

February 3, 2014

The Honorable Patrick Leahy
Chairman
Committee on the Judiciary
U.S. Senate
Washington, D.C. 20510

The Honorable Charles Grassley
Ranking Member
Committee on the Judiciary
U.S. Senate
Washington, D.C. 20510

Re: Hearing Titled “Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime”

Dear Chairman Leahy and Senator Grassley:

The undersigned organizations representing the financial services industry are writing to commend you for holding this hearing on the recent breaches of sensitive consumer financial and personal information at several major retailers across the country. The financial services industry stands ready to assist policymakers in ensuring that robust security requirements apply to all participants in the payments system, and we respectfully request that this letter be made part of the record for your hearing.

In all data breaches, including the recent retailer breaches, the financial services industry’s first priority is to protect consumers from fraud caused by the breach. Banks and credit unions do this by providing consumers “zero liability” from fraudulent transactions in the event of a breach. Although financial institutions bear no responsibility for the loss of the data from a retailer’s system, they assume the liability for a majority of the resulting card-present fraud. In most instances, financial institutions have historically received very little reimbursement from the breached entities – literally pennies on the dollar.

For example, virtually every bank and credit union in the country is impacted by the Target breach. Our understanding is that the breach affects up to 40 million credit and debit card accounts nationwide, and also has exposed the personally identifiable information (name, address, email, telephone number) of potentially 70 million people. To put the scope of the breach in perspective, on average, the breach has affected 10 percent of the credit and debit card customers of every bank and credit union in the country.

The Target breach alone is estimated to cost financial institutions millions of dollars to reissue cards and increase customer outreach, with substantial longer-term costs associated with fraud and mitigation efforts to limit the damage to customers. Although a variety of factors can go into the calculation, for banks and credit unions the cost of reissuing cards can range from \$5 up to \$15 per card, and a preliminary survey of banks impacted by the Target breach conducted by the Consumer Bankers Association indicated that more than 15.3 million debit and credit cards have been replaced to date. The numbers of cards issued, along with the total costs, are nearly certain to rise, especially as the extent to which other retailers have been breached becomes more certain.

For consumers, the critical issue is the security of their personal information. Banks, credit unions, and other financial companies dedicate hundreds of millions of dollars annually to data security and adhere to strict regulatory and network requirements at both the federal and state levels for compliance with security standards. However, criminal elements are growing increasingly sophisticated in their efforts to breach vulnerable links in the payments system where our retailer partners have not yet been able to align with the financial sector's higher standards of practice in security. In fact, according to the Identity Theft Resource Center, there were more than 600 reported data breaches in 2013 – a 30 percent increase over 2012. The two sectors reporting the highest number of breaches were healthcare (43 percent) and business, including merchants (34 percent). Because of the Target breach, the business sector accounted for almost 82 percent of the breached records in 2013. In contrast, the financial sector accounted for only 4 percent of all breaches and less than 2 percent of all breached records.

Our payments system is made up of a wide variety of players: financial institutions, card networks, retailers, processors, and new entrants. Protecting this eco-system is a shared responsibility of all parties involved and all must invest the necessary resources to combat increasingly sophisticated breach threats to the payments system.

Indeed, extensive efforts are under way to improve card security, including implementation of EMV (chip-based technology) standards by encouraging investment in point-of-sale terminal upgrades and card reissuance to accommodate EMV transactions, and investing in additional security innovations. The major card networks started the EMV migration domestically in 2011, and in 2015 at the retail point-of-sale the party that is not EMV capable (either the issuer or merchant) will be responsible for counterfeit fraud. EMV migration will be fully implemented by October 2017. This liability shift incentivizes both retailers and financial institutions to implement chip-based technology.

EMV technology improves current security by generating a one-time code for each transaction, so that if the card number is stolen it cannot be used at an EMV card-present environment. However, while EMV addresses card-present fraud, it does not increase the security of on-line transactions, which is an increased target in countries that have implemented EMV.

Threats to data security are ever changing and unpredictable. Therefore, policymakers should not mandate or embrace any one solution or technology, such as EMV, as the answer to all concerns. As the threat evolves, so too must coordinated efforts to combat fraud and data theft that harm consumers. To address the emerging risks posed by mobile payments, for example, industry-driven solutions, such as the TCH Secure Cloud, are already underway employing “tokenization” technology.

Tokenization adds additional security by generating a random limited-used number for e-commerce or mobile transactions, rather than using the actual account number. If stolen and attempted to be used as a legitimate account number, it would be of limited or no use. It also takes merchants out of harm's way by eliminating the need for them to even store sensitive account numbers. As threats continue to evolve, so too must our efforts to combat fraud and data theft that harm consumers, financial institutions, and the economy.

As you and your colleagues consider next steps for dealing with this important issue, we have several recommendations that would help to strengthen the payments system and better protect consumers in the event of a breach.

- 1) **Establish a national data security breach and notification standard.** We believe that legislation should be enacted to better protect consumers by replacing the current patchwork of state laws with a national standard for data protection and notice. A good example of this is the Data Security Act of 2014 (S. 1927) introduced by Senators Tom Carper (D-DE) and Roy Blunt (R-MO).
- 2) **Make those responsible for data breaches responsible for their costs.** Financial institutions bear the brunt of fraud costs. An entity that is responsible for a breach that compromises sensitive customer information should be responsible for the costs associated with that breach to the extent the entity has not met necessary security requirements.
- 3) **Better Sharing of Threat Information.** Unnecessary legal and other barriers to effective threat information sharing between law enforcement and the financial and retail sectors should be removed through private sector efforts and enactment of legislation. For example, one such private sector effort is the expansion of membership in the Financial Services Information Sharing and Analysis Center to include the merchant community. No one organization or sector alone can meet the challenges of sophisticated cyber-crime syndicates, so robust communities of trust and collective protection must constantly be developed.

Our organizations and the thousands of banks, credit unions, and financial services companies we represent are aggressively investing in a safe and secure payments system for our nation. Protecting this system is a shared responsibility of all parties involved and we need to work together to combat the ever-present threat of criminal activity. The financial services industry stands ready to assist policymakers in ensuring that robust security requirements apply to all facets of the payments system.

Sincerely,

American Bankers Association
The Clearing House
Consumer Bankers Association
Credit Union National Association
Financial Services Information Sharing and Analysis Center
The Financial Services Roundtable
Independent Community Bankers of America
National Association of Federal Credit Unions

Cc: Members of the Senate Judiciary Committee



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 Patrick Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

The Honorable Chuck Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Re: The Importance of Data Security to Our Nation's Credit Unions

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 tomorrow's important hearing, "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime." 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.

Unfortunately, large national data breaches are becoming all too common. Consumers and credit unions have not only been hit with the recent Target Corporation breach, but also with additional national breaches recently coming to light at Neiman Marcus, Michaels and the White Lodging hotel management company. Tens of millions of Americans have been adversely impacted by these breaches. While these breaches draw national attention, the reality is that data breaches are also happening all the time, often on a smaller scale that doesn't garner the national headlines but still, when taken together, impact just as many American consumers.

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 stripe 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.

We applaud you and the Committee for your leadership on this issue. NAFCU would welcome the opportunity to work with you on legislation to strengthen data security standards for those who do not have such requirements now.

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 Judiciary Committee

**STATEMENT OF THOMAS M. BOYD
COUNSEL
NATIONAL BUSINESS COALITION ON E-COMMERCE AND PRIVACY
BEFORE THE SENATE JUDICIARY COMMITTEE
ON S.1897
FEBRUARY 4, 2014**

Chairman Leahy, Senator Grassley, Members of the Committee, thank you for allowing me to submit a statement for the record at this hearing. My name is Thomas M. Boyd, and I am a partner in the Washington, D.C. office of DLA Piper LLP. I am submitting this statement on behalf of the National Business Coalition on E-Commerce and Privacy (the "Coalition"), to which I serve as Counsel; the Coalition's Chairman is Tony Hadley, of Experian, and its Vice-Chair is Tamara Salmon, of the Investment Company Institute ("ICI"). Created at the behest of former GE CEO Jack Welch following the adoption of Title V of the Gramm-Leach-Bliley ("GLB") Act in 1999, the Coalition opened for business in February, 2000, and it has been an active participant in the public policy and regulatory debate affecting privacy ever since.

The Coalition represents brand name American companies, many of which have global operations, and each of which wish to see reasonable, workable, and commercially sustainable public policy put in place where privacy is concerned, both at the Federal and state level. Its members include, among others, Acxiom, JP MorganChase, Bank of America, VISA, The Vanguard Group, Charles Schwab & Co., Fidelity Investments, Ally Financial, The Principal Financial Group, Fiserv, Inc., Deere and Co., and the ICI. While its membership is disproportionately financial, the Coalition is not solely a financial services entity. Through the years its membership has included, in addition to its current non-financial members, several other brand name non-financial companies.

I.

With respect to data security and breach notification, the Coalition has long and consistently supported enactment of a national, preemptive Federal law. We specifically endorsed S. 1212, legislation introduced in April, 2007, by Sen. Jeff Sessions (R-AL), and ever since we have actively encouraged policymakers in the Congress, as well as the Executive Branch, to focus on passing uniform data security and breach notification legislation in a stand-alone bill.

Until now, each time it has been considered, legislation that should have narrowly focused on data security and breach notification has been broadened to include a number of privacy-related provisions. This has inevitably resulted in consistently and repeatedly forestalling the adoption of any legislation whatsoever, thereby sacrificing the enactment into Federal law of necessary provisions governing data security and breach notification. This sequence of events has been the same, now, for nearly eight years.

We believe it's time to try a new approach.

In the wake of Edward Snowden's decision to leak critical information from the National Security Agency and the recent, highly publicized consumer data breaches, we feel that the time has now come for the Senate and the House, in coordination with the business community, consumers, and the White House, to make enacting uniform data security and breach notification legislation a public policy priority. We

firmly believe that this effort can start with this Committee. Indeed, if there were bipartisan support on this Committee for a clean data security and breach notification bill – and there should be – we are confident that it would have the enthusiastic and active support of both consumers and the business community, leading, in relatively short order, to a Federally-preemptive final result.

As the Committee well knows, since 2005, the absence of Federal action on data security and breach notification has not resulted in a landscape devoid of compliance obligations for custodians of sensitive personally identifiable data. Instead, some 46 states and the District of Columbia have attempted to fill the void at the Federal level by enacting statutes designed to address this issue. The patchwork and inconsistency of these various laws have proved challenging for Coalition members and others subject to them. Moreover, states are constantly revising these laws, which only adds to the complexity of the compliance challenge for firms, such as members of the Coalition, that operate in all 50 states. A single set of national standards would adequately protect individuals throughout our country, without requiring companies to ensure compliance with myriad different and ever-changing laws, with the unfortunate result that resources would be unnecessarily diverted that should otherwise be focused on privacy and data security protection efforts. Already in 2014, there are six such bills pending in five states.

The time is ripe, therefore, for this Committee to act and quickly report a clean data security and breach notification bill. The Coalition is happy to provide whatever assistance it can to help the Committee achieve this critically important goal.

II.

As it considers legislation in this area, we believe it is very important that the Committee and the Senate segregate the facts and circumstances surrounding the recent and ongoing NSA debate from data privacy and data security generally. They are very different from one another and they should be considered and addressed separately. Unfortunately, this is not always the case. For example, in his January 17th speech outlining steps he planned to take to address issues surrounding the NSA leaks, President Obama unfortunately conflated the intelligence community's collection and use of national security data with "[c]orporations of all shapes and sizes [that] track what you buy, store and analyze our data and use it for commercial purposes". That is a link that was as unfortunate as it was inapplicable. America's companies collect data to improve the products they offer and sell and to provide consumers with a more relevant shopping experience. Companies make their data collection and use practices transparent through readily-accessible privacy policies, and many provide consumers choices about how information pertaining to them is used.

While the essential legal obligation to secure sensitive personally identifiable data is already required by Federal law, currently it applies only to HIPAA-regulated entities and "financial institutions", as defined by GLB, as well as to certain other narrow industry sectors (such as consumer reporting agencies under the Fair Credit Reporting Act) and types of information (such as personal information about children under the age of 13). In section 501(b) of Title V of GLB, functional regulators were required to, and have adopted rules to insure the "security and confidentiality of customer records and information", protect against any "anticipated threats or hazards to the security or integrity of such records", and protect against "unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer". Entities outside the scope of these functional regulators are currently not subject to similar requirements. We believe they should be and such obligations should be extended nationally to any custodian that maintains sensitive personally identifiable data on 10,000 or more United States persons.

Once the obligation to secure the confidentiality of sensitive personally identifiable data is in place, there are a number of other important provisions that the Coalition believes ought to be incorporated into any final data security and breach notification legislation. In summary, these provisions are as follows:

1. **Encryption.** As a practical matter, eliminating breaches is virtually impossible. What can happen, however, is that stored data can be rendered unusable, without a cryptographic “key” to convert it into readable, or usable, form. It is therefore imperative that all sensitive personally identifiable data be unusable if accessed by a person without appropriate authorization. This could be achieved through means such as the use of encryption technology, as long as other necessary measures, such as securing the cryptographic key and implementing appropriate system access controls, are in place. Since such technology is expensive and not always technologically feasible to install (such as on legacy mainframe systems and applications where the cryptographic conversions unreasonably slow transaction speeds), custodians can be incentivized to employ it if a discretionary “safe harbor” from prosecution is available and applied with respect to data that is stored using commercially reasonable encryption technology and processes.

2. **Breach.** Since a breach sets in motion an often complicated and costly notification and remediation process, it is similarly critical that the term “breach” be properly and reasonably defined to protect appropriately any individuals to whom sensitive personally identifiable data pertains. Toward this end, the standard for notification should be a reasonable basis on the part of the custodian to conclude that a significant risk of identity theft exists as a result of the unauthorized access to protected data. In other words, the trigger that initiates the breach notification process should be consistent with that set forth in section 212(b)(1)(A) of Chairman Leahy’s bill, S. 1897.

3. **Notification.** Once the breach notification process has been triggered, all affected persons should be notified by the custodian and informed of what steps need to be taken to protect themselves from the risk of identity theft. The timing of such notification should be swift and expeditious, without unreasonable delay. Specific timelines, however, such as the 48-hour timeline referenced in some proposals, are too short and do not take into consideration the often difficult practical process of performing necessary systems analysis and data forensics, including assessing the damage, identifying those who may be at risk, protecting against the risk of additional data exposure, and ensuring that proper persons are effectively notified. Moreover, there may also be circumstances in which federal law enforcement agencies such as the Federal Bureau of Investigation or the Secret Service may wish to delay notification, and that option needs to be available as well.

4. **Preemption.** In the absence of effective preemption, there is no practical public policy reason to have a Federal law; there are already 46 state laws on the subject. In our view, language such as that in sections 219 and 204(a) of S.1897, are examples of generally effective preemption language. To be effective, such preemptive language *must totally* supersede State law on the same subject; merely setting a floor does not achieve the significant benefits of having a uniform national standard. This result can best be achieved by using language, as S. 1897 does, that covers any State law that “relates to” the subject of the Federal law (*i.e.*, data security and breach notification). Some proposals have sought to exclude from preemption undefined State “consumer laws,” thereby resulting in such generalized exclusions becoming loopholes that can be used to defeat the purpose of the preemption clause altogether. The language in section 214(b) of S. 1897 could similarly be read to create a loophole in an otherwise sound preemption section.

5. **Enforcement.** The general rule with respect to preemptive statutes is that if State law is superseded, then Federal law enforcement takes priority. Thus, either a Federal functional regulator or, for those persons without a functional Federal regulator, the United States Attorney General or the Federal Trade Commission (“FTC”), are charged with enforcing the Federal law. That does not mean, however, that State Attorneys General should be excluded from the enforcement process. On the contrary, they -- and only they -- should serve to augment Federal enforcement because they collectively have greater resources and are closer in proximity to the consumer. However, contrary to language contained in section 203(c)(1) of S. 1897, no other state offices or agencies should be authorized to enforce the Federal statute. It is similarly important, once a Federal enforcement action is undertaken, that all State enforcement options are superseded, as it serves no public purpose to subject the target of such Federal action to the prospect of 51 separate actions based on the same alleged violation and the same facts. Section 218(c) of S. 1897 takes the position that such State enforcement action should be superseded, and we agree with it.

6. **Private Right of Action.** Given the range of enforcement options available at the Federal and State level, and the importance ensuring that a safe harbor that provides strong incentives with respect to data security are effective, there is no public policy justification for the existence of a private right of action in the event of a data breach. Like section 218(f) of S. 1897, any bill on this subject should therefore bar any such action.

7. **Criminal/Civil Action.** Only the United States Attorney General and State Attorneys General should have jurisdiction to bring *criminal* actions against violators of this statute, and those actions should be limited to cases of egregious violations. By contrast, both Federal and State Attorneys General, as well as the FTC, should have jurisdiction to bring *civil* actions, subject to a publicly available memorandum of understanding (“MOU”) with the United States Department of Justice. That said, we also do not believe that there should be unplugged multipliers for civil damages or that the FTC should have rulemaking authority such as that envisioned in proposed sections 216(c) and 217(f) of S. 1897.

Again, Mr. Chairman and Members of the Committee, the Coalition urges the Committee and the Leadership of the Senate to seize upon this opportunity to craft a bipartisan bill that would, once and for all, establish a nationally uniform standard for data security and breach notification, one that, in concert with the states, would provide consumers with a high degree of confidence that their sensitive personally identifiable data that is held by private sector custodians is secure and, in the event of a breach that creates a significant risk of identity theft, affected consumer can be assured that they would be promptly notified and able to take appropriate steps to protect themselves against the risk of identity theft. We stand available to work with you and the Committee staff every step of the way, and we welcome the opportunity.



National Retail Federation[®]

The Voice of Retail Worldwide

Statement
On Behalf of

The National Retail Federation,
The National Council of Chain Restaurants,
and Shop.org

For

The Senate Judiciary Committee's

Hearing on

**"Privacy in the Digital Age:
Preventing Data Breaches and Combating Cybercrime"**

February 4, 2014

Prepared by
Mallory Duncan
General Counsel and
Senior Vice President

National Retail Federation
325 7th Street, N.W., Suite 1100
Washington, D.C. 20004
(202) 783 -7971
www.nrf.com

Chairman Leahy, Ranking Member Grassley and members of the Committee, thank you for holding a hearing examining data breaches and cyber crime. The National Retail Federation (NRF) is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the nation's largest private sector employer, supporting one in four U.S. jobs – 42 million working Americans. Contributing \$2.5 trillion to annual GDP, retail is a daily barometer for the nation's economy.

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

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

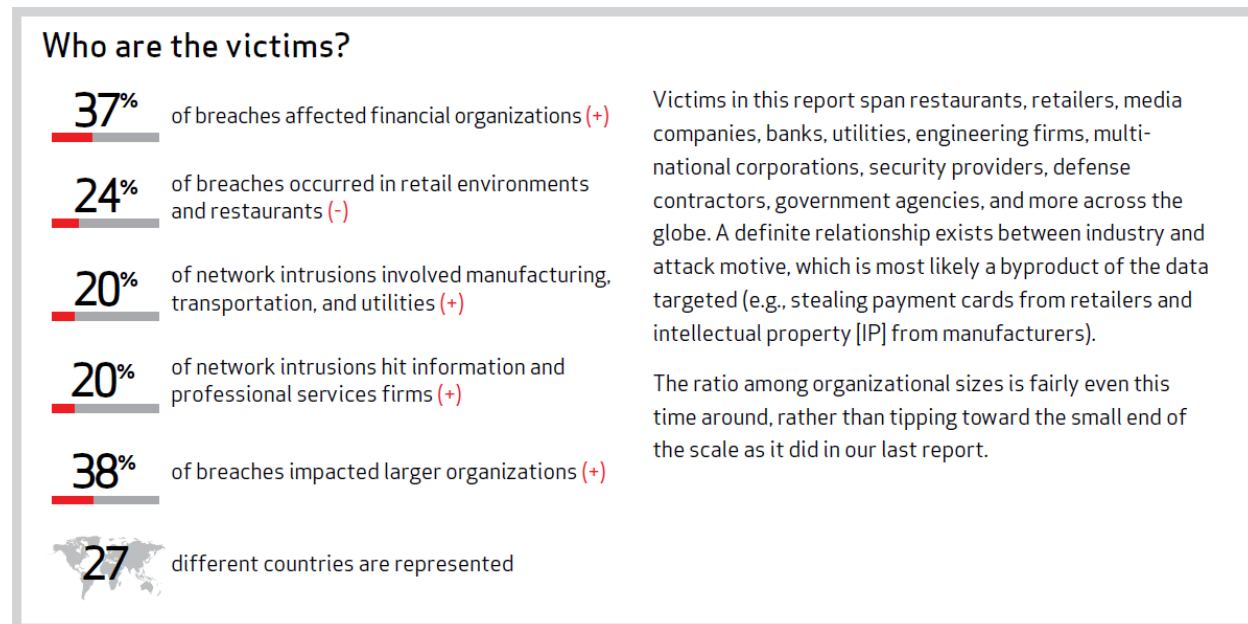
With that in mind, this testimony is designed to provide some background on data breaches and on fraud, explain how these events interact with our payments system, discuss some of the technological advancements that could improve the current situation, raise some ways to achieve those improvements, and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

Data Breaches in the United States

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

It may be surprising to some given recent media coverage that more data breaches occur at financial institutions than at retailers. And, it should be noted, even these figures obscure the fact that there are far more merchants that are potential targets of criminals in this area. There are hundreds of times as many merchants accepting card payments in the United States than there are financial institutions issuing and processing those payments. So, proportionally, and

not surprisingly, the thieves focus far more often on banks which have our most sensitive financial information – including not just card account numbers but bank account numbers, social security numbers and other identifying data that can be used to steal identities beyond completing some fraudulent transactions.



Source: 2013 Data Breach Investigations Report, Verizon

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

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

Background on Fraud

Fraud numbers raise similar concerns. Just a year ago, Forbes found that Mexico and the United States were at the top of the charts worldwide in credit and debit card fraud.² And fraud losses in the United States have been going up in recent years while some other countries have had success reducing their fraud rates. The United States in 2012 accounted for nearly 30

¹ 2013 Data Breach Investigations Report, Verizon.

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

percent of credit and debit card charges but 47 percent of all fraud losses.³ Credit and debit card fraud losses totaled \$11.27 billion in 2012.⁴ And retailers spend \$6.47 billion trying to prevent card fraud each year.⁵

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

Online fraud is a significant problem. It has jumped 36 percent from 2012 to 2013.⁹ In fact, estimates are that online and other fraud in which there is no physical card present accounts for 90 percent of all card fraud in the United States.¹⁰ And, not surprisingly, fraud correlates closely with data breaches among consumers. More than 22 percent of breach victims suffered fraud while less than 3 percent of consumers who didn’t have their data breached experienced fraud.¹¹

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

⁴ “Credit Card and Debit Card Fraud Statistics,” CardHub 2013, available at <http://www.cardhub.com/edu/credit-debit-card-fraud-statistics/>.

⁵ *Id.*

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

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

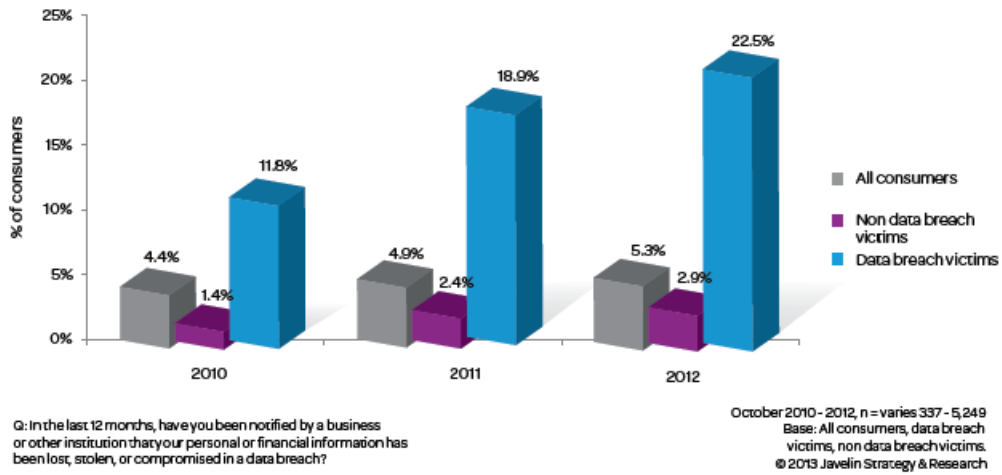
⁸ “House of Cards: Why your accounts are vulnerable to thieves,” Consumer Reports, June 2011.

⁹ 2013 True Cost of Fraud, LexisNexis at 6.

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

¹¹ 2013 True Cost of Fraud, LexisNexis at 20.

Figure 11. Fraud Incidence Rate Among All Consumers, Data Breach Victims, And Non Data Breach Victims (2010 -2012)



Source: 2013 True Cost of Fraud, LexisNexis

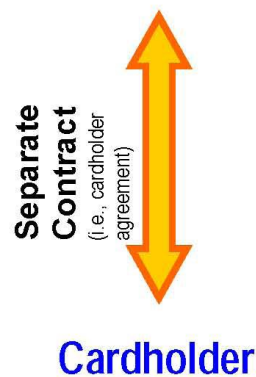
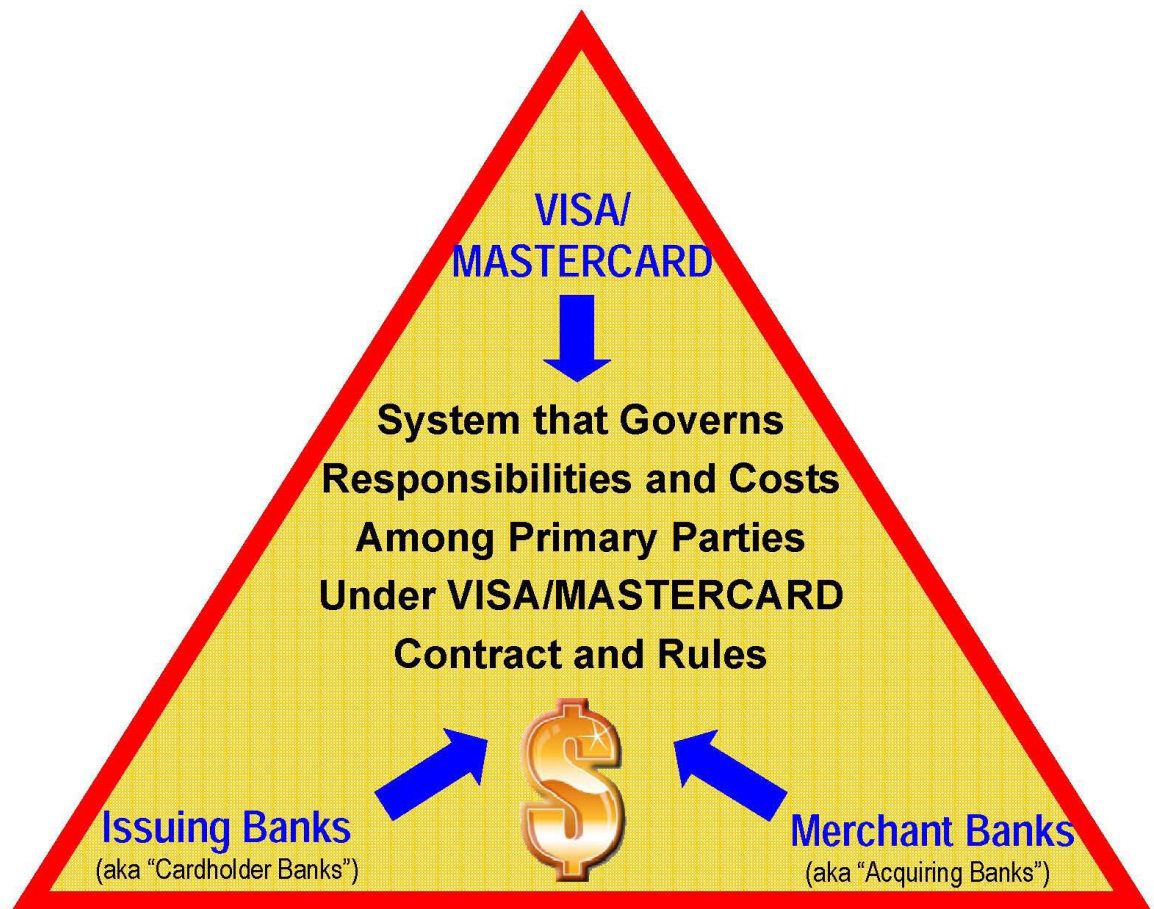
These numbers provide insights as to how to get to the right solutions of better safeguarding consumer and cardholder data and the need to improve authentication of transactions to protect against fraud. But before delving into those areas, some background on our payments system could be helpful.

The Payments System

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

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

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



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

Thus consumers are obligated to keep their cards safe and secure in their wallets and avoid misuse, but must necessarily turn their card data over to others in order to effectuate a

transaction. Retailers are likewise obligated to collect and protect the card data they receive, but are obligated to deliver it to processors in order to complete a transaction, resolve a dispute or process a refund. In contrast, those inside the triangle have much more systemic control.

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

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

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

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

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

In fact, cards include the cardholder’s name, card number, expiration date, signature and card verification value (CVV) code. Everything a fraudster needs is right there on the card. The

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

bottom line is that cards are poorly designed and fraud-prone products that the system has allowed to continue to proliferate.

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

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

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

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

Improved Technology Solutions

There are technologies available that could reduce fraud. An overhaul of the fraud-prone cards that are currently used in the U.S. market is long overdue. As I noted, requiring the use of a PIN is one way to reduce fraud. Doing so takes a vulnerable piece of data (the card number) and makes it so that it cannot be used on its own. This ought to happen not only in the brick-

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

¹⁵ *Id.* at 46262.

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

and-mortar environment in which a physical card is used but also in the online environment in which the physical card does not have to be used. Canada, for example, is exploring the use of a PIN for online purchases. The same should be true here. Doing so would help directly with the 90 percent of U.S. fraud which occurs online. It is not happenstance that automated teller machines (ATMs) require the entry of a PIN before dispensing cash. Using the same payment cards for purchases should be just as secure as using them at ATMs.

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

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

Another technological solution that could help deter and prevent data breaches and fraud is encryption. Merchants are already required by PCI standards to encrypt cardholder data but, as noted earlier, not everyone in the payments chain is required to be able to accept data in encrypted form. That means that data may need to be de-encrypted at some points in the process. Experts have called for a change to require "end-to-end" (or point-to-point) encryption which is simply a way to describe requiring everyone in the payment-handling chain to accept, hold and transmit the data in encrypted form.

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

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

According to the September 2009 issue of the Nilson Report “most recent cyberattacks have involved intercepting data in transit from the point of sale to the merchant or acquirer’s host, or from that host to the payments network.” The reason this often occurs is that “data must be decrypted before being forwarded to a processor or acquirer because Visa, MasterCard, American Express, and Discover networks can’t accept encrypted data at this time.”¹⁸

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

Tokenization is another variant that could be helpful. Tokenization is a system in which sensitive payment card information (such as the account number) is replaced with another piece of data (the “token”). Sensitive payment data could be replaced with a token to represent each specific transaction. Then, if a data breach occurred and the token data were stolen, it could not be used in any other transactions because it was unique to the transaction in question. This technology has been available in the payment card space since at least 2005.¹⁹

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

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

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

In this section, I have merely described some of the solutions available, but the United States isn’t using any of them the way that it should be. While everyone in the payments space has a responsibility to do what they can to protect against fraud and data theft, the card networks

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

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

have arranged the establishment of the data security requirements and yet, in light of the threats, there is much left to be desired.

A Better System

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

Steps Taken by Retailers After Discovery of a Breach of Security

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

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

Breaches require retailers to devote significant resources to remedy the breach, help inform customers and take preventative steps to ward off future attacks and any other potential vulnerabilities discovered in the course of the breach investigation. Weeks or months of forensic analysis may be necessary to definitively discover the cause and scope of the breach. Any discovered weaknesses must be shored up. Quiet and cooperative law enforcement efforts may be necessary in an effort to identify and capture the criminals. Indeed, law enforcement may

temporarily discourage publication of the breach so as to not alert the perpetrators that their efforts have been detected.

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

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

Legislative Solutions

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

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

We also support legislation that provides more tools to law enforcement to ensure that unauthorized network intrusions and other criminal data security breaches are thoroughly investigated and prosecuted, and that the criminals that breach our systems to commit fraud with our customers' information are swiftly brought to justice.

Finally, and for nearly a decade, NRF has supported passage of legislation that would establish one, uniform federal breach notification law that would be modeled on, and preempt, the varying breach notification laws currently in operation in 46 states, the District of Columbia and federal territories. A federal law could ensure that all entities handling the same type of sensitive consumer information, such as payment card data, are subject to the same statutory rules and penalties with respect to notifying consumers of a breach affecting that information. Further, a preemptive federal breach notification law would allow retailers and other businesses

that have been victimized by a criminal breach to focus their resources on remedying the breach and notifying consumers rather than hiring outside legal assistance to help guide them through the myriad and sometimes conflicting set of 50 data breach notification standards in the state and federal jurisdictions. Additionally, the use of one set of standardized notice rules would permit the offering to consumers of the same notice and the same rights regardless of where they live.

Conclusion

In closing three points are uppermost.

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

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

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



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

Statement for the Record

Bob Russo
General Manager
Payment Card Industry Security Standards Council

Senate Judiciary Committee
United States Senate

Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime

February 4, 2014

Introduction

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

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

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

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

Payment card security: a dynamic environment

Since the threat landscape is constantly evolving, the PCI SSC expects its standards will do the same. Confidence that businesses are protecting payment card data is paramount to a healthy economy and

payment process—both in person and online. That's why to date, more than one thousand of the world's leading retailers, airlines, banks, hotels, payment processors, government agencies, universities, and technology companies have joined the PCI Council as members and as part of our assessor community to develop security standards that apply across the spectrum of today's global multi-channel and online businesses.

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

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

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

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

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

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

EMV Chip & PCI Standards—a strong combination

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

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

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

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

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

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

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

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

Beyond Standards – building a support infrastructure

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

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

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

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

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

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

Public – private collaboration

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

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

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

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

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

Conclusion

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

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

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

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

###



1700 NORTH MOORE STREET
SUITE 2250
ARLINGTON, VA 22209
T (703) 841-2300 F (703) 841-1184
WWW.RILA.ORG

February 4, 2014

Senator Patrick Leahy
Chairman
Senate Committee on the Judiciary
United States Senate
224 Dirksen Senate Office Building
Washington, D.C. 20510

Senator Charles Grassley
Ranking Member
Senate Committee on the Judiciary
United States Senate
152 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Leahy and Senator Grassley:

On behalf of the Retail Industry Leaders Association (RILA), I welcome the opportunity to offer our comments on the record relevant to the Committee's hearing, "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime." RILA is the trade association of the world's largest and most innovative retail companies. RILA promotes consumer choice and economic freedom through public policy and industry operational excellence. Its members include more than 200 retailers, product manufacturers, and service suppliers, which together account for more than \$1.5 trillion in annual sales, millions of American jobs and operate more than 100,000 stores, manufacturing facilities and distribution centers domestically and abroad.

Retailers take the threat of cyber attacks extremely seriously and work diligently every day to stay ahead of the sophisticated criminals behind them. Retail companies individually and the industry collectively, are taking aggressive steps to counter these threats. While enhanced security measures help retailers thwart cyber-attacks nearly every day, unfortunately some attacks are successful and the resulting incidents can affect millions of our American customers. For retailers, such a breach can damage the relationship that we have with our customers. However, more broadly, a breach can undermine consumers' faith in the electronic payments system, as stolen information can be used to produce fraudulent cards for illicit use.

Given these facts, retailers take extraordinary steps to strengthen overall cybersecurity and prevent attacks. Retailers secure their systems with substantial investments in experts and technology. Retailers employ many tactics and tools to secure data, such as data encryption, tokenization and other redundant internal controls, including a separation of duties. While these enhanced security measures help to rebuff attacks, retailers are constantly working to expand existing cybersecurity efforts.

Collaboration within the industry and coordination with other stakeholders is essential. On January 27, RILA launched its Cybersecurity and Data Privacy Initiative which focuses on strengthening overall cybersecurity. As part of this initiative, RILA is forming the Retail Cybersecurity Leaders Council (RCLC) and calling for the development of both federal data breach notification legislation and federal cybersecurity legislation. Made up of senior retail executives responsible for cybersecurity, the RCLC will aim to improve industry-wide cybersecurity by providing a trusted forum for all stakeholders to share threat information and discuss effective security solutions.

In the weeks ahead, this Committee and others are likely to consider a range of legislative solutions to cybersecurity threats. RILA will engage with federal lawmakers and other stakeholders to develop sound and effective data breach notification and federal cybersecurity legislation that sets a national baseline to preempt the current patchwork of state laws and supports information sharing between the public- and private sectors.

While retailers understand and manage their internal systems and security, they have little or no influence over the actions taken by other players in the payments universe, actions with enormous implications on fraud. Instead, retailers must rely on others in the payments ecosystem to dictate critical security decisions, including card technology, retailer terminals, and when data can be encrypted during the transmission between retailers and the card networks. Retailers have long argued that the card technology in place today is antiquated and because of that criminals can use stolen consumer data to create counterfeit cards with stunning ease. For years, retailers have urged banks and card networks to adopt the enhanced fraud prevention technology in use around the world here in the United States. While their resistance to doing so has been great, retailers continue to press all other stakeholders in the payments system to make this a priority.

Also as part RILA's Initiative, RILA called for collaboration among retailers, banks and card networks to advance improved payments security. The RILA plan focused on four major steps that should be taken to improve the security of debit and credit cards. First, quickly establish a plan to retire the antiquated magnetic stripe technology in place today. Second, require cardholders to input a PIN on all card transactions. Banks require that cardholders enter a PIN number to withdraw money from an ATM, the same fraud protection should apply to retail transactions. Third, establish a roadmap to migrate to chip-based smart card technology with PIN security, also known as Chip and PIN. Finally, recognizing that card security must outpace

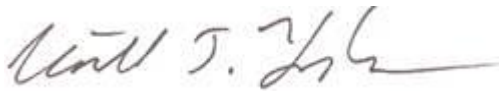
criminal advancements, the members of the payments ecosystem must work together to identify new technologies and long-term, comprehensive solutions to the threats.

We have little doubt that all parties share the goals of protecting consumers and maintaining confidence in our industry's cybersecurity. In order to accomplish these goals, the perpetual adversaries that make up the payments ecosystem must work together. That is why RILA is reaching out to representatives across the merchant community, as well as those representing the card networks and financial institutions of all sizes, in an effort to work together to identify near- and long-term solutions.

By working together with public-private sector stakeholders, our ability to develop innovative solutions and anticipate threats will grow, enhancing our collective security and giving our customers the service and peace of mind they deserve.

We look forward to working with the Committee and request that these comments be included in the record.

Sincerely,

A handwritten signature in black ink, appearing to read "William J. Hughes", with a long horizontal flourish extending to the right.

William Hughes
Senior Vice President, Government Affairs
Retail Industry Leaders Association