FEDERAL LEGISLATIVE BRIEF

Data Security Reform

Background

Retailers accepting electronic payments do not face the same strict data security standards that financial institutions are subject to under the Gramm Leach Bliley Act (GLBA). The personal financial information of millions of American consumers has been compromised in merchant data breaches within the last five years alone. The retail industry's self-policing standards are clearly inadequate. Major merchant data breaches expose credit unions to significant monetary costs and reputational risk. In the wake of a data breach, credit unions cover not only the cost of fraud, but also the cost associated with blocking transactions, reissuing cards, increasing staff and monitoring of consumer accounts.

Financial institutions are subject to GLBA, and therefore required to develop a robust information security program; perform risk assessments in the areas of employee training, information technology and detection and response to attacks; design and implement safeguards to protect against identified risks; monitor vendors to ensure they properly protect customer information; and test to identify emerging risks.

Retailers are not subject to these high standards. In contrast, with the passage of the Dodd-Frank Act, new debit interchange restrictions shifted $20 billion from financial institutions, used to combat breaches and offset their costs, into the pockets of retailers. The shift was not accompanied by any increased security or consumer protection standards, giving merchants a pass on fraud responsibility while realizing the benefit from interchange income.

Impact on Credit Unions

Security breaches are a rapidly expanding threat, occurring in record numbers across the country and affecting local businesses and national retail giants alike. Credit unions are increasingly responsible for protecting consumer financial safety, but not without significant costs. On average, credit unions pay $6.38 to replace each credit or debit card affected by a breach. The cost-per-card amount includes increased staffing costs and card reissuance. In addition, credit unions assume responsibility for any fraudulent charges associated with a data breach. Credit unions incurred losses in excess of $30 million from the Target data breach alone. MCUL surveyed our member credit unions soon after the Target breach to assess the impact to their individual institutions. Several respondents reported losses in excess of $100,000.

Credit unions are not-for-profit, member-owned financial cooperatives, meaning profits are distributed back to the membership through lower rates and fees, free product offerings, and dividends. The costs associated with a merchant data breach have a direct impact on member-owners, often in the form of unfortunate fee or interest rate increases and diminished product or program offerings.

Impact to Credit Union Members

Theft of personal financial information has significant consequences for credit union members. Common issues include the loss of access to accounts via debit/credit card, delays in card reissuance of up to 7–10 business days, replacing PIN numbers and rejection of recurring auto-pay transactions until card information is updated or replaced. Enhanced fraud protections may also lead to card transactions being delayed or declined. While some of these are short-term issues for the member, the negative effects on fees, products and services also eventually impact them. Depending on the data that is compromised, some breaches can lead to larger, systemic credit problems for victims.

Legislative Status

In late 2017, the House Energy and Commerce Committee requested input from stakeholders regarding potential data breach legislation. CUNA joined a joint trades letter to provide input and express industry concerns. These comments highlighted critical issues the financial industry believes any potential legislation should be address. MCUL and CUNA will seek to introduce meaningful legislation in the next Congress and will continue to work with policymakers at all stages of the legislative process until a common-sense data breach bill is passed into law.

MCUL Position

MCUL supports efforts to help Michigan credit unions combat data breaches and the harm they cause to Michigan's 5.3 million credit union members. By placing more responsibility on the retail industry and making them partners in security and data protection with financial institutions and consumers, the number of breaches will decline. Specifically, MCUL supports potential legislation that reflects the following priorities:

- A flexible, scalable standard for security and data protection that is equivalent to GLBA requirements.
- GLBA-equivalent requirements for timely notice to impacted consumers, law enforcement and applicable regulators, when there is a risk that a breach of unencrypted personal information exposes consumers to identity theft or other financial harm.
- Consistent and exclusive enforcement of data security and notification national standards by the Federal Trade Commission (FTC) and state Attorneys General, and clear preemption of the existing patchwork of state laws for all entities that follow this national data security and notification standard.