CONFIDENTIALITY COALITION

Statement of the Confidentiality Coalition

The Confidentiality Coalition respectfully submits this Statement to the Senate Judiciary Committee in connection with its February 4, 2014, hearing on "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime."

The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, patient groups, and others founded to advance effective patient confidentiality protections.

The Coalition's mission is to advocate policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions. The Confidentiality Coalition is committed to ensuring that consumers and thought leaders are aware of the privacy protections that are currently in place. As healthcare providers make the transition to a nationwide, interoperable system of electronic health information, the Confidentiality Coalition members believe it is essential to replace the current mosaic of sometimes conflicting state healthcare privacy laws, rules, and guidelines with a strong, comprehensive national confidentiality standard for healthcare information.

Our Coalition members strongly support appropriate activities to protect the confidentiality of personal information. The current privacy and security rules for the healthcare industry and its business associates stem from the regulations implemented following the passage of the Health Insurance Portability and Accountability Act (HIPAA)

in 1996. These rules – which have been in effect for more than a decade for health care companies and now apply directly to business associates as well – provide specific and detailed requirements for the protection of personal health information.

We support the approach the Committee takes regarding healthcare in the proposed language in sections 201 and 211 of the Personal Data Privacy and Security Act of 2014 (S.1897). This legislation provides important new consumer protections, while providing an exemption from the bill's new data security and breach notification provisions for entities subject to the HIPAA rules, including both covered entities and business associates. We believe that the current HIPAA Rules provide appropriate protections for the confidentiality of personal health information. Imposing additional, duplicative and potentially inconsistent regulation on these companies would create unnecessary and inappropriate burdens and costs. Therefore, we strongly support the Committee's efforts to exempt HIPAA covered entities and business associates from the provisions of this bill.

CUNA
Credit Union National Association

Bill Cheney
President & CEO

601 Pennsylvania Ave., NW
South Building, Suite 600
Washington D.C 20004-2601

Phone: 202-508-6745
Fax: 202-638-7734
bcheney@cuna.coop

February 4, 2014

The Honorable Patrick Leahy
Chairman
Committee on the Judiciary
United State Senate
Washington, DC 20510

The Honorable Chuck Grassley
Ranking Member
Committee on the Judiciary
United State Senate
Washington, DC 20510

Dear Chairman Leahy and Ranking Member Grassley:

On behalf of the Credit Union National Association (CUNA) and America's credit unions, I am writing today to thank you for holding today's hearing entitled "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime." CUNA is the largest credit union advocacy organization in the United States, representing America's 6,700 state and federally chartered credit unions and their 99 million members.

This hearing is an important and timely response to recent merchant data breaches affecting millions of Americans and their financial institutions. We appreciate the Committee's focus on safeguarding consumer data, and we look forward to today's testimony and discussion of what should be done to ensure an appropriate response to not only these data breaches, but data breaches that may occur next week, next month, or next year.

We encourage Congress to take a holistic approach to this issue. In the years to come, consumers will use many payment methods, including magnetic (mag) stripe cards, chip and PIN cards (EMV), cloud-based mobile payments, tokenization, and other methods we can only imagine at this point in time. Focusing on one payment method as the absolute answer to solving data security breaches is both shortsighted and distracts from the greater need of a federal data security framework for all entities. Instead, Congress should take a broad look at how consumer data is secured and the improvements that are necessary to prevent future breaches from taking place.

Data breaches occur, in part, because merchants are not required to adhere to the same statutory data security standards that credit unions and other financial institutions must follow, and merchants are rarely held accountable for the costs others incur as a result of the breaches. All participants in the payment process have a shared responsibility to protect consumer data, but the law and the incentive structure today allows merchants to abdicate that responsibility, making consumers vulnerable.

Since the initial reporting of the Target data breach, credit unions have focused on protecting their members from harm, to the extent they can. They have taken many steps including, but not limited to, notifying their members that a breach had occurred, reissuing new debit and credit cards to affected members, and increasing staff at call centers to account for additional member inquiries.

The impact of merchant data breach related costs is far reaching; for not-for-profit credit unions operating on already thin margins, these costs make a significant difference in their ability to offer services to their members. CUNA recently conducted a survey of credit unions regarding the costs they are incurring to help their members respond and recover from the recent breach at Target. Preliminary data indicates that credit unions are incurring a cost of approximately $5.10 per affected card and that the system has incurred a total estimated cost of between $25-30 million as a result of this breach. This figure will continue to increase because this data does not include fraud costs which may develop in the near future.

In addition to the actual costs credit unions must bear as result of the breach, they also face reputational damage because they have an obligation to notify their members that their account has been compromised but are often limited in their ability to disclose the name of the merchant where the breach occurred. So, when members are notified that their account has been compromised, the credit union is unable to tell them where the compromise occurred and some members assume the problem was with the credit union.

As Congress considers legislative remedies, credit unions support three basic principles:

1. All participants in the payments system should be responsible and be held to comparable levels of data security requirements.

Under current federal law, credit unions and other financial institutions are held to high standards of data security for consumer information under the *Gramm-Leach-Bliley Act*. There is no comparable federal data security responsibility for a national merchant holding consumer data. This represents a weak link in the chain and it needs to be addressed. We support legislation, such as S. 1927, the *Data Security Act of 2014*, introduced by Senators Carper and Blunt, that would provide a national standard for businesses to protect sensitive consumer information, rather than a myriad of differing state laws and regulations.

2. Those responsible for the data breach should be responsible for the costs of helping consumers.

It has been said by merchants that consumers will not be responsible for any financial loss in their accounts. That is true, but not because the merchant will reimburse affected consumers. It happens because the consumer's financial institution pays for the costs related to a merchant data breach involving accounts held at that institution. Under current law, the merchant is not obligated to reimburse financial institutions for any costs incurred as a result of the breach. In other words, even though the breach happened on the merchant's watch, retailers have no responsibility for the costs of the breach because financial institutions take care of their members and customers.

When a merchant data breach occurs, credit unions are there to help their members. Whether it is increased staffing to handle additional member questions, notifying members, reissuing cards, tracking possible fraudulent activity, or reimbursing a member for fraudulent charges caused by a third party, credit unions bear the costs even though the merchant was

responsible for the breach. We support legislation to address this problem and make it easier for credit unions to recoup the costs they incur. We believe that if Congress sets strong merchant data security standards and those standards are not met by a merchant whose data is breached, the merchant should be held responsible for the credit union's costs associated with that breach.

3. Consumers should know where their information was breached.

Credit unions also support legislation that requires merchants to provide notice to those consumers affected by a data breach, and permits credit unions to disclose where a breach occurs when notifying members that their account has been compromised.

When it comes to bad news like a data breach, it is easy to "blame the messenger." In today's world, the credit union is the messenger and, depending on the state, may not be permitted to identify the breach source to the consumer member. Consumers need transparency and knowledge to understand where their data has been put at risk. S. 1927 addresses this priority as well.

In conclusion, we look forward to the Committee's dialogue regarding data security. It is a complicated and dynamic issue. As these latest merchant breaches have demonstrated, millions of consumers, and their respective credit unions, are affected. We believe the best answer is a federal comprehensive approach to data security.

On behalf of America's credit unions and their 99 million members, thank you for your attention to this very critical matter and your consideration of our views.

Best regards,

Bill Cheney
President & CEO

February 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 to 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

Michaels
Where Creativity Happens

MICHAEL J. VEITENHEIMER
SVP, Secretary & General Counsel
Direct Dial: 972-409-1655
Telecopier: 972-409-1965
veitenhm@michaels.com

January 31, 2014

The Honorable Patrick Leahy
Chairman
Senate Committee on the Judiciary
221 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Leahy:

Thank you for your invitation to Michaels Stores, Inc. to testify on February 4, 2014 at the Senate Judiciary Committee hearing on "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime." I am writing to respectfully decline your invitation.

As you are aware, on January 25, 2014, Michaels issued a press release and posted a letter on our corporate website from our CEO Chuck Rubin to Michaels customers. In this letter, we noted that Michaels recently learned of possible fraudulent activity on some U.S. payment cards that had been used at our stores, suggesting that we may have experienced a data security attack. We took this action in the interest of consumer protection and in the context of great public attention to data security attacks against other retailers. Immediately, upon knowledge of this possible fraudulent activity, we began working closely with federal law enforcement officials, and we continue to do so. Additionally, we are conducting an investigation with the assistance of third-party data security experts to establish all of the facts. At this time, the investigation of this matter is ongoing and will not be completed by the date of your Committee hearing. Therefore, we are unable to testify about this matter.

Our first priority is our customers, and we are committed to protecting the safety and integrity of their privacy and data. The topic of your hearing is one we take very seriously at Michaels, and for that reason it is imperative that a full and fair investigation of this matter be completed before further comment. Additionally, we appreciate that your constituents in Vermont are also our customers. Their privacy and security is of critical importance to us, and we will continue to address this issue with vigilance. When a full investigation of this matter is concluded, we will appropriately inform you of relevant information in our findings.

Thank you again for your invitation, and I look forward to working with you in the future.

Sincerely,

Michael J. Veitenheimer

8000 BENT BRANCH DRIVE
IRVING, TEXAS 75063
972.409.1300

NAFCU

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 Welsh 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.

Symantec

SECURITY RESPONSE

A SPECIAL REPORT ON

Attacks on Point of Sales Systems

Version 1.0 – February 3, 2014

“Cybercrime gangs organize sophisticated operations to steal vast amounts of card data before selling it in underground marketplaces.”

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

CONTENTS

OVERVIEW

Credit and debit card data theft is one of the earliest forms of cybercrime and persists today. Cybercrime gangs organize sophisticated operations to steal vast amounts of data before selling it in underground marketplaces. Criminals can use the data stolen from a card's magnetic strip to create clones. It's a potentially lucrative business with individual cards selling for up to $100.

There are several routes attackers can take to steal this data. One option is to gain access to a database where card data is stored. But another option is to target the point at which a retailer first acquires that card data – the Point of Sale (POS) system.

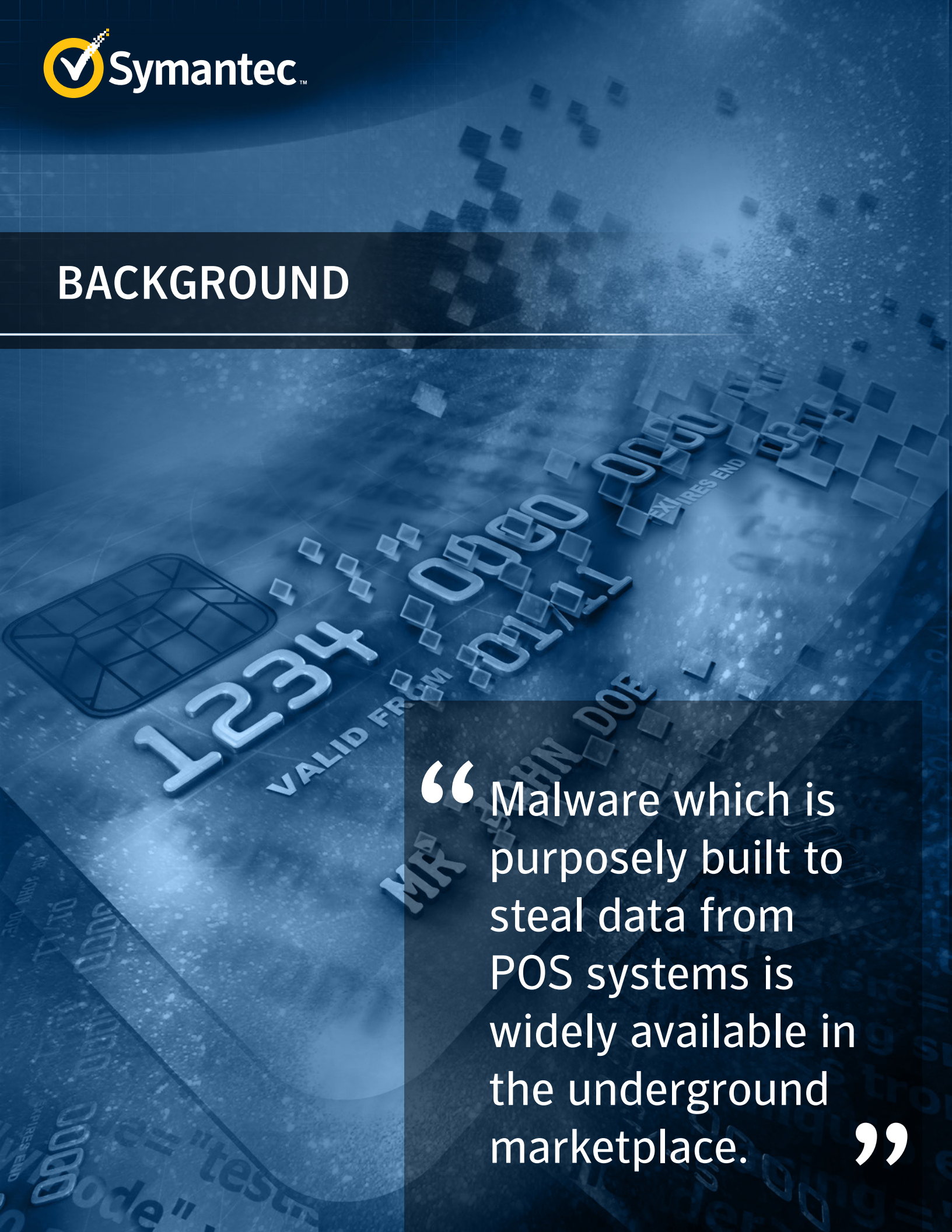
Modern POS systems are specially configured computers with sales software installed and are equipped with a card reader. Card data can be stolen by installing a device onto the card reader which can read the data off the card's magnetic strip. This is a process known as "skimming". As this requires additional hardware and physical access to the card reader it is difficult to carry out this type of theft on a large scale.

This led to the development of malware which can copy the card data as soon as it's read by the card reader. The first such attacks of this type were seen in 2005 with a series of campaigns orchestrated by Albert Gonzalez. These attacks led to the theft of over 170 million card numbers. Since then, an industry has developed around attacking POS systems, with tools readily available on the underground marketplace.

Despite improvements in card security technologies and the requirements of the Payment Card Industry Data Security Standard (PCI DSS), there are still gaps in the security of POS systems. This coupled with more general security weaknesses in corporate IT infrastructure means that retailers find themselves exposed to increasingly resourceful and organized cybercriminal gangs.

Symantec

BACKGROUND



> “Malware which is purposely built to steal data from POS systems is widely available in the underground marketplace.”

Background

The term POS (Point of Sale) device most commonly refers to the in-store systems where customers pay merchants for goods or services. While many POS transactions are in the form of cash, many of these payments are made by customers swiping their cards through a card reader. These card readers may be standalone devices but modern POS systems, particularly those in larger retailers, are all-in-one systems which can handle a variety of customer transactions such as sales, returns, gift cards and promotions. Most importantly from a security standpoint, they can handle multiple payment types.

Given the sensitive financial and sometimes, personal data to which modern POS systems have access, it is an obvious but not always well recognized fact that the security of these systems is of utmost importance.

POS security issues

Many all-in-one POS systems are based on general purpose operating systems such as Windows Embedded, Windows XP and later versions, and Unix operating systems including Linux. Consequently, these systems are susceptible to a wide variety of attack scenarios which could lead to large scale data breaches.

Accessibility

All organizations that handle payment card data are required to implement safeguards set down in the Payment Card Industry (PCI) Data Security Standard (DSS). These standards help organizations to ensure that their systems and procedures are properly secured. The standard describes a concept known as the cardholder data environment (CDE) and the need to protect it. This is defined as "The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components."

The current standards recommend, but do not require the CDE to be network-segmented from other non-POS systems and the public Internet. While a strictly controlled and completely isolated POS system network would be quite secure, it is too impractical for serious consideration. The POS systems must be accessible for software updates and maintenance, allow business data to be exported to other systems (e.g. purchasing data and inventory), to export system and security logs, have access to required support systems such as network time protocol (NTP) servers (as required by PCI standards), and have connectivity to external payment processors.

Despite lacking a rule for segmentation, the PCI standards do mandate certain levels of access security, for example, if remote access from a public network is allowed, the access must employ two-factor authentication. In most mature retail environments, the CDE is appropriately segmented to reduce risk. However, in these environments pathways still exist from the general corporate network to the CDE.

While previous breaches have occurred by gaining direct access to POS systems, the most common attack route against POS systems is through the corporate network. Once an attacker gains access to the corporate network, for example through a vulnerable public facing server or spearphishing email, the attacker could traverse the network until they gain access to an entry point to the POS network. This entry point is often the same as a corporate administrator would utilize to maintain the POS systems.

Lack of point to point encryption (P2PE)

When an individual pays by swiping a card credit at a POS system, data contained in the card's magnetic stripe is read and then passed through a variety of systems and networks before reaching the retailer's payment processor. When this data is transmitted over a public network, the data must be protected using network level encryption (e.g. secure socket layer (SSL)).

However, within internal networks and systems, the credit card number is not required to be encrypted except when stored. Albert Gonzalez famously took advantage of this weakness in 2005 by infiltrating many retail networks and installing network sniffing tools allowing him to collect over a hundred million credit card numbers as they passed through internal networks.

In response, many retailers today use network level encryption even within their internal networks. While that change protected the data as it travelled from one system to another, the credit card numbers are not encrypted in the systems themselves, and can still be found in plain text within the memory of the POS system and other computer systems responsible for processing or passing on the data. This weakness has led to the emergence of "RAM scraping" malware, which allows attackers to extract this data from memory while the data is being processed inside the terminal rather than when the data is travelling through the network.

Secure card readers (SCR) exist and have been implemented in some environments enabling P2PE, this can defeat RAM scraping attacks that work by searching the memory of the POS system for patterns of digits that matches those of payment card numbers. Such card readers encrypt the card data at time of swipe and the credit card number remains encrypted throughout the process even within the memory and underneath network level encryption.

Using P2PE within POS environments is not a new concept. Items such as PINs, when used with debit cards must be encrypted at the PIN pad terminal. When provisioning terminals, a payment processor or sponsor must provision the terminal by performing "key injection" where a unique encryption key is deployed directly to the device. With this scheme, the PIN remains encrypted at all times.

Software vulnerabilities

The majority of POS systems are running the older Windows XP version of Windows Embedded. This older version is more susceptible to vulnerabilities and therefore more open to attack. It should also be noted that support for Windows XP will end on April 8, 2014. In practice this means, no more patches will be issued for any software vulnerabilities found in the operating system from the cutoff date. This event will certainly place POS operators under increased risk of a successful attack and POS operators should already have mitigation plans in place to meet this coming deadline.

Susceptibility to malicious code

As many POS systems are running a version of Windows, they are also capable of running any malware that runs on Windows. This means that attackers do not need specialized skills in order to target POS systems and malware that were not specifically designed for use on POS systems could be easily repurposed for use against them.

Slow adoption of EMV

Europay, Mastercard and VISA (EMV) is a set of standards for card payments. It is often referred to as "Chip and PIN" and is a replacement for traditional magnetic stripe based cards. EMV cards contain embedded microprocessors that provide strong transaction security features. EMV never transmits the credit card data in the clear mitigating many common POS attacks. EMV cards are also less attractive to attackers as they are difficult to clone.

While EMV is commonly used in some parts of the world such as Europe, US merchants in particular have been slow to adopt the EMV standard and will not start implementing it until 2015.

Typical anatomy of attacks against POS systems

Attacks against POS systems in mature environments are typically multi-staged. First, the attacker must gain access to the victim's network. Usually, they gain access to an associated network and not directly to the CDE. They must then traverse the network, ultimately gaining access to the POS systems. Next, they will install malware in order to steal data from the compromised systems. As the POS system is unlikely to have external network access, the stolen data is then typically sent to an internal staging server and ultimately exfiltrated from the retailer's network to the attacker.

Infiltration

There are a variety of methods an attacker can use to gain access to a corporate network. They can look for weaknesses in external facing system, such as using an SQL injection on a Web server or finding a periphery device that still uses the default manufacturer password. Alternatively they can attack from within by sending a spearphishing email to an individual within the organization. The spearphishing email could contain a malicious attachment or a link to a website which installs a back door program onto the victim's machine.

Network traversal

Once inside the network, the attackers need to gain access to their ultimate targets – the POS systems. Attackers will typically use a variety of tools to map out the network in order to locate systems within the CDE. While they may use vulnerabilities or other techniques to gain access to these systems, often the simplest, yet effective method of gaining access is by obtaining user credentials. User credentials may be obtained through keylogging Trojans, password hash extraction, cracking, and/or replaying captured login sequences, or even brute force. Eventually, administrative level credentials may be obtained. Attackers may even gain control of a domain controller, giving them full access to all computers in the network. Once in control, they can then gain access to the CDE even if it is in a segmented network by using network and data pathways established for existing business purposes. Once inside the CDE, they then install malware which allows them to steal card data from the POS systems.

Data-stealing tools

Malware which is purposely built to steal data from POS systems is widely available in the underground marketplace. In some attacks, network sniffing tools are used to collect credit card numbers as they traversed internal unencrypted networks. Other times, RAM scraping malware is used to collect credit numbers as they are read into computer memory. Any collected data is then stored in a file locally until time for exfiltration. Often, this data file needs to be transferred to multiple computers hopping through the internal network until reaching a system that has access to external systems.

Persistence and stealth

Because the attacker is targeting a POS system and these attacks take time to gather data, they will need their code to remain persistent. Unlike database breaches where millions of records are accessible immediately, POS system breaches require the attacker to wait until transactions happen and then collect the data in real-time as each credit card is used. Because of this, early discovery of the attack can limit the extent of the damage. Malware persistence can be achieved using simple techniques to ensure the malware process is always running and restarts on any system restart.

Stealth techniques used will vary from simplistic obfuscation of filenames and processes to specific security software bypass techniques. In more secure environments, in order for attackers to succeed, they will likely already have access to compromised administrative credentials and can use them to scrub logs, disable monitoring software and systems, and even modify security software configuration (e.g. change file signing requirements or modify whitelisting entries) to avoid detection.

Exfiltration

The attackers may hijack an internal system to act as their staging server. They will attempt to identify a server that regularly communicates with the POS systems and piggyback on normal communications to avoid detection. Any data collected by the RAM-scraping malware will be sent to this staging server where it stored and aggregated until a suitable time to transmit to the attacker. At the appropriate time, the attackers may transfer the collected data through any number of other internal systems before finally arriving at an external system such as a compromised FTP server belonging to a third party. By using compromised servers from legitimate sites to receive the stolen data, the traffic to these sites are less likely to arouse suspicion on the part of the compromised retailer, particularly if they are sites that are often visited by users within the victim organization.

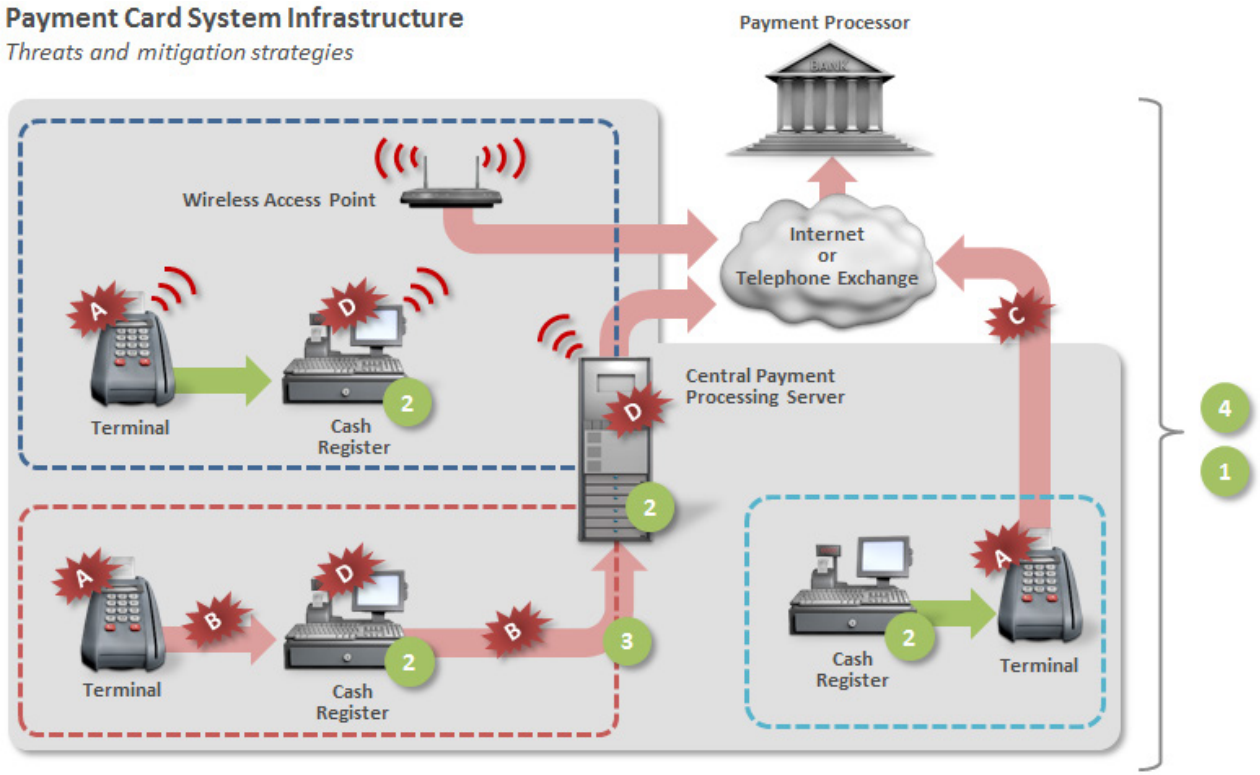
Symantec

PROTECTING POS SYSTEMS FROM ATTACK

> “There are many steps that POS operators can take to reduce the risk from attacks against POS systems.”

Protecting POS systems from attack

There are many steps that POS operators can take to reduce the risk from attacks against POS systems. The following diagram illustrates the typical infrastructure of payment card systems and the threats against them along with mitigation strategies that can be employed at various points in the system.



Threats

- **A** — Attacks on terminals. Skimmers, firmware, inserted hardware
- **B** — Network traffic sniffing
- **C** — Public network communication is susceptible if system is not PCI compliant or if there is a breach or flaw in the system. E.g. exposure of encryption key
- **D** — RAM scraping attack

Mitigation Strategies

1. Use a firewall, even between corporate networks
2. Endpoint security software
3. Double encrypt data (Encrypt data and then use SSL)
4. Security Information and Event Management (SIEM)

Method of operation

- Dumb terminal method. Terminal used as "PIN pad" only. Credit card details sent to cash register which in turn requests authorization.
- Smart terminal/Direct method. Transaction is requested directly by the terminal using phone line or Internet. Credit card numbers is not transmitted to the cash register.
- Wireless network scenario. PCI DSS requires WPA security. Can use either method.

Figure: Threat to payment card system and possible mitigation strategies

Practical steps to take

- Implementation of PCI Security Standards
  - Install and maintain a firewall to facilitate network segmentation
  - Change default system passwords and other security parameters
  - Encrypt transmission of cardholder data across open, public networks
  - Encrypt stored primary account number (PAN) and do not store sensitive authentication data
  - Use and regularly update security software
  - Use intrusion protection system (IPS) at critical points and the perimeter of the CDE
  - Use file integrity and monitoring software
  - Use strong authentication including two-factor authentication for remote systems
  - Monitor all network and data access (SIEM)
- Test security systems, perform pen-testing, and implement a vulnerability management program
- Maintain security policies and implement regular training for all personnel
- Implement multi-layered protections including outside the CDE. Typically, the attacker will need traverse multiple networks and layers of security before reaching a POS system. Any single layer that the attacker is unable to bypass prevents successful data exfiltration.
- Implement P2PE or EMV ("Chip and PIN")
- Increase network segmentation and reduce pathways between the CDE and other networks.
- Maintain strict auditing on connections to between the CDE and other networks. Reduce the number of personnel who have access to systems that have access to both the CDE and other networks.
- Employ two-factor authentication at all entry points to the CDE and for any personnel with access rights to the CDE
- Employ two-factor authentication for all system configuration changes within the CDE environment
- Implement system integrity and monitoring software to leverage features such as system lockdown, application control, or whitelisting

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems.

Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com