**Statement for the Record**

*On behalf of the*

**American Bankers Association**

**Consumer Bankers Association**

**Credit Union National Association**

**Independent Community Bankers of America**

**National Association of Federal Credit Unions**

**The Clearing House**

*before the*

**Financial Services Committee**
**United States House of Representatives**

Chairman Hensarling, Ranking Member Waters, and members of the Committee, the ABA, CBA, CUNA, ICBA, NAFCU and TCH appreciate the opportunity to submit for the record our combined views on the security of the payments system and in particular the recent breaches of security that have put literally millions of consumers at risk. Together, we represent thousands of banks and credit unions of all sizes.

The subject of today's hearing, "Protecting Consumers: Financial Data Security in the Age of Computer Hackers" is an important one. Our payment system remains strong and functional despite several highly-publicized data breaches at major retailers. Americans spend over $3 trillion safely and securely each year with their credit and debit cards. Customers can use these cards confidently because their financial institutions protect them from losses by investing in technology to detect and prevent fraud, reissuing compromised debit and credit cards and absorbing fraud costs**.**

At the same time, recent breaches have reignited the long-running debate over consumer data security policy. Banks and credit unions, from the smallest to the very largest, recognize the paramount importance of a safe and secure payments system to our nation and its citizens. We thank the Committee for holding this hearing and welcome the ongoing discussion. In our statement for the record we will focus on the following:

I. Data Security Risks and Vulnerabilities.

II. How to Improve Data Security.

# I. Data Security Risks and Vulnerabilities

## A. Data Breaches

Since January 2005 to May 6, 2015, over 5,000 breaches exposing more than 800 million records have occurred nationwide[1]. (Source: Identity Theft Resource Center) More than 100 million records have been compromised between January and May of this year – much of it due to the breach of healthcare provider, Anthem, Inc. in which 78 million records were compromised. While the healthcare sector currently accounts for the highest percentage of records compromised in 2015 (nearly 98 percent), the retail sector accounts for the most breaches at nearly 40 percent. 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 oftentimes the bank's and credit union's customer at the end of the line who must be protected.

## B. Protecting Consumers is Our First Priority

When a retailer or other breached party speaks of its customers having "zero liability" from fraudulent transactions, it is because our nation's banks and credit unions are making customers whole, not the retailer that suffered the breach. Financial institutions are required to swiftly research and reimburse customers for unauthorized transactions, and routinely exceed legal

[1] Note: These numbers are based on the known number of records publicly reported. The exact number of records exposed is not always known or reported at the time of the compromise.

requirements by making customers whole within days of the customer alerting the bank or credit union of the fraud, if not immediately.[2]

After the bank or credit union has reimbursed a customer for the fraudulent transaction, it can then attempt to "charge-back" the retailer where the transaction occurred. Unfortunately, the majority of these attempts are unsuccessful, with the bank or credit union ultimately shouldering the vast majority of fraud loss and other costs associated with the breach. **In 2013, 61 percent of fraud losses were borne by issuers, while 36 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 financial institutions have made customers whole) banks and credit unions generally receive *pennies for each dollar* of fraud losses and other costs that were incurred by banks in protecting their customers. This minuscule level of reimbursement, when taken in concert with the fact that banks and credit unions bear over 60 percent of reported fraud losses yet have accounted for less than 8 percent of reported breaches in the United States since 2005, is clearly inequitable.

According to a 2014 survey conducted by the American Bankers Association among their membership, only 33.1 percent of the 535 respondents reported having received any reimbursements for breaches between 2009 and 2014. Of those, the majority of respondents (83.1 percent) reported a reimbursement rate of no more than 10 cents on the dollar, with 46.2 percent reporting less than 1 cent on the dollar. Additionally, according to the Independent Community Bankers of America, recent wide-scale retailer data breaches resulted in community banks reissuing more than 11.5 million debit and credit cards at a cost of more than $130 million. That is why banks and credit unions should be fully reimbursed for the costs they bear for breaches that occur elsewhere.

Each bank and credit union makes its own decision as to when and whether to reissue cards, which on average costs banks about $3-13 per card depending upon the size of the institution and

---

[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] *2013 Interchange Fee Revenue, Covered Issuer Costs, and Covered Issuer and Merchant Fraud Loss Related to Debit Card Transactions,* September 2014, Board of the Governors of the Federal Reserve System, available at: http://www.federalreserve.gov/paymentsystems/files/debitfees_costs_2013.pdf

number and type of cards reissued. Those cards that have not been reissued are being closely monitored for fraudulent transactions. In addition to proactively communicating with customers about the breach, bank and credit union call centers and branches have handled millions of calls and in-person inquiries regarding the card compromise. Many smaller credit unions 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 financial institution, which is why they call us, not the retailer or whoever actually suffered the breach.

We also remain vigilant to the potential for fraud to occur in the future as a result of breaches. Standard fraud mitigation methods that banks and credit unions 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 and credit unions can afford to relax their ongoing fraud protection and screening efforts. In addition there are ongoing customer support issues as customer's set up new card numbers for recurring transactions related to health club memberships and online stores such as iTunes.

## II. What Can be done to Improve Data Security

## A. All Players in the Payments System Must Improve Their Internal Systems as Criminal Threats Continue to Evolve

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 major breaches at retailers and others 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 42 percent.[4]

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

## B. 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 financial services 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, credit unions, 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.

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.

---

[4] *2014 Cost of Data Breach Study: United States*, May 2013, Ponemon Institute.

[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.

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.

## C. 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 or credit unions rather than taking the reputational hit themselves. In such cases, the bank and credit union 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 and credit unions have expressed great frustration regarding this process, with their customers -- absent better information -- blaming the bank or credit union 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 and credit unions is governed by guidance from the Federal Financial Institutions Examination Council (FFIEC), as enacted in the Gramm-Leach-Bliley Act, requiring every bank and credit union 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 are not always consistent. Banks and credit unions 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, 47 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.

## D. The Data Security Act (H.R. 2205)

Establishing a national data security and notification law, and requiring any business that maintains sensitive personal and financial information – including banks, credit unions, 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, would provide better protection for consumers nationwide.

That is why we strongly support H.R. 2205 the Data Security Act of 2015, introduced by Financial Institutions Subcommittee Chairman Neugebauer (R-TX) and Representative Carney (D-DE). This important legislation would apply to all industries that handle sensitive information and would provide meaningful and consistent protection for consumers nationwide. H.R. 2205 recognizes that it is not necessary or productive to duplicate data protection and consumer notice requirements that are already in place for financial institutions under the Gramm-Leach-Bliley Act (GLBA) and subsequent regulations. Banks and credit unions already have a system in place that protects sensitive customer information and it makes sense to extend similar safeguards to other industries that handle sensitive information.

The reforms in the bill would effectively replace the current patchwork of state and federal regulations for data breaches with a national law that provides uniform protections across the country. This comprehensive approach would better serve consumers by making it easier for businesses and government agencies to take the steps necessary to adequately protect all Americans from identity theft and account fraud.

Our existing payments system serves hundreds of millions of consumers, retailers, financial institutions and the economy well. Protecting this system is a shared responsibility of all parties involved and we must work together and invest the necessary resources to combat increasingly sophisticated threats to the payments system. We look forward to working with you and your colleagues in the House on this important issue.