Testimony of

James A. Reuter

On behalf of the

American Bankers Association

before the

Subcommittee on National Security and International Trade and Finance

of the

Committee on Banking, Housing, and Urban Affairs

United States Senate

Testimony of James A. Reuter

On behalf of the

American Bankers Association

before the

Subcommittee on National Security and International Trade and Finance

of the

Committee on Banking, Housing, and Urban Affairs

United States Senate

February 3, 2014

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

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

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

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

In my testimony I will focus on four main points:

- **Protecting consumers is the banking industry's first priority.**
  As the stewards of the direct customer relationship, the banking industry's overarching priority in breaches like that of Target's is to protect consumers and make them whole from any loss due to fraud.

- **A National data breach standard is essential.** Consumers' electronic payments are not confined by borders between states. As such, a national standard for data security and breach notification is of paramount importance, and we strongly support S. 1927, the Data Security Act of 2014.

- **All players in the payments systems, including retailers, must significantly improve their internal security systems as the criminal threat continues to evolve.**

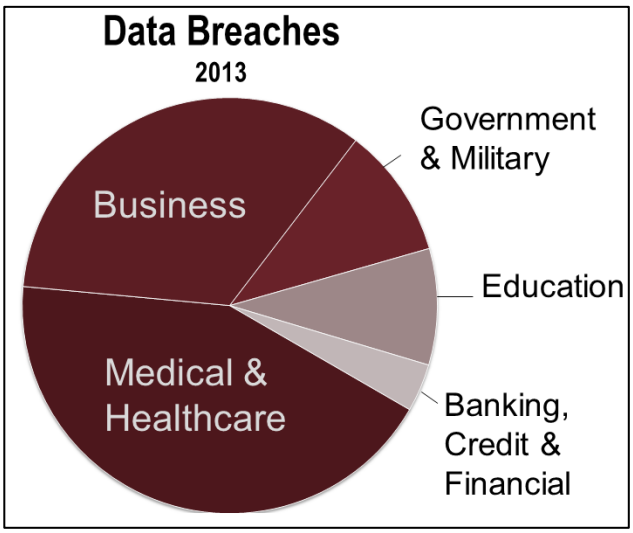
- **Protecting the Payments System is a Shared Responsibility.** Banks, retailers, processors, and all of the participants in the payments system must share the responsibility of keeping the system secure, reliable, and functioning in order to preserve consumer trust. That responsibility should not fall predominantly on the financial services sector.

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

I. Data Security: Where are the Vulnerabilities?

It is a sobering fact that, since January 2005, a total of over 4,200 breaches exposing almost 600 million records have occurred nationwide. (Source: Identity Theft Resource Center) There were over 600 reported data breaches during 2013 alone, an increase of 30 percent over 2012 and the third highest number of breaches over the last nine years. The two sectors reporting the highest number of breaches were the healthcare sector at 43 percent of reported breaches and the business sector, including merchants, which accounted for nearly 34 percent of reported breaches.

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



Source: Identity Theft Resource Center

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

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

II. Protecting Consumers is Our First Priority

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

Paying for Fraud

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

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

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

---

[2] With traditional card payments, the rights and obligations of all parties are well-defined by federal statute when an unauthorized transaction occurs. For example, Regulation E describes consumers' rights and card issuers' obligations when a debit card is used, while Regulation Z does so for credit card transactions. The payment networks also have well-established rules for merchants and issuers. For instance, while Regulation Z limits a customer's liability for unauthorized transactions on a lost or stolen credit card to $50, the card networks require issuers to provide their cardholders with zero liability.

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

inequitable. We believe banks should be fully reimbursed for the costs they bear for breaches that occur elsewhere.

Reissuing and Ongoing Monitoring

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

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

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

III. A National Data Breach Standard is Essential

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

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

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

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

to implement, maintain, and enforce reasonable policies and procedures to protect the confidentiality and security of sensitive information from unauthorized use.

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

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

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

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

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

- While Target's last public statement on the issue stated that the PINs that were compromised as part of the breach were encrypted, the company originally stated that PINs were not compromised at all. If the PINs were unencrypted, this would be particularly troubling, as that would make bank customer accounts vulnerable to ATM cash withdrawals as well as unauthorized purchases. We call on law enforcement and those in the forensics process to be as transparent as possible in outlining what are the precise threats to our customers.

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

- Even if the PINs that were breached were in fact encrypted, there is still the potential that they could be decrypted, placing our customers at just as much risk as if unencrypted PINs had been captured.
- Banks also do not know the extent to which their customers' bank account numbers, which are linked to Target's RedCard, were compromised as a result of the breach. If this information was compromised, customers could be vulnerable to unauthorized Automated Clearing House (ACH) transactions directly from their accounts.
- More generally, banks have also encountered significant customer confusion as to the nature of Target's RedCard and the bank's ability to help. Many believe the bank can cancel the card and reissue it even though the card was issued by Target. This confusion points to a broader problem with the emergence of many non-traditional payments providers: customers have a hard time understanding which payment entity is responsible for what, and often just assume the bank is the responsible party.

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

V. Protecting the Payments System is a Shared Responsibility

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

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

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

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

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

VI. The Path Forward

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

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

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

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

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

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

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

Banks are committed to doing our share, but cannot be the sole bearer of that responsibility. Policymakers, card networks, and all industry participants have a vital role to play in addressing the regulatory gaps that exist in our payments system, and we stand ready to assist in that effort. Thank

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

you for giving ABA the opportunity to provide this testimony. We look forward to continuing to work with Congress to enhance the security of our nation's payment system, and maintain the trust and confidence hundreds of millions of Americans place in it every day.