CUNA
Credit Union National Association

cuna.org

BILL CHENEY
President & CEO

601 Pennsylvania Ave., NW | South Building, Suite 600 | Washington, DC 20004-2601 | PHONE: 202-508-6745 | FAX: 202-638-3389

July 17, 2013

The Honorable Lee Terry, Chairman
Subcommittee on Commerce, Manufacturing and Trade
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Terry:

On behalf of the Credit Union National Association (CUNA), I am writing about today's hearing entitled "Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?" CUNA is the largest credit union advocacy organization in the United States, representing America's state and federally chartered credit unions and their 96 million members. We are pleased to offer comments for the hearing record on this very important topic.

The chain of data security is only as strong as its weakest link. A data breach can occur anywhere along the payments transaction, from the merchant, to the merchant bank, the issuing card bank, and ultimately the financial institutions. As we describe below, credit unions are subject to very high data security standards under the Gramm-Leach Bliley Act of 1999 (GLBA).[1] However, merchants are not required to follow these standards, and until they are held to the same standard, consumers will remain vulnerable to a system that does not protect their information.

We encourage Congress to consider legislation that holds merchants to the same standards as financial institutions when they handle financial transactions, and that permits financial institutions to disclose the source of the data breach and seek reimbursement from the merchant for the cost of the breach.

Merchant Data Breaches

Merchants benefit greatly from the electronic payments system. The largest benefit to the merchant is the elimination of risk they would otherwise have to assume if the transaction were paid with cash (theft risk, handling and security costs) or a check (bounce risk, which includes non-payment and collection expenses). Merchants also benefit from streamlined accounting, reduced credit risk, faster check-out and increased purchase amounts compared to checks or cash.[2]

[1] P.L. 106-102, Title V (November 12, 1999).
[2] Adam J. Levitin. ―Interchange Regulation: Implications for Credit Unions. Filene Research Institute. 6

AMERICA'S CREDIT UNIONS®

PO Box 431 | Madison, WI 53701-0431 | 5710 Mineral Point Road | Madison, WI 53705-4454 | PHONE: 608-231-4000

With the electronic payment system, card issuers, such as credit unions, assume all of the risk and guarantees the merchant will receive payment. In the process, the consumer receives a very important service: an efficient, convenient, seamless, and universally-accepted transaction. That very consumer service redounds to the benefit of merchants. The easier it is for a consumer to access his or her funds at the point of sale, the more likely he or she is to spend them on the goods or services the merchant is offering. There is tremendous benefit and value attached to the debit card, as evidenced by the significant increase in its acceptance by merchants and its use by consumers over the last decade.

The question is: What happens when something goes wrong? Unfortunately, merchant data breaches happen, and experience tells us, it is the card issuers who take the loss and take steps to protect the consumers. In the event of a merchant data breach there are no federal requirements for merchants to notify consumers of that breach. The onus of notification to the consumer lies on the financial institution that issued the payment card. However, financial institutions cannot specify which merchant was responsible for the breach and also bears the costs of issuing new payment cards, and making any loss to the consumer's account whole. The merchant bears no financial responsibility in the case of a data breach.

Merchants are not subject to federal data security requirements, nor are they financially liable for damages. In some cases, merchants do not even face reputational risk as a result of a breach because they are not required, under federal law, to disclose a breach. The financial institutions of consumers affected by the breach in most cases do not know the source of the breach, and when the source is known, are not permitted to identify the merchant responsible. While there are industry standards, merchants are not required by law to follow these standards.[3]

Until there are consequences to these bad actions, voluntary standards will not be sufficient to protect consumers. It is common sense that if merchants receive benefits from debit cards payments that they should be subject to the same high data security standards as financial institutions. To protect consumers, Congress should require merchants to be regulated to at least the same extent that financial institutions are when it comes to data security. In the event of a merchant data breach, Congress should allow financial institutions to name the source of the merchant data breach and require the merchant responsible for the breach to be financially liable for the cost of the breach of the affected consumers and financial institutions.

Data Security Requirements for Credit Unions

The National Credit Union Administration (NCUA), implements data security standards for credit unions, as does the Federal Financial Institutions Examination Council (FFIEC), of which NCUA is a member.[4]

[3] In 2004, the card brands agreed to a common worldwide standard for the protection of cardholder data, as defined by the Payment Card Industry Security Stands Council. Payment Card Industry Data Security Standards (PCI DSS) applies to all organization that hold, process, or exchange cardholder information from any card branded with the logo of one of the card brands.

[4] The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions. Its membership includes leadership from the Federal Reserve Board, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee. The Office of Thrift Supervision, a past member, was eliminated in July 2011, and many of its functions transferred to the Office of the Comptroller of the Currency.

Credit unions are subject to data security requirements as required by §501(b) of the GLBA and Part 748 of the NCUA's regulations. Specifically, under §501(b) of the GLBA, Congress required NCUA and other federal financial regulators to establish standards to ensure financial institutions protect the security and confidentiality of the nonpublic personal information of their members or customers.

Part 748 of NCUA's regulations requires credit unions to establish a comprehensive data security program addressing the safeguards for customer records and information. These safeguards are intended 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 any unauthorized access to or use of such records or information that would result in substantial harm or inconvenience to any customer. In addition, Part 748 also requires credit unions to develop and implement "risk-based" response programs to address instances of unauthorized access to member information.

Data security requirements under the GLBA and NCUA's regulations are subject to the supervision and enforcement of NCUA for federal credit unions or the state supervisory agencies for federally-insured state-chartered credit unions. Additionally, the Federal Trade Commission has enforcement authority for compliance with these requirements for state-chartered credit unions.

Federal banking agencies have developed and published additional information security requirements which cover specific threats and mitigation of identified risks. The FFIEC has issued specialized IT handbooks that outline cyber security requirements for all depository institutions within the banking and finance sector. The FFIEC IT Handbooks are actually comprised of 11 separate booklets, and are very similar to the current cyber security guidance that pertains to federal agencies. The IT Handbook addresses various topics, including (1) audit, (2) business continuity planning, (3) development and acquisition, (4) electronic banking, (5) information security, (6) management, (7) operations, (8) outsourcing technology services, (9) retail payment systems, (10) supervision of technology service providers, and (11) wholesale payment systems. Credit unions are required to adhere to this FFIEC guidance and these requirements are incorporated into NCUA's examination practices for credit unions, as further detailed below.

The methodologies that federal banking regulators including the FFIEC and NCUA use to provide oversight and supervision vary, but include periodic examinations, self-reporting, and other administrative and legal supervisory actions to enforce compliance.

NCUA has also issued regulations that outline data security and anti-identity-theft requirements, along with publishing agency Letters to Credit Unions, Regulatory Alerts, Legal Opinion Letters and final regulation Part 748 addressing credit union security programs. NCUA's examiners use Automated Integrated Regulatory Examination Software (AIRES) consisting of multiple information technology examination questionnaires to assist with reviewing a credit union's information systems and technology. These AIRES examination questionnaires incorporate all

of the supervisory requirements contained within the FFIEC's IT Handbooks previously discussed. Each of these additional regulatory measures and guidance documents have been developed over the last several years in response to data security and other cyber security and consumer protection laws, some of which include the GLBA and the Fair Credit Reporting Act.

Additionally, Part 716 of NCUA Rules and Regulations governs credit unions' use of customer and member non-public personal information, in accordance with Title V, Subtitle A of GLBA, which contains various requirements including prohibitions on sharing of account numbers, a requirement that all credit unions provide privacy notices to members and customers, and when applicable, credit unions must also provide a conspicuous notice that explains the right of the person whose non-public personal information is going to be shared with certain nonaffiliated parties to "opt out," and credit unions must provide a reasonable means by which and a reasonable time in which the person may exercise the opt-out right. Other provisions of Part 716 include a prohibition on sharing account numbers with third parties for marketing purposes, and limitations on the re-disclosure and reuse of information shared with nonaffiliated third parties.

Conclusion

Data security is a critical issue, and it is clear that there are areas where Congress needs to consider legislation. To protect consumers, Congress should require merchants to meet the same high standards for data protection to which financial institutions are subject. In addition, Congress should permit financial institutions to disclose the source of data breaches affecting their members or customers, and merchants should be required to reimburse consumers and financial institutions for the costs associated with data breaches.
On behalf of America's credit unions and their 96 million members, thank you again for holding this hearing. We appreciate your leadership on this issue.

Best regards,

Bill Cheney
President & CEO