MCUL & Affiliates Government Affairs

Data Breach Liability

2015

Federal Issue Brief

Background

Over the past few years, several major national retailers reported massive data breaches. In 2013, Target was compromised during the peak of the holiday shopping season, exposing the card or personal identifying information of nearly 70 million consumers. By early 2014, stolen information from this breach began turning up in the illegal marketplace, costing credit unions over $30 million. Since the Target breach other major breaches have occurred at national retailers including Home Depot, Neiman Marcus and Michaels.

The retail industry's self-policing is clearly inadequate. Financial institutions are required to assume the costs related to card replacement, fraud control and member communication.

While credit unions have been subject to strict federal privacy requirements since 1999, retailers have no similar obligations requiring investment to protect their customer transaction data.

Data Breaches Cost Credit Unions

It costs Michigan credit union's an average of $6.38 just to replace a debit or credit card after a breach. This includes member service costs, increased call center volume, and actual card replacement – it does not include the cost of actual fraud.

MCUL Position

MCUL supports data security legislation that includes the following principles:

- Strong national data protection and consumer notification standards with effective enforcement provisions must be part of any comprehensive data security regime. These standards must apply to any party with access to important consumer financial information – including retailers.
- Inconsistent state laws and regulations should be preempted in favor of strong federal data protection and notification standards.
- Credit unions and banks are already subject to robust data protection and notification standards. These Gramm-Leach-Bliley Act requirements must be extended to other businesses in possession of consumer financial information.
- In the event of a breach, the public should be informed where the breach occurred as soon as it is discovered to allow consumers to protect themselves from fraud.
- Credit unions and banks bear a disproportionate burden in covering the costs of breaches occurring beyond their scope of control. All parties, including retailers, should share responsibility for costs associated with a data breach.

Legislative Status

S. 1927, the Data Security Act of 2014, was introduced in the 113th Congress by Senator Carper (D-DE). No members from the Michigan delegation co-sponsored this bill. On January 27, 2015 the House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade held a hearing to review the elements of sound data breach legislation.