data is at risk without being able to divulge where the breach occurred. Many banks have expressed great frustration regarding this process, with their customers—absent better information—blaming the bank for the breach itself and inconvenience they are now suffering.

---

consumers' rights and card issuers' obligations when a debit card is used, while Regulation Z does so for credit card transactions. The payment networks also have well-established rules for merchants and issuers. For instance, while Regulation Z limits a customer's liability for unauthorized transactions on a lost or stolen credit card to $50, the card networks require issuers to provide their cardholders with zero liability.

[3] *2009 Interchange Revenue, Covered Issuer Cost, and Covered Issuer and Merchant Fraud Loss Related to Debit Card Transactions,* June 2011, Board of the Governors of the Federal Reserve System, *available at: http://www.federalreserve.gov/paymentsystems/files/debitfees_costs.pdf.*

Like the well-defined Federal regulations surrounding consumer protections for unauthorized credit or debit transactions, data breach notification for State and nationally chartered banks is governed by guidance from the Federal Financial Institutions Examination Council (FFIEC), as enacted in the Gramm-Leach-Bliley Act, requiring every bank to have a customer response program. Retail establishments have no comparable Federal requirements. In addition, not only are retailers, healthcare organizations, and others who suffer the majority of breaches not subject to Federal regulatory requirements in this space, no entity oversees them in any substantive way. Instead they are held to a wide variety of State data breach laws that aren't always consistent. Banks too must also abide by many of these State laws, creating a patchwork of breach notification and customer response standards that are confusing to consumers as well as to companies.

Currently, 46 States, three U.S. territories, and the District of Columbia have enacted laws governing data security in some fashion, such as standards for data breach notification and for the safeguarding of consumer information. Although some of these laws are similar, many have inconsistent and conflicting standards, forcing businesses to comply with multiple regulations and leaving many consumers without proper recourse and protections.

Establishing a national data security and notification law would provide better protection for consumers nationwide. It is for this reason that we applaud and fully support the introduction of the Data Security Act of 2014 (S. 1927) by Senators Tom Carper (D–DE) and Roy Blunt (R–MO). This bipartisan legislation would better protect consumers by replacing the current patchwork of State laws and establishing one set of national requirements. The bill requires any business that maintains sensitive personal and financial information—including banks, verified-retailers, and data brokers—to implement, maintain, and enforce reasonable policies and procedures to protect the confidentiality and security of sensitive information from unauthorized use.

Our existing national payments system serves hundreds of millions of consumers, retailers, banks, and the economy well. It only stands to reason that such a system functions most effectively when it is governed by a consistent national data breach policy.

IV. All Players in the Payments System Must Improve Their Internal Systems as the Criminal Threat Continues to Evolve

While many details of the Target breach are still largely unknown, it is clear that criminal elements responsible for such attacks are growing increasingly sophisticated in their efforts to breach the payments system. This disturbing evolution, as demonstrated by the Target breach, will require enhanced attention, resources, and diligence on the part of all payments system participants.

The increased sophistication and prevalence of breaches caused by criminal attacks—as opposed to negligence or unintentional system breaches is also borne out in a recent study by the Ponemon Institute. Evaluating annual breach trends, the Institute found that 2012 was the first year in which malicious or criminal attacks were the most frequently encountered root cause of data breaches by organizations in the study, at 41 percent.[4]

Emerging details of the Target breach are allowing us to see a troubling picture of the direction the criminal evolution is taking, and what it means for at-risk consumer data. For example:

- While Target's last public statement on the issue stated that the PINs that were compromised as part of the breach were encrypted, the company originally stated that PINs were not compromised at all. If the PINs were unencrypted, this would be particularly troubling, as that would make bank customer accounts vulnerable to ATM cash withdrawals as well as unauthorized purchases. We call on law enforcement and those in the forensics process to be as transparent as possible in outlining what are the precise threats to our customers.
- Even if the PINs that were breached were in fact encrypted, there is still the potential that they could be decrypted, placing our customers at just as much risk as if unencrypted PINs had been captured.
- Banks also do not know the extent to which their customers' bank account numbers, which are linked to Target's RedCard, were compromised as a result of the breach. If this information was compromised, customers could be vulnerable

[4] 2013 Cost of Data Breach Study: United States, May 2013, Ponemon Institute, *available at: http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-us-report-2013.enus.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Jun_worldwide_CostofaDataBreach.*

to unauthorized Automated Clearing House (ACH) transactions directly from their accounts.

- More generally, banks have also encountered significant customer confusion as to the nature of Target's RedCard and the bank's ability to help. Many believe the bank can cancel the card and reissue it even though the card was issued by Target. This confusion points to a broader problem with the emergence of many nontraditional payments providers: customers have a hard time understanding which payment entity is responsible for what, and often just assume the bank is the responsible party.

These threats to bank customer accounts point to the security vulnerabilities associated with nontraditional payments companies, such as Target, having direct linkages to the payments system without information security regulatory requirements comparable to that of financial institutions.

V. Protecting the Payments System is a Shared Responsibility

While much has recently been made about the on-going disagreements between the retail community and the banking industry over who is responsible for protecting the payments system, in reality our Nation's payments system is made up of a wide variety of players: banks, card networks, retailers, processors, and even new entrants, such as Square, Google, and PayPal. Protecting this system is a shared responsibility of all parties involved and we need to work together and invest the necessary resources to combat increasingly sophisticated threats to breach the payments system.

We must work together to combat the ever-present threat of criminal activity at our collective doorstops. Inter-industry squabbles, like those over interchange, have had a substantial impact on bank resources available to combat fraud. Policymakers must examine that impact closely to ensure that the necessary resources are not diverted from addressing the real concern at hand—the security of our Nation's payment system and the need to protect consumers. *All* participants must invest the necessary resources to combat this threat.

In the wake of this breach, there has been significant discussion over how to enhance payment card security, focusing on the implementation of chip-based security technology known as EMV.[5] This technology makes it much harder for criminals to create duplicate cards or make sense of encrypted data that they steal.

We encourage the implementation of chip technology, both on the card and at the point-of-sale. In fact, the rollout of this technology in the United States is well underway, with the next set of deadlines for banks and retailers coming in late 2015. It takes time for full implementation of chip technology in the United States, as our country supports the largest economy in the world, with over 300 million customers, 8 million retailers, and 14,000 financial institutions.

Even though EMV is an important step in the right direction, there is no panacea for the everchanging threats that exist today. For instance, EMV technology would not have prevented the potential harm of the Target breach to the 70 million customers that had their name, address, email, and/or telephone number compromised. Moreover, EMV technology will help to address potential fraud at the point-of-sale, but it does not address online security, nor is it a perfect solution even at the point-of-sale as criminal efforts evolve. Because it is impossible to anticipate what new challenges will come years from now, we must therefore be cautious not to embrace any "one" solution as the answer to all concerns.

VI. The Path Forward

Any system is only as strong as its weakest link. The same certainly holds true in our rapidly changing consumer payments marketplace. The innovations that are driving the industry forward and presenting consumers with exciting new methods of making purchases is also rapidly expanding beyond the bounds of our existing regulatory and consumer protection regimes. And, as has historically been the case, the criminals are often one step ahead as the marketplace searches for consensus. That said, there are several positive steps policymakers can take to facilitate a higher level of security for consumers going forward. For example:

Raise all participants in the payments system to comparable levels of security. Security within the payments system is currently uneven. In addition to adhering to the Payment Card Industry Data Security Standards, banks and other financial institutions are also subject to significantly higher information security re-

[5] EMV stands for Europay, Mastercard, and Visa, the developers of a global standard for interoperation of integrated circuit, or "chip" cards and chip card compatible point-of-sale terminals and automated teller machines.

quirements than others that facilitate electronic payments and house bank customer payment data.[6] More must be done to buttress and enforce the current regulatory requirements that merchants face.

Establish a national data security breach and notification standard. A national data breach standard would provide better and more consistent protection for consumers nationwide. We applaud and fully support the introduction of The Data Security Act of 2014 (S. 1927) by Senators Carper and Blunt and believe this legislation meets that goal by replacing the current patchwork of State laws and establishing one set of national requirements.

Make those responsible for data breaches responsible for their costs. Banks bear the majority of costs associated with the fraud caused by breaches even though our industry is responsible for only a small percentage of the breaches that have occurred since 2005. When any entity—be it a bank, merchant, college or hospital—is responsible for a breach that compromises customer payment data or personally identifiable information, that entity should be responsible for the range of costs associated with that breach to the extent it was not adhering to the necessary security requirements.

Increase the speed and transparency with which the results of forensic investigations are shared with the financial community. When a breach occurs, there is much banks and others do not know and are not told for extended periods of time regarding the vulnerability of certain aspects of their customers' data. Similar to the robust manner in which banks and law enforcement currently share other cybersecurity threat data, we must examine ways to share the topline threat data from merchant and other breaches that does not impede the overall investigation. For example, banks and payment networks currently share an increasing amount of cybersecurity threat and fraud information through groups such as the Financial Services Information Sharing and Analysis Center and other groups within ABA. Our efforts would be greatly enhanced if that information sharing capacity expanded to include the merchant community. We would welcome such expansion and look forward to working collectively with merchants to combat our common adversaries.

Banks are committed to doing our share, but cannot be the sole bearer of that responsibility. Policymakers, card networks, and all industry participants have a vital role to play in addressing the regulatory gaps that exist in our payments system, and we stand ready to assist in that effort. Thank you for giving ABA the opportunity to provide this testimony. We look forward to continuing to work with Congress to enhance the security of our Nation's payment system, and maintain the trust and confidence hundreds of millions of Americans place in it every day.

PREPARED STATEMENT OF MALLORY DUNCAN

GENERAL COUNSEL AND SENIOR VICE PRESIDENT
NATIONAL RETAIL FEDERATION

FEBRUARY 3, 2014

Chairman Warner, Ranking Member Kirk and Members of the Subcommittee, thank you for giving me this opportunity to provide you with my thoughts on safeguarding consumers' financial information. My name is Mallory Duncan, and I am General Counsel of the National Retail Federation (NRF). NRF is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the Nation's largest private sector employer, supporting one in four U.S. jobs—42 million working Americans. Contributing $2.5 trillion to annual GDP, retail is a daily barometer for the Nation's economy.

Collectively, retailers spend billions of dollars safeguarding consumers' data and fighting fraud. Data security is something that our members strive to improve every day. Virtually all of the data breaches we've seen in the United States during the past couple of months—from those at retailers that have been prominent in the news to those at banks and card network companies that have received less attention—have been perpetrated by criminals that are breaking the law. All of these companies are victims of these crimes and we should keep that in mind as we explore this topic and public policy initiatives relating to it.

---

[6] For instance, banks are subject to the information security requirements contained within the Gramm-Leach-Bliley Act, the FFIEC Red Flag Rules regarding identity theft, and are continually examined against these requirements.

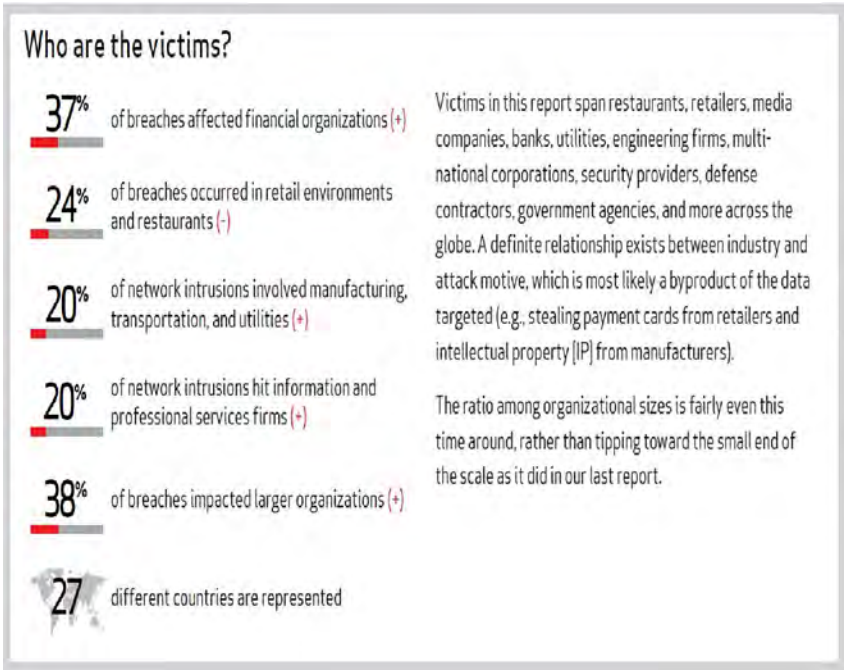
This issue is one that we urge the Committee to examine in a holistic fashion: we need to reduce fraud. That is, we should not be satisfied with deciding what to do after a data breach occurs—who to notify and how to assign liability. Instead, it's important to look at why such breaches occur and what the perpetrators get out of them so that we can find ways to reduce and prevent not only the breaches themselves, but the fraudulent activity that is often the goal of these events. If breaches become less profitable to criminals then they will dedicate fewer resources to committing them and our goals will become more achievable.

With that in mind, this testimony is designed to provide some background on data breaches and on fraud, explain how these events interact with our payments system, discuss some of the technological advancements that could improve the current situation, raise some ways to achieve those improvements, and then discuss the aftermath of data breaches and some ways to approach things when problems do occur.

Data Breaches in the United States

Unfortunately, data breaches are a fact of life in the United States. In its 2013 data breach investigations report, Verizon analyzed more than 47,000 security incidents and 621 confirmed data breaches that took place during the prior year. Virtually every part of the economy was hit in some way: 37 percent of breaches happened at financial institutions; 24 percent happened at retail; 20 percent happened at manufacturing, transportation and utility companies; and 20 percent happened at information and professional services firms.

It may be surprising to some given recent media coverage that more data breaches occur at financial institutions than at retailers. And, it should be noted, even these figures obscure the fact that there are far more merchants that are potential targets of criminals in this area. There are hundreds of times as many merchants accepting card payments in the United States than there are financial institutions issuing and processing those payments. So, proportionally, and not surprisingly, the thieves focus far more often on banks which have our most sensitive financial information—including not just card account numbers but bank account numbers, social security numbers and other identifying data that can be used to steal identities beyond completing some fraudulent transactions.



Source: 2013 Data Breach Investigations Report, Verizon

Nearly one-fifth of all of these breaches were perpetrated by State-affiliated actors connected to China. Three in four breaches were driven by financial motives. Two-thirds of the breaches took months or more to discover and 69 percent of all breaches were discovered by someone outside the affected organization.[1]

These figures are sobering. There are far too many breaches. And, breaches are often difficult to detect and carried out in many cases by criminals with real resources behind them. Financially focused crime seems to most often come from organized groups in Eastern Europe rather than State-affiliated actors in China, but the resources are there in both cases. The pressure on our financial system due to the overriding goal of many criminals intent on financial fraud is acute. We need to recognize that this is a continuous battle against determined fraudsters and be guided by that reality.

Background on Fraud

Fraud numbers raise similar concerns. Just a year ago, Forbes found that Mexico and the United States were at the top of the charts worldwide in credit and debit card fraud.[2] And fraud losses in the United States have been going up in recent years while some other countries have had success reducing their fraud rates. The United States in 2012 accounted for nearly 30 percent of credit and debit card charges but 47 percent of all fraud losses.[3] Credit and debit card fraud losses totaled $11.27 billion in 2012.[4] And retailers spend $6.47 billion trying to prevent card fraud each year.[5]

Fraud is particularly devastating for retailers in the United States. LexisNexis and Javelin Strategy & Research have published an annual report on the "True Cost of Fraud" each year for the last several years. The 2009 report found, for example, that retailers suffer fraud losses that are 10 times higher than financial institutions and 20 times the cost incurred by consumers. This study covered more than just card fraud and looked at fraudulent refunds/returns, bounced checks, and stolen merchandise as well. Of the total, however, more than half of what merchants lost came from unauthorized transactions and card chargebacks.[6] The founder and President of Javelin Strategy, James Van Dyke, said at the time, "We weren't completely surprised that merchants are paying more than half of the share of the cost of unauthorized transactions as compared to financial institutions. But we were very surprised that it was 90–10."[7] Similarly, Consumer Reports wrote in June 2011, "The Mercator report estimates U.S. card issuers' total losses from credit- and debit-card fraud at $2.4 billion. That figure does not include losses that are borne by merchants, which probably run into tens of billions of dollars a year."[8]

Online fraud is a significant problem. It has jumped 36 percent from 2012 to 2013.[9] In fact, estimates are that online and other fraud in which there is no physical card present accounts for 90 percent of all card fraud in the United States.[10] And, not surprisingly, fraud correlates closely with data breaches among consumers. More than 22 percent of breach victims suffered fraud while less than 3 percent of consumers who didn't have their data breached experienced fraud.[11]

---

[1] 2013 Data Breach Investigations Report, Verizon.

[2] "Countries with the most card fraud: U.S. and Mexico," *Forbes* by Halah Touryalai, Oct. 22, 2012.

[3] "U.S. credit cards, chipless and magnetized, lure global fraudsters," by Howard Schneider, Hayley Tsukayama and Amrita Jayakumar, *Washington Post,* January 21, 2014.

[4] "Credit Card and Debit Card Fraud Statistics," CardHub 2013, *available at http://www.cardhub.com/edu/creditdebit-card-fraud-statistics/*.

[5] *Id.*

[6] A fraud chargeback is when the card-issuing bank and card network take the money for a transaction away from the retailer so that the retailer pays for the fraud.

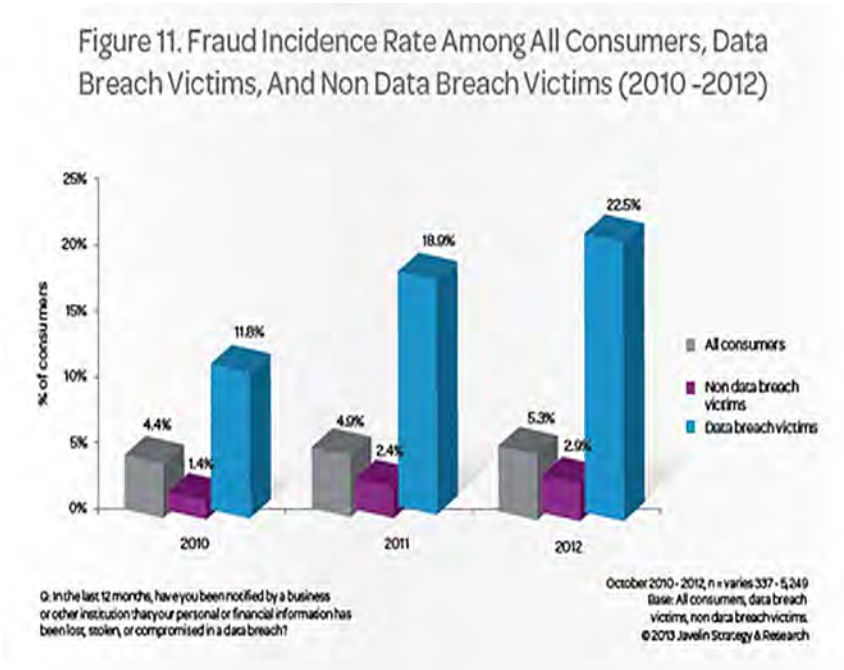
[7] "Retailers are bearing the brunt: New report suggests what they can do to fight back," by M.V. Greene, NRF Stores, Jan. 2010.

[8] "House of Cards: Why your accounts are vulnerable to thieves," Consumer Reports, June 2011.

[9] 2013 True Cost of Fraud, LexisNexis at 6.

[10] "What you should know about the Target case," by Penny Crosman, *American Banker,* Jan. 23, 2014.

[11] 2013 True Cost of Fraud, LexisNexis at 20.



Source: 2013 True Cost of Fraud, LexisNexis

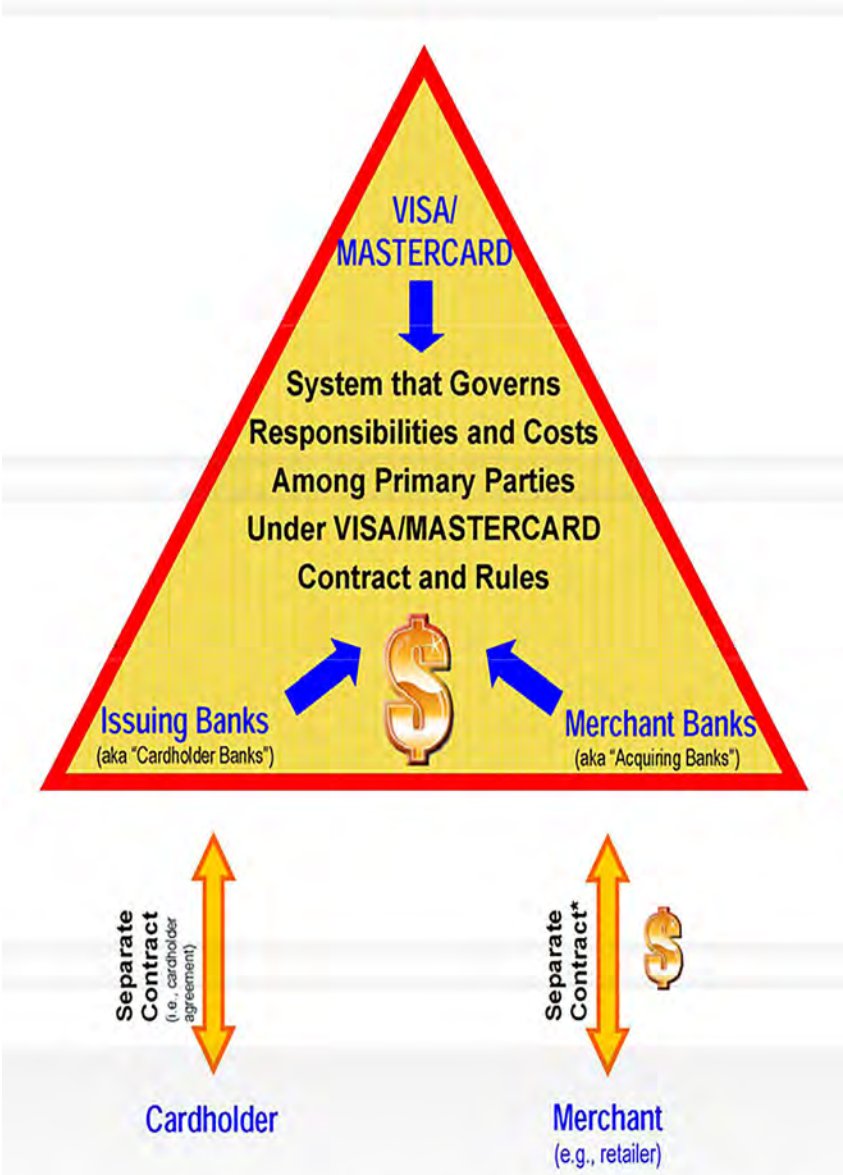
These numbers provide insights as to how to get to the right solutions of better safeguarding consumer and cardholder data and the need to improve authentication of transactions to protect against fraud. But before delving into those areas, some background on our payments system could be helpful.

The Payments System

Payments data is sought in breaches more often than any other type of data.[12] Now, every party in the payment system, financial institutions, networks, processors, retailers and consumers, has a role to play in reducing fraud. However, although all parties have a responsibility, some of those parties are integral to the system's design and promulgation while others, such as retailers and consumers, must work with the system as it is delivered to them.

As the following chart shows, while the banks are intimately connected to Visa and MasterCard, merchants and consumers have virtually no role in designing the payment system. Rather, they are bound to it by separate agreements issued by financial intermediaries.

[12] 2013 Data Breach Investigations Report, Verizon at 445, figure 35.



* Typically contract between merchant bank and its retailers requires retailers to reimburse merchant bank for any costs, penalties, or fees imposed by the system on the merchant bank (including chargebacks – i.e., disputed charges – and costs of data breaches)

Thus consumers are obligated to keep their cards safe and secure in their wallets and avoid misuse, but must necessarily turn their card data over to others in order to effectuate a transaction. Retailers are likewise obligated to collect and protect the card data they receive, but are obligated to deliver it to processors in order to complete a transaction, resolve a dispute or process a refund. In contrast, those inside the triangle have much more systemic control.

For example, retailers are essentially at the mercy of the dominant credit card companies when it comes to protecting payment card data. The credit card networks—Visa, MasterCard, American Express, Discover and JCB—are responsible for an organization known as the PCI (which stands for Payment Card Industry) data security council. PCI establishes data security standards (PCI–DSS) for payment cards. While well intentioned in concept, these standards have not worked quite as well in practice. They have been inconsistently applied, and their avowed purpose has been significantly altered.

PCI has in critical respects over time pushed card security costs onto merchants even when other decisions might have more effectively reduced fraud—or done so at lower cost. For example, retailers have long been required by PCI to encrypt the payment card information that they have. While that is appropriate, PCI has not required financial institutions to be able to accept that data in encrypted form. That means the data often has to be de-encrypted at some point in the process in order for transactions to be processed.

Similarly, merchants are expected to annually demonstrate PCI compliance to the card networks, often at considerable expense, in order to benefit from a promise that the merchants would be relieved of certain fraud inherent in the payment system, which PCI is supposed to prevent. However, certification by the networks as PCI Compliant apparently has not been able to adequately contain the growing fraud and retailers report that the "promise" increasingly has been abrogated or ignored. Unfortunately, as card security expert Avivah Litan of Gartner Research wrote recently, "The PCI (Payment Card Industry) security standard has largely been a failure when you consider its initial purpose and history."[13]

PCI has not addressed many obvious deficiencies in cards themselves. There has been much attention to the fact that the United States is one of the last places on earth to put card information onto magnetic stripes on the backs of cards that can easily be read and can easily be counterfeited (in part because that data is static and unchanging). We need to move past magstripe technology.

But, before we even get to that question, we need to recognize that sensitive card data is right on the front of the card, embossed with prominent characters. Simply seeing the front of a card is enough for some fraudsters and there have been fraud schemes devised to trick consumers into merely showing someone their cards. While having the embossed card number on the front of the card might have made sense in the days of knuckle-buster machines and carbon copies, those days are long passed.

In fact, cards include the cardholder's name, card number, expiration date, signature and card verification value (CVV) code. Everything a fraudster needs is right there on the card. The bottom line is that cards are poorly designed and fraud-prone products that the system has allowed to continue to proliferate.

PCI has also failed to require that the identity of the cardholder is actually verified or authenticated at the time of the transaction. Signatures don't do this. Not only is it easy to fake a signature, but merchants are not allowed by the major card networks to reject a transaction based on a deficient signature. So, the card networks clearly know a signature is a useless gesture which proves nothing more than that someone was there purporting to be the cardholder.

The use of personal identification numbers (PINs) has actually proven to be an effective way to authenticate the identity of the cardholder. PIN numbers are personal to each cardholder and do not appear on the cards themselves. While they are certainly not perfect, their use is effective at reducing fraud. On debit transactions, for example, PIN transactions have one-sixth the amount of fraud losses that signature transactions have.[14] But PINs are not required on credit card transactions. Why? From a fraud prevention perspective, there is no good answer except that the card networks which set the issuance standards have failed to protect people in a very basic way.

---

[13] "How PCI Failed Target and U.S. Consumers," by Avivah Litan, Gartner Blog Network, Jan. 20, 2014, *available at http://blogs.gartner.com/avivah-litan/2014/01/20/how-pci-failed-target-and-u-s-consumers/*.

[14] *See* 77 Fed. Reg. 46261 (Aug. 3, 2012) reporting $1.11 billion in signature debit fraud losses and $181 million in PIN debit fraud losses.

As noted by LexisNexis, merchant fraud costs are much higher than banks' fraud costs. When credit or debit card fraud occurs, Visa and MasterCard have pages of rules providing ways that banks may be able to charge back the transaction to the retailer (which is commonly referred to as a "chargeback"). That is, the bank will not pay the retailer the money for the fraudulent transaction even though the retailer provided the consumer with the goods in question. When this happens, and it happens a lot, the merchant loses the goods *and* the money on the sale. According to the Federal Reserve, this occurs more than 40 percent of the time when there is fraud on a signature debit transaction,[15] and our members tell us that the percentage is even higher on credit transactions. In fact, for online transactions, which as noted account for 90 percent of fraud, merchants pay for the vast majority of fraudulent transactions.[16]

Retailers have spent billions of dollars on card security measures and upgrades to comply with PCI card security requirements, but it hasn't made them immune to data breaches and fraud. The card networks have made those decisions for merchants and the increases in fraud demonstrate that their decisions have not been as effective as they should have been.

Improved Technology Solutions

There are technologies available that could reduce fraud. An overhaul of the fraud-prone cards that are currently used in the U.S. market is long overdue. As I noted, requiring the use of a PIN is one way to reduce fraud. Doing so takes a vulnerable piece of data (the card number) and makes it so that it cannot be used on its own. This ought to happen not only in the brick-and-mortar environment in which a physical card is used but also in the online environment in which the physical card does not have to be used. Canada, for example, is exploring the use of a PIN for online purchases. The same should be true here. Doing so would help directly with the 90 percent of U.S. fraud which occurs online. It is not happenstance that automated teller machines (ATMs) require the entry of a PIN before dispensing cash. Using the same payment cards for purchases should be just as secure as using them at ATMs.

Cards should also be smarter and use dynamic data rather than magnetic stripes. In much of the world this is done using computer chips that are integrated into physical credit and debit cards. That is a good next step for the United States. It is important to note, however, that there are many types of technologies that may be employed to make this upgrade. EMV, which is an acronym for Europay, MasterCard and Visa, is merely one particular proprietary technology. As the name indicates, EMV was established by Europay, MasterCard and Visa. A proprietary standard could be a detriment to the other potentially competitive networks.[17] Adopting a closed system, such as EMV, means we are locking out the synergistic benefits of competition.

But even within that closed framework, it should also be noted that everywhere in the world that EMV has been deployed to date the card networks have required that the cards be used with a PIN. That makes sense. But here, the dominant card networks are proposing to force chips (or even EMV) on the U.S. market without requiring PIN authentication. Doing that makes no sense and loses a significant part of the fraud prevention benefits of chip technology. To do otherwise would mean that merchants would spend billions to install new card readers without they or their customers obtaining PINs' fraud-reducing benefits. We would essentially be spending billions to combine a 1990s technology (chips) with a 1960s relic (signature) in the face of 21st century threats.

Another technological solution that could help deter and prevent data breaches and fraud is encryption. Merchants are already required by PCI standards to encrypt cardholder data but, as noted earlier, not everyone in the payments chain

---

[15] *Id.* at 46262.

[16] Merchants assume 74 percent of fraud losses for online and other card-not-present signature debit transactions. 77 Fed. Reg. 46262.

[17] There are issues with EMV because the technology is just one privately owned solution. For example, EMV includes specifications for near field communications that would form the technological basis of Visa and MasterCard's mobile payments solutions. That raises serious antitrust concerns for retailers because we are just starting to get some competitors exploring mobile payments. If the currently dominant card networks are able to lock-in their proprietary technology in a way that locks-out competition in mobile payments, that would be a bad result for merchants and consumers who might be on the verge of enjoying the benefits of some new innovations and competition.

So, while chip cards would be a step forward in terms of improving card products, if EMV is forced as the chip card technology that must be used—rather than an open-source chip technology which would facilitate competition and not predetermine mobile payment market-share—it could be a classic case of one step forward and two steps backward.

is required to be able to accept data in encrypted form. That means that data may need to be de-encrypted at some points in the process. Experts have called for a change to require "end-to-end" (or point-to-point) encryption which is simply a way to describe requiring everyone in the payment-handling chain to accept, hold and transmit the data in encrypted form. According to the September 2009 issue of the Nilson Report "most recent cyber attacks have involved intercepting data in transit from the point of sale to the merchant or acquirer's host, or from that host to the payments network." The reason this often occurs is that "data must be decrypted before being forwarded to a processor or acquirer because Visa, MasterCard, American Express, and Discover networks can't accept encrypted data at this time."[18]

Keeping sensitive data encrypted throughout the payments chain would go a long way to convincing fraudsters that the data is not worth stealing in the first place—at least, not unless they were prepared to go through the arduous task of trying to de-encrypt the data which would be necessary in order to make use of it. Likewise, using PIN-authentication of cardholders now would offer some additional protection against fraud should this decrypted payment data be intercepted by a criminal during its transmission "in the clear."

Tokenization is another variant that could be helpful. Tokenization is a system in which sensitive payment card information (such as the account number) is replaced with another piece of data (the "token"). Sensitive payment data could be replaced with a token to represent each specific transaction. Then, if a data breach occurred and the token data were stolen, it could not be used in any other transactions because it was unique to the transaction in question. This technology has been available in the payment card space since at least 2005.[19]

And, mobile payments offer the promise of greater security as well. In the mobile setting, consumers won't need to have a physical card—and they certainly won't replicate the security problem of physical cards by embossing their account numbers on the outside of their mobile phones. It should be easy for consumers to enter a PIN or password to use payment technology with their smart phones. Consumers are already used to accessing their phones and a variety of services on them through passwords. Indeed, if we are looking to leapfrog the already aging current technologies, mobile-driven payments may be the answer.

Indeed, as much improved as they are, chips are essentially dumb computers. Their dynamism makes them significantly more advanced than magstripes, but their sophistication pales in comparison with the common smartphone. Smartphones contain computing powers that could easily enable comparatively state-of-the-art fraud protection technologies. The phones soon may be nearly ubiquitous, and if their payment platforms are open and competitive, they will only get better.

The dominant card networks have not made all of the technological improvements suggested above to make the cards issued in the United States more resistant to fraud, despite the availability of the technology and their adoption of it in many other developed countries of the world, including Canada, the United Kingdom, and most countries of Western Europe.

In this section, I have merely described some of the solutions available, but the United States isn't using any of them the way that it should be. While everyone in the payments space has a responsibility to do what they can to protect against fraud and data theft, the card networks have arranged the establishment of the data security requirements and yet, in light of the threats, there is much left to be desired.

A Better System

How can we make progress toward the types of solutions that would reduce the crimes of data theft and fraud? One thing seems clear at this point: we won't get there by doing more of the same. We need PIN-authentication of card holders, regardless of the chip technology used on newly issued cards. We also need chip cards that use open standards and allow for competition among payment networks as we move into a world of growing mobile commerce. Finally, we need companies throughout the payment system to work together on achieving end-to-end encryption so that there are no weak links in the system where sensitive card payment information may be acquired more easily than in other parts of the system.

---

[18] The Nilson Report, Issue 934, Sept. 2009 at 7.

[19] For information on Shift4's 2005 launch of tokenization in the payment card space *see http://www.internetretailer.com/2005/10/13/shift4-launches-security-tool-that-lets-merchants-re-use-credit.*

Steps Taken by Retailers After Discovery of a Breach of Security

In our view, it is after a fulsome evaluation of data breaches, fraud, the payments system and how to improve each of those areas in order to deter and prevent problems that we should turn to the issue of what to do when breaches occur. Casting blame and trying to assign liability is, at best, putting the cart before the horse and, at worst, an excuse for some actors to ignore their own responsibility for trying to prevent these crimes.

One cannot reasonably demand greater security of a system than the system is reasonably capable of providing. Some participants act as if the system is more robust than it is. Currently, when the existing card products are hit in a criminal breach, that company is threatened from many sides. The threats come from entities seeking to exact fines and taking other penalizing action even before the victimized company can secure its network from further breaches and determine through a forensic analysis what has happened in order to notify potentially affected customers. For example, retailers that have suffered a breach are threatened with fines for the breach based on allegations of noncompliance with PCI rules (even when the company has been certified as PCI-compliant). Other actors may expect the breached party to pay for all of the fraudulent transactions that take place on card accounts that were misused, even though the design of the cards facilitated their subsequent counterfeiting. Indeed, some have seriously suggested that retailers reimburse financial institutions for the cost of reissuing more fraud-prone cards. And, as a consequence of the breach, some retailers must then pay higher fees on its card transactions going forward. Retailers pay for these breaches over and over again, despite often times being victims of sophisticated criminal methods not reasonably anticipated prior to the attack.

Breaches require retailers to devote significant resources to remedy the breach, help inform customers and take preventative steps to ward off future attacks and any other potential vulnerabilities discovered in the course of the breach investigation. Weeks or months of forensic analysis may be necessary to definitively discover the cause and scope of the breach. Any discovered weaknesses must be shored up. Quiet and cooperative law enforcement efforts may be necessary in an effort to identify and capture the criminals. Indeed, law enforcement may temporarily discourage publication of the breach so as to not alert the perpetrators that their efforts have been detected.

It is worth noting that in some of these cases involving payment card data, retailers discover that they actually were not the source of the breach and that someone else in the payments chain was victimized or the network intrusion and theft occurred during the transmission of the payment card data between various participants in the system. For this reason, early attempts to assign blame and shift costs are often misguided and policymakers should take heed of the fact that often the earliest reports are the least accurate. Additionally, policymakers should consider that there is no independent organization devoted to determining where a breach occurred, and who is to blame—these questions are often raised in litigation that can last for years. This is another reason why it is best to at least wait until the forensic analysis has been completed to determine what happened. Even then, there may be questions unanswered if the attack and technology used was sophisticated enough to cover the criminals' digital tracks.

The reality is that when a criminal breach occurs, particularly in the payments system, all of the businesses that participate in that system and their shared customers are victimized. Rather than resort to blame and shame, parties should work together to ensure that the breach is remedied and steps are taken to prevent future breaches of the same type and kind.

Legislative Solutions

In addition to the marketplace and technological solutions suggested above, NRF also supports a range of legislative solutions that we believe would help improve the security of our networked systems, ensure better law enforcement tools to address criminal intrusions, and standardize and streamline the notification process so that consumers may be treated equally across the Nation when it comes to notification of data security breaches.

NRF supports the passage by Congress of the bipartisan "Cyber Intelligence Sharing and Protection Act" (H.R. 624) so that the commercial sector can lawfully share information about cyber-threats in real-time and enable companies to defend their own networks as quickly as possible from cyber-attacks as soon as they are detected elsewhere by other business.

We also support legislation that provides more tools to law enforcement to ensure that unauthorized network intrusions and other criminal data security breaches are

thoroughly investigated and prosecuted, and that the criminals that breach our systems to commit fraud with our customers' information are swiftly brought to justice.

Finally, and for nearly a decade, NRF has supported passage of legislation that would establish one, uniform Federal breach notification law that would be modeled on, and preempt, the varying breach notification laws currently in operation in 46 States, the District of Columbia and Federal territories. A Federal law could ensure that all entities handling the same type of sensitive consumer information, such as payment card data, are subject to the same statutory rules and penalties with respect to notifying consumers of a breach affecting that information, Further, a preemptive Federal breach notification law would allow retailers and other businesses that have been victimized by a criminal breach to focus their resources on remedying the breach and notifying consumers rather than hiring outside legal assistance to help guide them through the myriad and sometimes conflicting set of 50 data breach notification standards in the State and Federal jurisdictions. Additionally, the use of one set of standardized notice rules would permit the offering to consumers of the same notice and the same rights regardless of where they live.

Conclusion

In closing three points are uppermost.

First, retailers take the increasing incidence of payment card fraud very seriously. We do so as Main Street members of the community, because it affects our neighbors and our customers. We do so as businesses, because it affects the bottom line. Merchants already bear at least an equal, and often a greater, cost of fraud than any other participant in the payment card system. We have every reason to want to see fraud reduced, but we have only a portion of the ability to make that happen. We did not design the system; we do not configure the cards; we do not issue the cards. We will work to effectively upgrade the system, but we cannot do it alone.

Second, the vast majority of breaches are criminal activity. The hacked party, whether a financial institution, a card network, a processor, a merchant, a governmental institution, or a consumer is the victim of a crime. Traditionally, we don't blame the victim of violence for the resulting stains; we should be similarly cautious about penalizing the hackee for the hack. The payment system is complicated. Every party has a role to play; we need to play it together. No system is invulnerable to the most sophisticated and dedicated of thieves. Consequently, eliminating all fraud is likely to remain an aspiration. Nevertheless, we will do our part to help achieve that goal.

Third, it is long past time for the United States to adopt PIN and chip card technology. The PIN authenticates and protects the consumer and the merchant. The chip authenticates the card to the bank. If the goal is to reduce fraud we must, at a minimum, do both.

PREPARED STATEMENT OF EDMUND MIERZWINSKI

CONSUMER PROGRAM DIRECTOR, U.S. PIRG

FEBRUARY 3, 2014

Chairman Warner, Senator Kirk, Members of the Committee, I appreciate the opportunity to testify before you on the important matter of consumer data security. Since 1989, I have worked on data privacy issues, among other financial system issues, for the U.S. Public Interest Research Group. The State PIRGs are nonprofit, nonpartisan public interest advocacy organizations that take on powerful interests on behalf of their members.

Summary:

The authoritative Privacy Rights Clearinghouse has estimated that since 2005, 663,182,386 records have been breached in a total of 4,163 separate data breaches.[1] The latest exploit against Target Stores, depending on how it is measured, is among the largest ever.

Target should be held accountable for its failure to comply with applicable security standards but that does not mean it is 100 percent responsible for this breach. Merchants, and their customers, have been forced by the card monopolies to use an unsafe payment card system that relies on obsolete magnetic stripe technology. When the technology was used only for safer credit cards, this may have been acceptable, but since the banks and card networks have also aggressively promoted the use of debit cards on the unsafe signature (not safer PIN) based platform, consumer bank accounts have also been placed at risk.

Congress should carefully weigh its response to the breach. Increasing consumer protections under the Electronic Funds Transfer Act (EFTA), which applies to debit cards, to the gold standard levels of the Truth In Lending Act, which applies to credit cards, should be the first step. Facing higher liability may "focus the mind" of the banks on improving security. Second, Congress should not preempt the strongest State breach notification laws, especially with a Federal breach law that may include a Trojan Horse preemption provision eliminating not only State breach laws, but all future State actions to protect privacy. That's the wrong response as we discuss below. Finally, Congress should also investigate the deceptive marketing of subscription-based credit monitoring and ID theft insurance products, which are over-priced and provide a false sense of security. In this case, although the highest risk to consumers is fraud on existing accounts, the modest credit monitoring product offered (for free) to Target customers will at best warn that you have become an identity theft victim. We make additional recommendations in the testimony below and are at all times available to brief Committee staff or members.

The Target Breach:

The card information acquired in the first 40 million breached accounts that Target reported placed those debit/ATM or credit card customers at ***risk of fraud on their existing accounts.*** Because the scope of the records acquired in that RAM-scraping incident included not only the card number but also the expiration date, 3-digit security code (from the back of the card) and the (encrypted but probably hackable) PIN number or password, these numbers became very valuable on the underground market, as the Secret Service has already explained.

Target's later admission that additional information—including telephone numbers and email addresses—for up to a total of 70–110 million consumer records (some may have been the same consumers) held in a Customer Relations Management (CRM) database was also obtained, placed those customers ***at the risk of new account identity theft.*** Criminals will seek to obtain additional information, such as a consumer's Social Security Number, which would enable them to submit false applications for credit in your name.

When bad guys obtain emails and phone numbers, they make phishing attacks to obtain more information: While the emails and phone numbers are not enough information to commit identity theft, it is enough information to conduct such "phishing attacks" designed to collect additional information, including Social Security Numbers and encrypted passwords, from consumers.

They do this either through placing dangerous links in emails or various "social engineering" techniques to trick you into providing more information. A phishing email will appear to be from your bank. But if you click on any links, either a virus explodes on your computer to collect any personal information stored on it, or you are redirected to a site that will allow them to obtain the information they need.

---

[1] *See* "Chronology of Data Breaches," Privacy Rights Clearinghouse, last visited 30 January 2014: *https://www.privacyrights.org/data-breach.*

Or, if they call you, they use the information that they have as a validation that they are from the bank, to trick you into providing the information that they need. The additional information the bad guys seek, then, would either allow them direct access to your account (through the PIN) or to open new accounts in your name (with your Social Security Number) by committing identity theft. They use what they know to convince you to tell them what they don't know. They want your PIN, or your birth date and Social Security Number. They hope to trick you into giving it up.

However, I believe the greater risk in this case is fraud on existing accounts, not identity theft. That is why so many banks re-issued debit and credit cards, or both, following the incident. But disappointingly, Target's main response to consumers—offering a free credit monitoring service—won't stop or warn of fraud on existing accounts. That provides consumers a false sense of security.[2]

It actually won't even stop identity theft, it will simply notify you after the fact of changes to your Experian credit report (but not to your Trans Union or Equifax reports, which may include different account information). Positively, the offered product terminates after 1 year, rather than auto-renewing for a monthly fee (when similar products were offered after some previous breaches, the over-priced, under-performing credit monitoring products were sometimes set to auto-renew for a fee).

Despite my reservations about Target's delayed and drawn out notifications to customers about the breach,[3] and its provision of the inadequate credit monitoring product, I don't believe that Target or other merchants deserve all of the blame for the data breaches that occur on their watch.

The card networks are largely at fault. They have continued to use an obsolete 1970s magnetic stripe technology well into the 21st century. When the technology was solely tied to credit cards, where consumers enjoy strong fraud rights and other consumer protections by law, this may have been barely tolerable.

But when the big banks and credit card networks asked consumers to expose their bank accounts to the unsafe signature-based payment system, by piggybacking once safer PIN-only debit cards onto the signature-based system, the omission became unacceptable. The vaunted "zero-liability" promises of the card networks and issuing banks are by contract, not law. Of course, the additional problem any debit card fraud victim faces is that she is missing money from her own account while the bank conducts an allowable reinvestigation for 10 days or more, even if the bank eventually lives up to its promise.[4]

Further, the card networks' failure to upgrade, let alone enforce, their PCI or security standards, despite the massive revenue stream provided by consumers and merchants through swipe, or interchange, fees, is yet another outrage by the banks and card networks.

Incredibly, the Federal Reserve Board's rule interpreting the Durbin amendment limiting swipe fees on the debit cards of the biggest banks also provides for additional fraud revenue to the banks in several ways. Even though banks and card networks routinely pass along virtually all costs of fraud to merchants in the form of chargebacks, the Fed rule interpreting the Durbin amendment allows for much more revenue. So, not only are banks and card networks compensated with general revenue from the ever-increasing swipe fees, but the Fed allows them numerous additional specific bites of the apple for fraud-related fees.

To be sure, Target should be held accountable if it turns out, as has been reported, that it was not in compliance with the latest and highest level of security standards throughout its system. But understand that that system was inadequate at best because, like acting as any monopolists would, the card duopoly refused to make adequate technological improvements to its system, preferring to extract excess rents for as long as possible. For that reason, I cannot endorse any reform that makes Target, or other merchants, the only ones at blame. In many ways, the merchants are as much victims of the banks' unsecure systems as consumers are.

Recommendations:

1) **Congress should improve debit/ATM card consumer rights and make all plastic equal:**

---

[2] Even worse, consumers who accept the monitoring product, ProtectmyID from the credit bureau Experian, must accept a boilerplate forced arbitration clause that restricts their ability to sue Experian. *See http://www.protectmyid.com/terms/*. And under current U.S. Supreme Court jurisprudence, that clause's outrageous ban on joining a class action is also permissible.

[3] I understand that some State Attorneys General are investigating whether adequate notification was made under their breach laws.

[4] Compare some of the Truth In Lending Act's robust credit card protections by law to the Electronic Funds Transfer Act's weak debit card consumer rights at this FDIC Web site: *http://www.fdic.gov/consumers/consumer/news/cnfall09/debit_vs_credit.html.*

Up until now, both banks and merchants have looked at fraud and identity theft as a modest cost of doing business and have not protected the payment system well enough. They have failed to look seriously at harms to their customers from fraud and identity theft—including not just monetary losses and the hassles of restoring their good names, but also the emotional harm that they must face as they wonder whether future credit applications will be rejected due to the fraudulent accounts.

Currently, debit card fraud victims are reimbursed at "zero liability" only by promise. The EFTA's fraud standard actually provides for 3-tiers of consumer fraud losses. Consumers lose up to $50 if they notify the bank within 2 days of learning of the fraud, up to $500 if they notify the bank within 60 days and up to their entire loss, including from any linked accounts, if they notify the bank after 60 days. However, if the physical debit card itself is not lost or stolen, consumers are not liable for any fraud charges if they report them within 60 days of their bank statement.

This shared risk fraud standard under the EFTA, which governs debit cards, appears to be vestigial, or left over from the days when debit cards could only be used with a PIN. Since banks encourage consumers to use debit cards, placing their bank accounts at risk, on the unsafe signature debit platform, this fraud standard should be changed.

As a first step, Congress should institute the same fraud cap, $50, on debit/ATM cards as exists on credit cards. (Or, even eliminate the cap of $50 in all cases, since it is never imposed.) Congress should also provide debit and prepaid card customers with the stronger billing dispute rights and rights to dispute payment for products that do not arrive or do not work as promised that credit card users enjoy (through the Fair Credit Billing Act, a part of the Truth In Lending Act).[5]

Debit/ATM card customers already face the aforementioned cash-flow and bounced check problems while banks investigate fraud under the Electronic Funds Transfer Act. Reducing their possible liability by law, not simply by promise, won't solve this particular problem, but it will force banks to work harder to avoid fraud. If they face greater liability to their customers and account holders, they will be more likely to develop better security.

2) Congress should not endorse a specific technology, such as EMV (parent technology of Chip and PIN and Chip and Signature). If Congress takes steps to encourage use of higher standards, its actions should be technology-neutral and apply equally to all players.

Chip and PIN and CHIP and signature are variants of the EMV technology standard commonly in use in Europe. The current pending U.S. rollout of chip cards will allow use of the less-secure Chip and Signature cards rather than the more-secure Chip and PIN cards. Why not go to the higher Chip and PIN authentication standard immediately and skip past Chip and Signature? As I understand the rollout schedule, there is still time to make this improvement.

This example demonstrates why Congress should not embrace a specific technology. Instead, it should take steps to encourage all users to use the *highest possible* existing standard. Congress should also take steps to ensure that additional technological improvements and security innovations are not blocked by actions or rules of the existing players.

If Congress does choose to impose higher standards, then it must impose them equally on all players. For example, current legislative proposals may unwisely impose softer regimes on financial institutions subject to the weaker Gramm-Leach-Bliley rules than to merchants and other nonfinancial institutions.

Further, as most observers are aware, chip technology will only prevent the use of cloned cards in card-present (Point-of-Sale) transactions. It is an improvement over obsolete magnetic stripe technology in that regard, yet it will have no impact on online transactions, where fraud volume is much greater already than in point-of-sale transactions. Experiments, such as with "virtual card numbers" for one-time use, are being carried out online. It would be worthwhile for the Committee to inquire of the industry and the regulators how well those experiments are proceeding and whether requiring the use of virtual card numbers in all online debit and credit transactions should be considered a best practice.

Further, as I understand it, had Chip and PIN (or Chip and Signature) been in use, it would not have stopped the Target breach, since unencrypted information

[5] For a detailed discussion of these problems and recommended solutions, *see* Hillebrand, Gail (2008) "Before the Grand Rethinking: Five Things to Do Today with Payments Law and Ten Principles to Guide New Payments Products and New Payments Law," Chicago-Kent Law Review: Vol. 83, Iss. 2, Article 12, *available at http://scholarship.kentlaw.iit.edu/cklawreview/vol83/iss2/12.*

was collected from the Target system's internal RAM memory, after the cards had already been used.

3) Investigate card security standards bodies and ask the prudential regulators for their views:

To ensure that improvements continue to be made in the system, the Committee should also inquire into the governance and oversight of the development of card network security standards. Do regulators sit on the PCI board? As I understand it, merchants do not; they are only allowed to sit on what may be a meaningless "advisory" board. Further, do regulators have any mandatory oversight function over standards body rules?

Recently, the networks have been in to see the Federal Reserve Board ostensibly to talk about interchange fees. Since the Fed is not a witness today, the Committee should ask the Fed and other prudential regulators about these matters at its pending Oversight hearing on these matters later this week. In particular, ask the Fed to testify as to the purposes and discussions at these meetings. Its summary of one of these meetings indicates that the issue was EMV (CHIP card technology) rollout:

> Summary (Meeting Between Federal Reserve Board Staff and Representatives of Visa, January 8, 2014): Representatives of Visa met with Federal Reserve Board staff to discuss their observations of market developments related to the deployment of EMV (*i.e.,* chip-based) debit cards in the United States. Topics discussed included an overview of their current EMV roadmap and Visa's proposed common application for enabling multiple networks on an EMV card while preserving merchant routing and choice.[6]

4) Congress should *not* enact any new legislation sought by the banks to impose their costs of replacement cards on the merchants:

Target should pay its share but this breach was not entirely Target's fault. The merchants are forced to use an obsolete and unsafe system designed by the banks and card networks, which, to make matters worse, don't uniformly enforce their additional often-changing security standards intended to ameliorate the flaws in the underlying platform. Disputes over costs of replacement cards should be handled by contracts and agreements between the players. How could you possibly draft a bill to address all the possible shared liabilities?

Of course, the Federal Reserve has already allowed compensation to banks for card replacement in circumstances where the Fed's Durbin amendment rule applies. It states:

"Costs associated with research and development of new fraud-prevention technologies, card reissuance due to fraudulent activity, data security, card activation, and merchant blocking are all examples of costs that are incurred to detect and prevent fraudulent electronic debit transactions. Therefore, the Board has included the costs of these activities in setting the fraud prevention adjustment amount to the extent the issuers reported these costs in response to the survey on 2009 costs."[7]

Under the Fed's Durbin rules the amount of this compensation is as follows: banks can also get 5 basis points per transaction for fraud costs, 1.2 cents per transaction for transaction monitoring, and 1 cent per transaction for the fraud prevention adjustment. Again, this is in addition to merchants already paying chargebacks for fraud as well as PCI violation fines, plus litigation damages.

5) Congress should *not* enact any Federal breach law that preempts State breach laws or, especially, preempts other State data security rights:

In 2003, when Congress, in the FACT Act, amended the Fair Credit Reporting Act, it specifically did not preempt the right of the States to enact stronger data security and identity theft protections.[8] We argued that since Congress hadn't solved all the problems, it shouldn't prevent the States from doing so.

From 2004–today, 46 States enacted security breach notification laws and 49 State-enacted security freeze laws. Many of these laws were based on the CLEAN

---

[6] *Available at http://www.federalreserve.gov/newsevents/rr-commpublic/pin-debit-networks-20131107.pdf.*

[7] *See* 77 Fed. Reg. page 46264 (August 3, 2012), *available at http://www.gpo.gov/fdsys/pkg/FR-2012-08-03/pdf/2012-18726.pdf.*

[8] *See* "conduct required" language in Section 711 of the Fair and Accurate Credit Transactions Act of 2003, Public Law 108–159. Also *see* Hillebrand, Gail, "After the FACT Act: What States Can Still Do to Prevent Identity Theft," Consumers Union, 13 January 2004, *available at http://consumersunion.org/research/after-the-fact-act-what-states-can-still-do-to-prevent-identity-theft/.*

Credit and Identity Theft Protection Model State Law developed by Consumers Union and U.S. PIRG.[9]

A security freeze, not credit monitoring, is the best way to prevent identity theft. If a consumer places a security freeze on her credit reports, a criminal can apply for credit in her name, but the new potential creditor cannot access your "frozen" credit report and will reject the application. The freeze is not for everyone, since you must unfreeze your report on a specific or general basis whenever you re-enter the credit marketplace, but it is only way to protect your credit report from unauthorized access. *See* this footnoted Consumers Union page for a list of security freeze rights.[10]

The other problem with enacting a preemptive Federal breach notification law is that industry lobbyists will seek language that not only preempts breach notification laws but also prevents States from enacting any future data security laws, despite the laudable 2003 FACT Act example above.

Simply as an example, S. 1927 (Carper) includes sweeping preemption language that is unacceptable to consumer and privacy groups and likely also to most State Attorneys General:

> **SEC. 7. RELATION TO STATE LAW.**
>
> No requirement or prohibition may be imposed under the laws of any State with respect to the responsibilities of any person to——
>
> (1) protect the security of information relating to consumers that is maintained or communicated by, or on behalf of, the person;
>
> (2) safeguard information relating to consumers from potential misuse;
>
> (3) investigate or provide notice of the unauthorized access to information relating to consumers, or the potential misuse of the information, for fraudulent, illegal, or other purposes; or
>
> (4) mitigate any loss or harm resulting from the unauthorized access or misuse of information relating to consumers.

Other bills before the Congress include similar, if not even more sweeping, abuses of our Federal system, despite that at least one merchant I have spoken with told me: "Actually, Ed, it is relatively easy to comply with the different State breach laws. We haven't had a problem."

Such broad preemption will prevent States from acting as first responders to emerging privacy threats. Congress should not preempt the States. In fact, Congress should think twice about whether a Federal breach law that is weaker than the best State laws is needed at all.

6) Congress should allow for private enforcement and broad State and local enforcement of any law it passes:

The marketplace only works when we have strong Federal laws and strong enforcement of those laws, buttressed by State and local and private enforcement.

Many of the data breach bills I have seen specifically state no private right of action is created. Such clauses should be eliminated and it should also be made clear that the bills have no effect on any State private rights of action. Further, no bill should include language reducing the scope of State Attorney General or other State-level public official enforcement. Further, any Federal law should not restrict State enforcement only to State Attorneys General.

For example, in California not only the State Attorney General but also county District Attorneys and even city attorneys of large cities can bring unfair practices cases.

Although we currently have a diamond age of Federal enforcement, with strong but fair enforcement agencies including the CFPB, OCC and FDIC, that may not always be the case. By preserving State remedies and the authority of State and local enforcers, you can better protect your constituents from the harms of fraud and identity theft.

7) Any Federal breach law should not include any "harm trigger" before notice is required:

The better State breach laws, starting with California's, require breach notification if information is presumed to have been "acquired." The weaker laws allow the company that failed to protect the consumer's information in the first place to decide

---

[9] *See http://consumersunion.org/wp-content/uploads/2013/02/model.pdf.*

[10] *http://defendyourdollars.org/document/guide-to-security-freeze-protection.*

whether to tell them, based on its estimate of the likelihood of identity theft or other harm.

Only an acquisition standard will serve to force data collectors to protect the financial information of their trusted customers, account holders or, as Target calls them, "guests," well enough to avoid the costs, including to reputation, of a breach.

8) Congress should further investigate marketing of overpriced credit monitoring and identity theft subscription products:

In 2005 and then again in 2007 the FTC imposed fines on the credit bureau Experian for deceptive marketing of its various credit monitoring products, which are often sold as add-ons to credit cards and bank accounts. Prices range up to $19.99/month. While it is likely that recent CFPB enforcement orders [11] against several large credit card companies for deceptive sale of the add-on products—resulting in recovery of approximately $800 million to aggrieved consumers—may cause banks to think twice about continuing these relationships with third-party firms, the Committee should also consider its own examination of the sale of these credit card add-on products.

In addition to profits from credit monitoring, banks and other firms reap massive revenues from ID Theft insurance, sometimes sold in the same package and sometimes sold separately. Companies that don't protect our information as the law requires add insult to injury by pitching us over-priced monitoring and insurance products. The Committee should call in the companies that provide ID theft insurance and force the industry to open its books and show what percentage of premiums are paid out to beneficiaries. It is probable that the loss ratio on these products is so low as to be meaningless, meaning profits are sky-high.

Consumers who want credit monitoring can monitor their credit themselves. No one should pay for it. You have the right under Federal law to look at each of your 3 credit reports (Equifax, Experian and TransUnion) once a year for free at the federally mandated central site *annualcreditreport.com.* Don't like Web sites? You can also access your Federal free report rights by phone or email. You can stagger these requests—1 every 4 months—for a type of do-it-yourself no-cost monitoring. And, if you suspect you are a victim of identity theft, you can call each bureau directly for an additional free credit report. If you live in Colorado, Georgia, Massachusetts, Maryland, Maine, New Jersey, Puerto Rico or Vermont, you are eligible for yet another free report annually under State law by calling each of the Big 3 credit bureaus.

Although Federal authority against unfair monitoring marketing was improved in the 2009 Credit CARD Act,[12] the Committee should also ask the regulators whether any additional changes are needed.

9) Review Title V of the Gramm-Leach-Bliley Act and its data security requirements:

The 1999 Gramm-Leach-Bliley Act imposed data security responsibilities on regulated financial institutions, including banks. The requirements include breach notification in certain circumstances.[13] The Committee should ask the regulators for information on their enforcement of its requirements and should determine whether additional legislation is needed. The Committee should also recognize, as noted above, that compliance with GLBA should not constitute constructive compliance with any additional security duties imposed on other players in the card network system as that could lead to a system where those other nonfinancial-institution players are treated unfairly.

10) Congress should investigate the over-collection of consumer information for marketing purposes. More information means more information at risk of identity theft. It also means there is a greater potential for unfair secondary marketing uses of information:

In the Big Data world, companies are collecting vast troves of information about consumers. Every day, the collection and use of consumer information in a virtually unregulated marketplace is exploding. New technologies allow a web of inter-

---

[11] We discuss some of the CFPB cases here *http://www.uspirg.org/news/usp/cfpb-gets-results-orders-chase-bank-repay-consumers-over-300-million-over-sale-junky-credit.*

[12] The Credit Card Accountability, Responsibility and Disclosure (CARD) Act of 2009, Public Law 111–24. *See* Section 205.

[13] *See* the Federal Financial Institutions Examination Council's "Final Guidance on Response Programs: Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," 2005, *available at http://www.fdic.gov/news/news/financial/2005/fil2705.html.*

connected businesses—many of which the consumer has never heard of—to assimilate and share consumer data in real-time for a variety of purposes that the consumer may be unaware of and may cause consumer harm. Increasingly, the information is being collected in the mobile marketplace and includes a new level of localized information.

Although the Fair Credit Reporting Act limits the use of financial information for marketing purposes and gives consumers the right to opt-out of the limited credit marketing uses allowed, these new Big Data uses of information may not be fully regulated by the FCRA. The development of the Internet marketing ecosystem, populated by a variety of data brokers and advertisers buying and selling consumer information without their knowledge and consent, is worthy of Congressional inquiry.[14]

Thank you for the opportunity to provide the Committee with our views. We are happy to provide additional information to Members or staff.

PREPARED STATEMENT OF TROY LEACH

CHIEF TECHNOLOGY OFFICER, PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL

FEBRUARY 3, 2014

Introduction

Chairman Warner, Ranking Member Kirk, Members of the Subcommittee, on behalf of the PCI Security Standards Council, thank you for inviting us to testify today before the Subcommittee.

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

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

The PCI Security Standards Council is an excellent example of effective industry collaboration to develop private sector standards. Simply put, the PCI Standards are the best line of defense against the criminals seeking to steal payment card data. And while several recent high profile breaches have captured the Nation's attention, great progress has been made over the past 7 years in securing payment card data, through a collaborative cross-industry approach, and we continue to buildupon the way we protect this data.

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

Payment card security: a dynamic environment

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

---

[14] *See* the FTC's March 2012 report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers," *available at http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.* Also *see* Edmund Mierzwinski and Jeff Chester, "Selling Consumers Not Lists: The New World of Digital Decision-Making and the Role of the Fair Credit Reporting Act," 46 Suffolk University Law Review Vol. 3, page 845 (2013), also *available at http://suffolklawreview.org/selling-consumers-not-lists/.*

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

The Council develops standards through a defined, *published* 3-year lifecycle. Our Participating Organization *members told us* that 3 years was the appropriate timeframe to update and deploy security approaches in their organizations. In addition to the formal lifecycle, the Council and the PCI community have the resources to continually monitor and provide updates through standards, published FAQs, Special Interest Group work, and guidance papers on emerging threats and new ways to improve payment security. Examples include updated *wireless guidance* and security guidelines for merchants wishing to *accept mobile payments.*

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

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

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

In addition to developing and updating standards, every year the PCI community votes on which topics they would like to explore with the Council and provide guidance on. Over the last few years the working groups formed by the Council to address these concerns have drawn hundreds of organizations to collaborate together to produce resources on third party security assurance, cloud computing, best practices for maintaining compliance, e-commerce guidelines, virtualization, and wireless security. Other recent Council initiatives have addressed ATM security, PIN security, and mobile payment acceptance security for developers and merchants.

EMV Chip & PCI Standards—a strong combination

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

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

Payment cards are used in variety of remote channels—such as electronic commerce—where today's EMV chip technology is not typically an option for securing payment transactions. Security innovation continues to occur for online payments beyond existing fraud detection and prevention systems. Technologies such authen-

tication, tokenization, and other frameworks are being developed, including some solutions that may involve EMV chip—yet broad adoption of these solutions is not on the short-term horizon. Consequently, the industry needs to continue to protect cardholder data across all payment channels to minimize the ongoing risks of data loss and resulting cross-channel fraud such as may be experienced in the online channel.

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

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

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

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

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

Beyond Standards—building a support infrastructure

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

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

To help organizations improve payment data security, the Council takes a holistic approach to securing payment card data, and its work encompasses both PCI Standards development and maintenance of programs that support standards implementation across the payment chain. The Council believes that providing a full suite of tools to support implementation is the most effective way to ensure the protection of payment card data. To support successful implementation of PCI Standards, the Council maintains programs that certify and validate certain hardware and software products to support payment security. For example, the Council wants to make it easy for merchants and financial institutions to deploy the latest and most secure terminals and so maintains a *public listing on its Web site* for them to consult before purchasing products. We realize it takes time and money to upgrade POS terminals and we encourage businesses that are looking to upgrade for EMV chip to consider

other necessary security measures by choosing a POS terminal from this list. Similarly, we are supporting the adoption of point-to-point encryption, and listing appropriate solutions on our Web site to take a solutions-oriented approach to helping retailers more readily implement security in line with the PCI standards.

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

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

The work of the Council covers the entire payment security environment with the goal of providing or facilitating access to all the tools necessary—standards, products, assessors, educational resources, and training—for stakeholders to successfully secure payment card data. We do this because we believe that no one technology is a panacea and effective security requires a multi-layered approach.

Public-private collaboration

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

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

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

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

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

Conclusion

In 2011, the Ponemon Institute, a nonpartisan research center dedicated to privacy, data protection, and information security policy wrote, "The Payment Card In-

dustry Data Security Standard (PCI DSS) continues to be one of the most important regulations for all organizations that hold, process or exchange cardholder information."

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

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

There is no time to waste. The PCI Security Standards Council and business must commit to promoting stronger security protections while Congress leads efforts to combat global cyber-crimes that threaten us all. We thank the Committee for taking an important leadership role in seeking solutions to one of the largest security concerns of our time.

RESPONSE TO WRITTEN QUESTIONS OF SENATOR KIRK FROM JESSICA RICH

Q.1. Banks are bound by regulations (the Graham-Leach-Bliley Act and Reg. E to name a few) regarding how to store consumer data, and are regularly examined by Federal regulators to ensure ongoing and accurate compliance. Regulators have a number of enforcement mechanisms in place to deal with banks found to be noncompliant, such as requiring prompt corrective action for material violations—even before a breach occurs. What are the rules binding merchants to protect consumer information? How are they monitored and enforced?

A.1. The FTC enforces Section 5 of the FTC, which Act prohibits unfair or deceptive acts or practices. A company acts deceptively if it makes materially misleading statements or omissions about data security, and such statements or omissions are likely to mislead reasonable consumers. Further, a company engages in unfair acts or practices if its data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition. The FTC can bring an enforcement action against a company engaged in deceptive or unfair practices, either through administrative adjudication or in Federal district court. Through these mechanisms, the FTC can obtain injunctive relief, such as prohibitions on misrepresentations, additional disclosures, implementation of comprehensive data security programs, and outside third party audits.

Merchants may also be subject to other Federal laws that contain data security requirements. For example, the Fair Credit Reporting Act ("FCRA") imposes safe disposal obligations on any entity that maintains consumer report information. The FTC's Safeguards Rule, which implements the Gramm-Leach-Bliley Act, requires certain nonbank financial institutions to implement a comprehensive information security program. And, the Children's Online Privacy Protection Act ("COPPA") requires reasonable security for children's information collected online. In addition to the injunctive relief discussed above, the FTC can also seek civil penalties against merchants violating the FCRA and COPPA. To date, the Commission has settled 50 data security cases using its authority.

Beyond Federal laws, State data security and breach notification laws may place additional requirements on merchants. And, merchants may also be subject to self-regulatory standards that place additional security requirements on data they maintain.

Q.2. There has been a 30 percent increase in data breaches from 2012 to 2013. Clearly, these criminals are getting more sophisticated—but because the majority of these breaches are occurring within the healthcare space and with retailers, is there reason to believe more should be done in these spaces to protect consumers?

A.2. Yes—companies should ensure that they have sound information security practices. They can start by doing a thorough risk assessment of their security practices for managing personal information and then designing a security program to control and limit these risks. This should be done in all areas of a company's operations and not just its computer networks. Many breaches we have seen have not involved high-tech hacking or other sophisticated techniques. Some occurred because companies did not do background checks on employees with access to personal information, did not manage the termination of an employee well, or did not properly secure or dispose of paper records. In other cases, companies have failed to implement basic technical security measures such as requiring strong passwords, encrypting sensitive information, or updating security patches.

The Commission's Safeguards Rule under the Gramm-Leach-Bliley Act provides a good roadmap as to the procedures and basic elements necessary to develop a sound security program. Although it applies only to nonbank financial institutions, we believe it provides helpful guidance to other companies as well.

Finally, as discussed in more detail below, enacting a Federal data security and data breach notification law would help to ensure better data security practices, primarily by imposing civil penalties against companies that do not maintain reasonable security or do not send appropriate breach notices to consumers. Civil penalties can help further deter lax data security and breach notification practices.

Q.3. What additional authorities—such as additional monitoring, increased penalties for noncompliance, *etc.*—should we give to the FTC have to be more effective?

A.3. The FTC supports Federal legislation that would (1) strengthen its existing authority governing data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach. Legislation in both areas—data security and breach notification—should give the FTC the ability to seek civil penalties to help deter unlawful conduct, rulemaking authority under the Administrative Procedure Act, and jurisdiction over nonprofits. Under current laws, the FTC only has the authority to seek civil penalties for data security violations with regard to children's online information under COPPA or credit report information under the FCRA. To help ensure effective deterrence, we urge Congress to allow the FTC to seek civil penalties for all data security and breach notice violations in appropriate circumstances. Likewise, enabling the FTC to bring cases against nonprofits, such as universities and health systems, would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it. Finally, rulemaking authority under the Administrative Procedure Act would enable the FTC to respond to changes in technology in implementing the legislation.

Q.4. Do you feel that having a Merchant ISAC would be helpful in ensuring information about malware is quickly communicated to retail groups and others so that additional precautions can be taken?

A.4. In light of the recent data breaches at a number of large retailers, this is a particularly appropriate time to evaluate whether more can be done to secure consumers' information. Better information sharing, such as through ISACs, can be part of the solution. ISACs enable companies to pool information about security threats and defenses so that they can prepare for new attacks and quickly address potential vulnerabilities. This kind of information is valuable, and we are committed to working with retail businesses and associations to discuss these issues and to explore the formation of a Merchant ISAC, or similar organization.

RESPONSE TO WRITTEN QUESTIONS OF SENATOR KIRK FROM JAMES A. REUTER

Q.1. I understand that large banks and payment networks see and stop illegal attempts to intercept customer information on a daily basis. What have banks done to invest in keeping ahead of the criminals and what is the relationship with law enforcement to investigate and prosecute these crimes?

A.1. According to the American Bankers Association's (ABA's) most recent Deposit Account Fraud Survey and other benchmarking data, while fraud against bank deposit accounts cost the industry $1.744 billion in losses in 2012, bank prevention measures stopped approximately $13 billion in fraudulent transactions during that year. The fact that, in 2012, banks prevented over $7 in fraud for every $1 in actual fraud losses that occurred speaks to the substantial investment banks have made in counteracting attempts to compromise customer information or conduct unauthorized transactions against customer accounts.

In addition to individual institution efforts, banks collaborate, through the Financial Services Information Sharing and Analysis Center (FS–ISAC) to share vital cybersecurity threat and vulnerability information. Over 4,500 companies currently belong to the FS–ISAC. The ABA serves on the board of the Center on behalf of its membership, and in that capacity ensures that this information is also available to the broader financial community that the Association represents.

Banks are also currently investing, through the FS–ISAC, in an effort to automate that evaluation of threat data to the greatest extent possible. This initiative is consistent with the recently published NIST Cybersecurity Framework, which noted that the automated sharing of indicator information can provide organizations with timely, actionable information that they can use to detect and respond to cybersecurity events as they are occurring.

On February 13, 2014, ABA and other major financial institution trade associations announced a significant initiative with major merchant trade associations to work together to ensure customer personal and financial information is secure and protected. The partnership will focus on exploring paths to increased information sharing, better card security technology, and maintaining the trust of customers.

Banks have a strong relationship, at both the local and national levels, with law enforcement in the investigation and prosecution of cyber-crimes. The fact that many of the criminals are attacking

our banks and customers from overseas does, however, make prosecution difficult. As an industry we are heartened by the FBI's commitment to staffing offices in foreign countries, and we encourage Congress to support these efforts.

Q.2. How much does it cost to replace a single debit or credit card? How much does your bank expect to lose from the most recent Target data breach—including losses for both card replacement and for fraud?

A.2. After a breach of a third party affecting customer card data, each bank makes its own decision as to when and whether to reissue cards, which in the case of FirstBank costs on average $5 per card.

In addition to replacing the actual card, banks incur a number of other expenses associated with breaches of third parties, including sending notices to customers, increasing call center staffing, and monitoring for potential fraud. In some instances, losses due to fraud from the breach of a third party can occur many months after the breach occurred. Because of the sheer magnitude of the Target breach, impacting on average 10 percent of the retail customer base of every bank in the country, many banks, including FirstBank, made the decision to reissue cards to all customers that shopped at Target during the period the company's point-of-sale system was compromised. This swift action on the part of our and other banks should serve to limit fraud losses due to the breach.

Q.3. What recourse is available to community banks such as yours for these breaches? How much do you typically recoup from these breaches? Is 5 to 10 cents on the dollar a fairly good estimate?

A.3. After a bank has reimbursed a customer for a fraudulent transaction, it can then attempt to "chargeback" the retailer where the transaction occurred. Unfortunately, and certainly in my experience, the majority of these attempts are unsuccessful, with the bank ultimately shouldering the vast majority of fraud loss and other costs associated with the breach. In 2009, according to the Federal Reserve Board, 62 percent of reported debit card fraud losses were borne by banks, while 38 percent were borne by merchants.

Five to 10 cents on the dollar is a good estimate of what a community bank will typically recoup from the breach of a third party. And this reimbursement generally occurs often well after these banks have made customers whole. This minor level of reimbursement, when taken in concert with the fact that banks bear over 60 percent of reported fraud losses yet have accounted for less than 8 percent of reported breaches since 2005 is clearly inequitable.

Q.4. Are smaller banks more negatively and unfairly impacted in these payments? I am sure that, because this recourse is determined by contracts drafted by PCI and others, the larger banks might expect to get more back but the smaller banks often see nothing returned.

A.4. The experience of ABA members is that banks of all sizes are uniformly negatively and unfairly impacted by these payments. Large and small banks alike receive pennies for each dollar of

fraud losses and other costs that were incurred by banks in protecting their customers.

Q.5. I also understand that there are a number of smaller, lower-profile breaches, and in those, in most instances, a community bank can expect to receive nothing back. Correct?

A.5. In the case of smaller, lower-profile breaches, unless enough information is known about the time period associated with the breach and the specific cards that were compromised, it may be difficult to attribute individual transactions a customer deemed unauthorized to that breach. In those instances the experience of both small and large banks is that very little, if any reimbursement for fraud losses and other costs will occur.

RESPONSE TO WRITTEN QUESTIONS OF SENATOR KIRK FROM MALLORY DUNCAN

Q.1. What is the retailers' strategy to combat online fraud?

A.1. Online fraud may take many forms; some of these involve payment card fraud. The payment cards in use in the United States were designed for face-to-face transactions. The authentication of the card is generally based on verifying the numbers (and sometimes the codes) printed visibly on the card or embedded in a magnetic stripe. Authentication of the cardholder is premised on verifying the signature and occasionally on some corroborating data. In an ideal face-to-face transaction, the card is observed and the signed receipt results in a perfect match for the signature on the card. This is the customer authentication. In addition, the card's numbers are transmitted to the issuing bank which supplies an approval code to accomplish the former—the card authentication. If the media involved in the transaction is saved for some months by the retailer for use in subsequent retrieval requests, then the merchant is promised a "payment guarantee" by the card networks. All elements, including the contemporaneously signed duplicate receipt containing identifying details and the approval code indication must be present for payment to be guaranteed.

U.S. cards were not designed for remote ("card not present") transactions. Card issuers are unwilling to allow the transaction to be authenticated solely by the unobservable card's number unless two conditions are met. First, the interchange fee charged for the transaction is higher—ostensibly to cover the greater risk of fraud. Second, the merchant is essentially required to bear all risks of fraud—*i.e.,* there effectively is no payment guarantee.

In the early days of online sales, merchants with a tiny online footprint—indeed many were literally one-store sellers—were willing to accept these conditions on the assumption that most purchasers were honest and that use of a card was more efficient than was use of a check, as had been common with mail order catalog sellers. As online sales grew and become more mainstream, these requirements stuck. Thus merchants generally bear virtually all of the risk of online fraud. The transaction can be "charged back" to them and the merchants will be out both the goods and the money.

Consequently, merchants have adopted numerous techniques to reduce their exposure to, and to combat, online fraud. For example,

many merchants will not ship online orders to nonphysical location addresses. This is because thieves often use "drop boxes" where they can retrieve fraudulently purchased merchandise without being readily observed. Thieves are less likely to have fraudulently procured goods delivered to their homes. Nevertheless, because some do, merchants' loss prevention departments develop lists of names and physical addresses that are known to receive fraudulent deliveries and will not routinely ship to those locations as well. Merchants may also monitor characteristics of online orders searching for those that are indicative of fraud and respond accordingly. In conjunction with card companies, merchants may request the customer verification number (CVV) that is printed, rather than embossed, on the payment card. This provides greater assurance that the card used for the transaction was in the physical possession of the individual placing the order, even if it does not authenticate the customer to the merchant.

These and other techniques have allowed merchants to restrain online fraud. If more fraud migrates to the 6 percent of purchases that are now online, either more robust techniques may be needed (*e.g.,* computers with built-in chip readers; open, competition-friendly tokenization technology; or new mobile payment platforms) or merchants may need to more stringently monitor, control and price the transactions in which they will engage.

The development of payment platforms in which the loss of fraud is more equitably shared by the proponents of the platform would give all parties incentives to reduce online fraud.

Q.2. It is already a requirement for merchants and banks to move to chip technologies by 2015. Currently, less than 1 percent of U.S. retailers have chip-compatible point-of-sale terminals. What percentage of retailers do you expect will switch to chip-ready terminals by the end of next year?

A.2. It is not required that either banks or merchants move to chip technologies by 2015. Rather, the card networks have said they will abrogate their promise of a payment guarantee, and not pay for fraud inherent in their system, if merchants do not do so by that date. In short, the card networks have told merchants to invest huge sums to correct problems with the card networks' payment system, but have provided no equitable sharing of the costs of that fix—only increased penalties for not doing so.

There are approximately 15 million payment terminals in the United States of which roughly 9 million are in retail locations. Of these, approximately 18 percent are chip-ready. Those merchants are hoping card networks will require, and banks will begin issuing, fraud resistant PIN and Chip authenticated credit and debit cards. Only one major bank has suggested that it plans to do so. It will be difficult to convince the remaining merchants to collectively invest tens of billions of dollars to purchase and install new terminals if most banks and credit unions continue issuing cards that do not address obvious fraud flaws in the current system—*i.e.,* if they continue issuing signature authenticated cards. There is considerable reluctance to spend hugeamounts of money to accomplish a half-baked solution.

Policy makers could help by discouraging the continued issuance of fraud prone cards.

Q.3. Why are NRF and other retail groups pushing for chip and PIN and not tokenization?

A.3. Retailers are not opposed to tokenization. Like point-to-point encryption, it is a potentially useful element in a more secure payment card system. Successful nationwide deployment would take years. Furthermore, in many models tokenization occurs "after the fact"—generally post authorization. Thus some fraud risk remains. To deal with this point-to-point encryption is preferred and would be complimentary to tokenization. The former would occur between the card being read and the assignment of a token. From the merchant's perspective, tokenization involves significant operational changes and could carry significant out-of-pocket costs. Despite that, for the majority of transactions, tokenization still may not address both ends of the security/authentication equation as well as would PIN and Chip. It has greatest utility in the 6 percent of transactions that currently do not occur face-to-face. Consequently, while point-to-point encryption and tokenization could be valuable adjuncts to PIN and Chip authentication, they are not a substitute.

On the other hand, chip and PIN is relatively quickly achievable, and indeed is already deployed successfully in nearly all of the industrialized world (and much of the Third World). Ideally, the United States would at least move to the 21st century standard before attempting to chase the next new thing. Finally, the fact that 18 percent of U.S. retail point of sale locations have already, at the card networks' urging, invested billions of dollars to install PIN and Chip authentication equipment is not an inconsequential consideration.

Q.4. Could retailers voluntarily adopt tokenization?

A.4. To some extent we already have. Many retailers routinely encrypt sensitive data at rest in their systems and take steps to tokenize data in other locations on their own. For example retailers print receipts with the credit and debit card in a blocked format (*i.e.,* xxx xxxx xxxx 4115). More elaborate forms of encryption and tokenization would require coordinated activity by all parties to the payment card system and several years to fully deploy.

RESPONSE TO WRITTEN QUESTIONS OF SENATOR KIRK FROM TROY LEACH

Q.1. In your estimation, would chip and pin technology have prevented the major recent retail breaches? If chip and pin is not the silver bullet, what other options may work? What about tokenization or encryption?

A.1. From the details emerging in the press,[1] it does not appear as though the use of EMV chip in and of itself, regardless of whether it is used with or without PINs would have prevented the recent major breaches. However, use of EMV chip technology is likely to

[1]*See* for example, *http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/*.

have reduced the value of the compromised data as it would inhibit the creation of counterfeit cards.

Tokenization and encryption are both important additional technologies to further limit payment card data from being stolen. As the market migrates payment terminals to support deployment of EMV chip, the PCI Security Standards Council ("the Council") advocates for all involved to consider additional layers of security for data protection through these and other approaches. There are no silver bullets—one specific technological approach will not address all security challenges. The potential for a breach and damages caused by a breach can be mitigated if the entity has preventative, detective and incident response controls which employ a combination of people, process and technology, like those outlined in the PCI security standards. The PCI security standards are a critical layer of defense in this battle against cyber criminals.

Q.2. We've been told that retailers store some information to make transactions, such as returns, easier. What information is needed to process returns and for marketing purposes? Are retailers required to store the 16-digit code and expiration date to process returns? Why might retailers store credit card information?

A.2. As a technical standards body, the Council does not have insight into specific business processes of retailers or other groups. We set our standards to be the framework that all sectors of the payment chain can use to protect payment card data. To the extent that a merchant chooses to store card data, the PCI standards define how that data must be protected. This question is best directed to the banking and credit card companies that have contractual relationships with retailers. That said, possible use cases might include loyalty, marketing programs or legacy business processes.

To further minimize risk of payment card data exposure, the Council advocates that retailers and others take advantage of technologies and methods that help them reduce the amount of payment card data vulnerable to compromise. Such approaches include only storing the data that's needed; eliminating unnecessary user access; limiting the number of systems and networks used for payments; and deploying technologies such as Point-to-Point Encryption (P2PE) and tokenization that protect the data.

Q.3. Is the PIN technology that is widely touted a security measure or used for other purposes? Do retailers really need access to PINs?

A.3. The Personal Identification Number or PIN is used as a security measure by means of authenticating the legitimacy of the cardholder. Only cardholders themselves should have knowledge of the PIN. It is one of a number of measures that can be used to authenticate the legitimacy of the payment transaction. The PIN is also universally used as a cardholder authentication method for ATM transactions. PIN data should not be used for other purposes.

However, PINs are extremely sensitive static data that can be reused by criminals if stolen and requires special handling. That is why PCI requirements in the PIN Transaction Security (PTS) standards require that PINs be encrypted by an approved POS terminal upon entry. When using a properly validated POS terminal, merchants do not have access to non-encrypted PIN data before a transaction is authorized. PTS requirements prohibit the storage of

PINs by merchants after authorization of a transaction has been received by the acquiring bank. PINs also require stronger encryption methods as well as physical security to prevent shoulder surfing or pin hole cameras.

Q.4. Why would a retailer un-encrypt consumers' credit and debit card data as it travels through their system? Is there ever any reason that data should be unencrypted when it is passed from the retailer to the processor?

A.4. The Council cannot speak to an individual retailers need or decision to maintain unencrypted payment card data.

The Council recommends the use of point-to-point encryption or P2PE technology, through its PCI P2PE standard and supporting program. When implemented properly, current P2PE technology solutions that are part of our program ensure that payment card data is encrypted at the point of entry, such as a secured POS terminal, and not decrypted until received into a secured zone. The PCI Council is actively engaged with industry stakeholders to continue developing encryption standards usable for various types of merchant needs.

Q.5. Target was considered "PCI compliant" when it had its annual audit September. It appears that a merchant or other party can be PCI compliant and fall out of compliance the minute auditors walk out the door. Is this, then, really the best standard?

A.5. It is important to note that in order to remain compliant with any security standard (SOX, HIPAA, PCI, *etc.*), merchants must treat compliance efforts as "business as usual" rather than as a once-per-year activity. If a merchant has been validated as compliant, they generally only "fall out" of compliance when choosing to implement insecure changes after the auditor walks out the door. We encourage merchants to allocate their resources to maintaining a secure posture year round rather than focusing on being "compliant" once per year.

Proper implementation and ongoing maintenance are critical to protecting card data, as highlighted by the recently released Verizon 2014 PCI Compliance Report.[2] According to Verizon they, "continue to see many organizations viewing PCI compliance as a single annual event, unaware that compliance needs to have a 365 day-a-year focus." Organizations with security controls in place as part of complying with PCI security standards improve their chances both of avoiding a breach in the first place, and of minimizing the resulting damage if they are breached.

Organizations should focus on maintaining strong security controls, day in and day out. The Council believes that organizations following PCI Standards as the basis for their security programs are best positioned to protect consumers' payment card data. PCI security standards provide the baseline of security controls for card data. Just like a lock is no good if you forget to lock it, these controls are only effective if they are implemented properly and as a part of an everyday, ongoing business process.

---

[2] *http://newscenter.verizon.com/corporate/news-articles/2014/02-11-2014-pci-compliance-report/.*

To maintain the effectiveness of the standards, the Council continues to develop and evolve PCI security standards to be responsive to emerging threats. We do this through our unique global industry forum, taking feedback from retailers, hoteliers, airlines, restaurants, banks, processors, technology vendors and all those involved in the payment transaction chain around the world.

For example, based on industry feedback, with the release of version 3.0 of the PCI DSS and Payment Application-Data Security Standard (PA–DSS, the standard that covers payment applications) we made changes to address emerging threat areas such as third party remote access, POS terminal tampering, and vendor accountability. All updates are aimed at providing the right balance of flexibility, rigor and consistency to help organizations make payment security part of their business-as-usual activity, not something centered on an annual assessment. PCI security standards are developed to provide business process that must be performed consistently on a daily basis. Failing to commit to security as a regular practice of business operation is not meeting the intent of PCI DSS requirements.

Q.6. I understand that PCI sets the security standard and does not enforce compliance, but does do an annual audit for the larger retailers. In your opinion, should there be additional audits, oversight and precautions large retailers should be held to in order to best protect consumers' data?

A.6. It's important to clarify the PCI Council's role here. The Council does not mandate retailers' compliance with or auditing against any of the PCI standards. Additionally, the Council itself does not conduct an annual audit for large retailers or any type of audits for any organization. The Council's role is to develop and manage the PCI DSS and other standards. Frequency of assessment of an organization is determined between a merchant and its acquiring bank or payment card brand business partner.

To best protect consumers' payment card information, the Council recommends retailers deploy and maintain the controls outlined in the PCI DSS, which is a strong foundation for a multi-layered security program. Additional layers of security at the merchant level might include deployment of Point-to-Point Encryption (P2PE) and tokenization solutions that would devalue payment card data.

The Council also promotes the mantra "if you don't need it, don't store it", encouraging organizations to examine business process to reduce or eliminate storage of payment card data.

To support implementation and maintenance of PCI security controls the Council manages a number of programs and listings of information on our public Website. In addition to standards, Council programs include: Website listings of lab-tested secure PIN and non-PIN POS terminals and other payment devices; security of payment applications; testing and qualification of assessors performing PCI DSS audits, training and qualifying professionals to install payment equipment and software; and many other programs focused on the integrity of payment systems and third parties that merchants rely on to conduct business.

Q.7. Do you think that there should be a merchant ISAC formed?

A.7. Payment card security is a shared responsibility. The Council encourages any information sharing and collaboration that will drive greater awareness of risks, threats and solutions, within industry sectors and across the payment chain to help prevent future data breaches. From our own experience the Council has found that global merchant input to PCI security standards development through the lifecycle and feedback process, PCI Special Interest Groups, task forces and Board of Advisors participation continues to be highly valuable.

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

ICBA
INDEPENDENT COMMUNITY BANKERS of AMERICA®

February 3, 2014

Targeted Changes Needed to Curb Risk of Retailer Data Breach

On behalf of the nearly 7,000 community banks represented by the Independent Community Bankers of America (ICBA), thank you for convening today's hearing titled: "Safeguarding Consumers' Financial Data." Community bankers and their customers are deeply alarmed by recent, wide-scale data breaches at prominent, national retail chains. These breaches have the potential to jeopardize consumers' financial integrity and confidence in the payments system. This confidence is vital to sustaining consumer spending necessary for the economic recovery. It is critical we determine what happened, identify the weakest links in the payments processing chain, and implement targeted changes to enhance consumer financial data security. We appreciate the opportunity to offer the community bank perspective on this important issue.

Making Customers Whole

While all the facts of these breaches are not yet known, community banks are taking actionable steps to make credit and debit customers whole. Consumers are protected by a policy of zero-liability coverage with regard to any fraud losses. This coverage is primarily provided by community banks and other financial institutions. Financial institutions are required to provide this protection in order to issue Visa and MasterCard debit and credit cards.

With a vital stake in containing the damage caused by breaches and restoring consumer confidence, community banks absorb the upfront costs of reissuing cards, responding to customer concerns and inquiries, protecting against fraud and any other expenses. These costs may be significant depending on the scope of the breach. For smaller institutions, the cost of reissuing a single credit or debit card ranges from $10 to $15. In a wide-scale breach even a community bank may have to reissue thousands of payment cards. Community banks absorb these costs upfront because their primary concern is to accommodate their customers. However, we strongly believe that these costs should ultimately be borne by the party that experiences the breach. This is critical to aligning incentives to maximize data security by all parties that store consumer data.

While our current focus is on making customers whole, it is appropriate to begin to consider changes in policy, business practice, and technology that will strengthen payment system security and curb the risk of future breaches.

More Comprehensive Data Security Standards Are Needed

Since 1999, financial institutions have been subject to rigorous data protection standards under the Gramm-Leach-Bliley Act (GLBA). These standards have been effective in securing consumer data at financial institutions. To adequately protect consumers and the payments system, <u>all</u> participants in the payments system should be subject to GLBA-like standards.

Under current law, merchants and other parties that process or store consumer financial data are not subject to federal data security standards. Securing financial data at banks is of limited value if it remains exposed at the point-of-sale and other processing points.

Liability Should Be Used To Align Incentives

To maximize data security, the party that experiences a breach should bear responsibility for all costs associated with the breach. This change would better align incentives to keep consumer data safe and foster good business practices. As described above, when payment card information is compromised, mitigation costs are significant. If the party that experiences the breach does not bear these costs, they have little incentive to improve their data security.

New Technologies Will Reduce Risk But There Is No Universal Remedy

Community banks are already investing in technologies that will better secure transaction processing and thwart criminals. In particular, community banks are joining other financial institutions in the orderly migration to chip technology for debit and credit cards. Chip technology may not have prevented the recent retailer breaches but it would have reduced the market value of the card data as it would be far more difficult for criminals to make counterfeit cards. Using chip technology will not protect against fraud in "card-not-present" transactions, such as online purchases. Criminals will continue to try to find weakness regardless of the technology so it is crucial that the marketplace continues to have the flexibility to innovate.

Thank you again for convening this hearing. ICBA looks forward to working with this Committee to craft targeted solutions to enhance the security of consumer financial data.

1615 L Street NW, Suite 900, Washington, DC 20036 ▪ 202-659-8111 ▪ Fax 202-659-9216 ▪ www.icba.org

3138 10th Street North
Arlington, VA 22201-2149
703.842.2215 | 800.336.4644
F: 703.522.2734
dberger@nafcu.org

B. Dan Berger
President & Chief Executive Officer

National Association of Federal Credit Unions | www.nafcu.org

February 3, 2014

The Honorable Mark Warner
Chairman
Senate Banking, Housing, and Urban Affairs
Subcommittee on National Security and
International Trade and Finance
United States Senate
Washington, D.C. 20510

The Honorable Mark Kirk
Ranking Member
Senate Banking, Housing, and Urban Affairs
Subcommittee on National Security and
International Trade and Finance
United States Senate
Washington, D.C. 20510

Re: Ongoing Data Security Breaches at U.S. Retailers Warrant Strong Federal Data Security and Breach Notification Standards

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association exclusively representing the interests of our nation's federally chartered credit unions, I write in advance of this afternoon's important hearing, "Safeguarding Consumers Financial Data." As you know from previous correspondence, data security is a chief priority of NAFCU member credit unions and the 97 million credit union members they serve. We appreciate the opportunity to share our concerns with you and look forward to the hearing exploring the impact of ongoing data breaches on consumers as well as the community based financial institutions that serve them. As the number of data breaches at U.S. retailers continues to climb, so does the emotional toll and financial burden on tens of millions of consumers across the country.

While large breaches, like the massive Target Corporation breach, draw national attention, the reality is that data breaches are happening all the time, often on a smaller scale. A January 2014 survey of NAFCU-member credit unions found that, on average, credit unions were notified over 100 times in 2013 of possible breaches of their members' financial information. That same survey found that nearly 80% of the time those notifications led to the credit union issuing a new plastic card to the member at their request because of the security breach, at an average cost of $5.00 to $15.00 per card.

The recent Target breach has been especially onerous on credit unions. Our member credit unions report that, on average, they have received hundreds of inquiries from their members seeking assistance due to the recent Target breach. NAFCU estimates that this particular breach could end up costing the credit union community nearly $30 million. This cost comes from the monitoring, reissuance of cards and fraud investigations and losses from this breach, and does not count the intangible cost of the staff time needed to handle all of the member service issues that stem from the breach. Unfortunately, credit unions will likely never recoup much of this

cost, as there is no statutory requirement on merchants to be accountable for costs associated with breaches that result on their end.

As we first wrote to Congress last February as part of NAFCU's five-point plan on regulatory relief, these incidents must be addressed by lawmakers. Every time consumers choose to use plastic cards for payments at a register or make online payments from their accounts, they unwittingly put themselves at risk. Many are not aware that their financial and personal identities could be stolen or that fraudulent charges could appear on their accounts, in turn damaging their credit scores and reputations. Consumers trust that entities collecting this type of information will, at the very least, make a minimal effort to protect them from such risks. Unfortunately, this is not always true.

Financial institutions, including credit unions, have been subject to standards on data security since the passage of *Gramm-Leach-Bliley*. However, retailers and many other entities that handle sensitive personal financial data are not subject to these same standards, and they become victims of data breaches and data theft all too often. While these entities still get paid, financial institutions bear a significant burden as the issuers of payment cards used by millions of consumers. Credit unions suffer steep losses in re-establishing member safety after a data breach occurs. They are often forced to charge off fraud-related losses, many of which stem from a negligent entity's failure to protect sensitive financial and personal information or the illegal maintenance of such information in their systems. Moreover, as many cases of identity theft have been attributed to data breaches, and as identity theft continues to rise, any entity that stores financial or personally identifiable information should be held to minimum standards for protecting such data.

While some argue for financial institutions to expedite a switch to a "chip and pin" card, the reality is that it is no panacea for data security and preventing merchant data breaches. Many financial institutions that issue "chip and pin" cards had those cards stolen in the Target data breach as the retailer only accepted magnetic strip technology at the point of sale where the breach occurred. Furthermore, "chip and pin" cards can be compromised and used in online purchase fraud, as the technology is designed to hinder card duplication and card information can still be compromised. This fact highlights the need for greater national data security standards as the way to truly help protect consumer financial information.

Again, recent breaches are just the latest in a string of large-scale data breaches impacting millions of American consumers. The aftermath of these and previous breaches demonstrate what we have been communicating to Congress all along: credit unions and other financial institutions – not retailers and other entities – are out in front protecting consumers, picking up the pieces after a data breach occurs. It is the credit union or other financial institution that must notify its account holders, issue new cards, replenish stolen funds, change account numbers and accommodate increased customer service demands that inevitably follow a major data breach. Unfortunately, too often the negligent entity that caused these expenses by failing to protect consumer data loses nothing and is often undisclosed to the consumer.

NAFCU specifically recommends that Congress make it a priority to craft legislation and act on the following issues related to data security:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be to require entities to be accountable for costs of data breaches that result on their end, especially when their own negligence is to blame.

- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under Gramm-Leach-Bliley, credit unions and other financial institutions are required to meet certain criteria for safekeeping consumers' personal information. Unfortunately, there is no comprehensive regulatory structure akin to Gramm-Leach-Bliley that covers retailers, merchants and others who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any entity responsible for the storage of consumer data to meet standards similar to those imposed on financial institutions under the Gramm-Leach-Bliley Act.

- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to when they provide their personal information. NAFCU believes this problem can be alleviated by simply requiring merchants to post their data security policies at the point of sale if they take sensitive financial data. Such a disclosure requirement would come at little or no cost to the merchant but would provide an important benefit to the public at large.

- **Notification of the Account Servicer:** The account servicer or owner is in the unique position of being able to monitor for suspicious activity and prevent fraudulent transactions before they occur. NAFCU believes that it would make sense to include entities such as financial institutions on the list of those to be informed of any compromised personally identifiable information when associated accounts are involved.

- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones that place their personal information at risk.

- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by merchants and retailers who retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in their systems, which can be breached easily in many cases.

- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they are harmed by a data breach, NAFCU believes that the evidentiary burden of proving a lack of fault should rest with the merchant or retailer who incurred the breach. These parties should have the duty to demonstrate that they took all necessary precautions to guard consumers' personal information but sustained a violation nonetheless. The law is currently vague on this issue, and NAFCU asks that this burden of proof be clarified in statute.

As the subcommittee continues to look for ways to strengthen data security measures at various entities, we urge you to carefully review bipartisan legislation recently introduced by Senators Tom Carper and Roy Blunt – the *Data Security Act of 2014* (S. 1927) – that would make great strides toward ensuring that a strong federal standard is in place to protect sensitive financial data. NAFCU supports this legislation as a first step toward addressing ongoing data breaches at retailers across the country.

On behalf of our nation's credit unions and their 97 million members we thank you for your attention to this important matter. If my staff or I can be of assistance to you, or if you have any questions regarding this issue, please feel free to contact myself, or NAFCU's Vice President of Legislative Affairs, Brad Thaler, at (703) 842-2204.

Sincerely,

B. Dan Berger
President and CEO

cc: Members of the Senate Banking Committee

Statement for the Record
Senate Committee on Banking, Housing and Urban Affairs
Subcommittee on National Security and International Trade and Finance
February 3, 2014

Cyber criminals are becoming more sophisticated, and recent breaches of consumers' data underscore the urgency of updating the payments system to protect against current and future threats. At the same time, the way consumers pay for transactions is undergoing unprecedented change. In addition to ever increasing amounts of online shopping, all evidence indicates that more and more consumers will use smartphones for mobile payments at physical point-of-sale, bringing with it new risks to consumers and merchants alike.

While banks along with federal laws and regulations protect consumers, data breaches result in lost consumer confidence, as well as the inconvenience of card replacement, account monitoring, and fraud reporting. It is critical that the entire payments ecosystem- retailers, processors, banks and networks—embrace and deploy secure tokenization to protect consumers and merchants. "Tokenization" substitutes a limited-use random number (token) for customers' account numbers so that the sensitive information remains safe.

The planned U.S. migration to the EMV (Europay, MasterCard and Visa) standard is an important step in enhancing the overall protection of point-of-sale payments systems. Since EMV cards are designed to prevent counterfeiting, they lessen the resulting fraud consequences of a breach. However, because EMV-enabled transactions still transmit cardholder data at the point-of-sale, EMV would *not* have prevented the theft of customer account numbers that occurred in the Target and other recent retailer breaches. Moreover, as EMV was designed prior to the Internet, it does not protect consumers against online fraud, which is where the majority of these crimes are committed. As a result, the implementation of EMV in Europe has led to a shift in fraud from point-of-sale to online. [1] EMV, while an important step forward, is only a partial solution.

Research shows that the overwhelming majority of consumer account information breaches occur as the result of security vulnerabilities on the retailer side of the transaction.[2] Tokenization of sensitive data is the best possible solution because no actual customer account information will be stored in retailer environments. Rather, it will only exist behind the security of highly-regulated and closely-examined financial institutions and their service providers.

---

[1] While EMV & chip implementation in Europe has helped reduce losses at the point-of-sale by 24%, that is offset by card not present losses which remain high and now account for 56% of all card fraud. *Second Report on Card Fraud*, European Central Bank, July 2013, available at: http://www.finextra.com/News/FullStory.aspx?newsitemid=25023

[2] The business sector, because of the Target breach, accounted for almost 82 percent of 2013's breached records. The Banking, Credit and Financial sector accounted for only 4 percent of all breaches and less than 2 percent of all breached records. *2013 Data Breach Category Summary*, Identity Theft Resource Center, January 1, 2014, available at: http://www.idtheftcenter.org/images/breach/2013/BreachStatsReportSummary2013.pdf .

Tokenization substitutes a limited-use random number ("token") for customers' account numbers, with the real account numbers securely stored in bank data vaults. Tokenization protects *both* consumers and merchants from the risks of future data breaches. Even if compromised, the token is of limited or no use to criminals.[3] In addition to providing a significant increase in security for consumers, it alleviates a burden placed on retailers because they do not have to keep and safeguard vast quantities of sensitive data. Also, tokenization can be implemented with minimal disruption to retailer point-of-sale environments, while still supporting merchants' customer service and data analytics capabilities.

A number of tokenization efforts, including one undertaken by The Clearing House and its owner banks, are in progress. We believe it is important for Members of Congress to understand the promise that this technology holds to solve the security issues that seem to be plaguing our nations' top retailers. This endeavor is being pursued proactively by the industry and is designed to proceed quickly to implementation.[4]

All parties in the payments ecosystem have a responsibility to ensure that consumers remain protected and that the nations' payment systems remain safe, sound, and secure. The Clearing House and its banks will continue to work proactively and cooperatively with all participants in the payments ecosystem, including merchants, processors, and networks, to ensure that the best possible solutions are implemented to combat the increasing threats posed by cyber criminals.

About The Clearing House

Established in 1853, The Clearing House is the nation's oldest banking association and payments company. It is owned by the world's largest commercial banks, which collectively employ 1.4 million people in the United States and hold more than half of all U.S. deposits. The Association is a nonpartisan advocacy organization representing—through regulatory comment letters, amicus briefs, and white papers—the interests of its owner banks on a variety of systemically important banking issues. Its affiliate, The Clearing House Payments Company L.L.C., provides payment, clearing, and settlement services to its member banks and other financial institutions, clearing almost $2 trillion daily and representing nearly half of the funds transfer, automated clearinghouse, and check image payments made in the United States. For additional information, see The Clearing House's Web page at www.theclearinghouse.org.

---

[3] In a dynamic tokenization system, a token is valid either for a single transaction or for a limited number of transactions occurring in the typically very short time interval during which a new token is generated and provisioned to the mobile wallet. If a dynamic token were to be intercepted by malware residing in a retailer point-of-sale system, the ability to use that token for a subsequent fraudulent purchase is nearly impossible, would require the fraudster to be in the same immediate vicinity, and would be rapidly detected.

[4] Two years ago, The Clearing House banks recognized the emerging security risks related to mobile payments, as well as the growing risks due to the proliferation of sensitive customer account information online. They organized an initiative, TCH Secure Cloud, to mitigate these risks. Secure Cloud uses tokenization technology so that customers' real account numbers are never provided to the merchant and are never present on a mobile device. Secure Cloud is currently in a live pilot. The solution is being developed as an open standard, meaning it will be accessible to everyone, demonstrating the banking industry's commitment to work cooperatively with all participants in the payments ecosystem, including merchants, processors and networks.

CUNA
Credit Union National Association

Bill Cheney
President & CEO

601 Pennsylvania Ave., NW
South Building, Suite 600
Washington D.C. 20004-2601

Phone: 202-508-6745
Fax: 202-638-7734
bcheney@cuna.coop

February 3, 2014

The Honorable Mark Warner
Chairman
Subcommittee on National Security and International Trade and Finance
Committee on Banking, Housing and Urban Affairs
United State Senate
Washington, DC 20510

The Honorable Mark Kirk
Ranking Member
Subcommittee on National Security and International Trade and Finance
Committee on Banking, Housing and Urban Affairs
United State Senate
Washington, DC 2051

Dear Chairman Warner and Ranking Member Kirk:

On behalf of the Credit Union National Association (CUNA) and America's credit unions, I am writing today to thank you for holding today's hearing entitled "Safeguarding Consumers' Financial Data." CUNA is the largest credit union advocacy organization in the United States, representing America's 6,700 state and federally chartered credit unions and their 99 million members.

This hearing is an important and timely response to recent merchant data breaches affecting millions of Americans and their financial institutions. We appreciate the Subcommittee's focus on safeguarding consumer data, and we look forward to today's testimony and discussion of what should be done to ensure an appropriate response to not only these data breaches, but data breaches that may occur next week, next month, or next year.

We encourage Congress to take a holistic approach to this issue. In the years to come, consumers will use many payment methods, including magnetic (mag) stripe cards, chip and PIN cards (EMV), cloud-based mobile payments, tokenization, and other methods we can only imagine at this point in time. Focusing on one payment method as the absolute answer to solving data security breaches is both shortsighted and distracts from the greater need of a federal data security framework for all entities. Instead, Congress should take a broad look at how consumer data is secured and the improvements that are necessary to prevent future breaches from taking place.

Data breaches occur, in part, because merchants are not required to adhere to the same statutory data security standards that credit unions and other financial institutions must follow, and merchants are rarely held accountable for the costs others incur as a result of the breaches. All participants in the payment process have a shared responsibility to protect consumer data, but the law and the incentive structure today allows merchants to abdicate that responsibility, making consumers vulnerable.

Since the initial reporting of the Target data breach, credit unions have focused on protecting their members from harm, to the extent they can. They have taken many steps including, but not limited to, notifying their members that a breach had occurred, reissuing new debit and credit cards to affected members, and increasing staff at call centers to account for additional member inquiries.

The impact of merchant data breach related costs is far reaching; for not-for-profit credit unions operating on already thin margins, these costs make a significant difference in their ability to offer services to their members. CUNA recently conducted a survey of credit unions regarding the costs they are incurring to help their members respond and recover from the recent breach at Target. Preliminary data indicates that credit unions are incurring a cost of approximately $5.10 per affected card and that the system has incurred a total estimated cost of between $25-30 million as a result of this breach. This figure will continue to increase because this data does not include fraud costs which may develop in the near future.

In addition to the actual costs credit unions must bear as result of the breach, they also face reputational damage because they have an obligation to notify their members that their account has been compromised but are often limited in their ability to disclose the name of the merchant where the breach occurred. So, when members are notified that their account has been compromised, the credit union is unable to tell them where the compromise occurred and some members assume the problem was with the credit union.

As Congress considers legislative remedies, credit unions support three basic principles:

1. All participants in the payments system should be responsible and be held to comparable levels of data security requirements.

Under current federal law, credit unions and other financial institutions are held to high standards of data security for consumer information under the *Gramm-Leach-Bliley Act*. There is no comparable federal data security responsibility for a national merchant holding consumer data. This represents a weak link in the chain and it needs to be addressed. We support legislation, such as S. 1927, the *Data Security Act of 2014*, introduced by Senators Carper and Blunt, that would provide a national standard for businesses to protect sensitive consumer information, rather than a myriad of differing state laws and regulations.

2. Those responsible for the data breach should be responsible for the costs of helping consumers.

It has been said by merchants that consumers will not be responsible for any financial loss in their accounts. That is true, but not because the merchant will reimburse affected consumers. It happens because the consumer's financial institution pays for the costs related to a merchant data breach involving accounts held at that institution. Under current law, the merchant is not obligated to reimburse financial institutions for any costs incurred as a result of the breach. In other words, even though the breach happened on the merchant's watch,

retailers have no responsibility for the costs of the breach because financial institutions take care of their members and customers.

When a merchant data breach occurs, credit unions are there to help their members. Whether it is increased staffing to handle additional member questions, notifying members, reissuing cards, tracking possible fraudulent activity, or reimbursing a member for fraudulent charges caused by a third party, credit unions bear the costs even though the merchant was responsible for the breach. We support legislation to address this problem and make it easier for credit unions to recoup the costs they incur. We believe that if Congress sets strong merchant data security standards and those standards are not met by a merchant whose data is breached, the merchant should be held responsible for the credit union's costs associated with that breach.

3. Consumers should know where their information was breached.

Credit unions also support legislation that requires merchants to provide notice to those consumers affected by a data breach, and permits credit unions to disclose where a breach occurs when notifying members that their account has been compromised.

When it comes to bad news like a data breach, it is easy to "blame the messenger." In today's world, the credit union is the messenger and, depending on the state, may not be permitted to identify the breach source to the consumer member. Consumers need transparency and knowledge to understand where their data has been put at risk. S. 1927 addresses this priority as well.

In conclusion, we look forward to the Subcommittee's dialogue regarding data security. It is a complicated and dynamic issue. As these latest merchant breaches have demonstrated, millions of consumers, and their respective credit unions, are affected. We believe the best answer is a federal comprehensive approach to data security.

On behalf of America's credit unions and their 99 million members, thank you for your attention to this very critical matter and your consideration of our views.

Best regards,

Bill Cheney
President & CEO