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 obligation, to invest in systems designed to protect their customer transaction data.

Data Breaches Cost Credit Unions

Michigan credit unions are confronted with many costs when a data breach occurs. Credit unions pay an average of $6.38 just to replace each 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

The MCUL supports HR 2205 and S 961, and urges Congress to pass legislation which includes the following principles:

- Strong national data protection and consumer notification standards and effective enforcement provisions must be part of any comprehensive data security regime. The standards should apply to any party with access to important consumer information.
- Recognition of the robust data protection and notification standards which credit unions are already subject to under section V of the Gramm-Leach-Bliley Act (GLBA).
- Preemption of inconsistent state laws and regulations in favor of strong federal data protection and notification standards.
- The ability for credit unions to inform members about information regarding a breach, including where the breach occurred.
- Shared responsibility for all those involved in the payments system for protecting consumer data. The costs of a data breach should ultimately be borne by the entity that incurs the breach.

Legislative Status

HR 2205 was introduced and referred to the House Energy and Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade on 05/08/2015.

S 961 was introduced and referred to the Senate Committee on Commerce, Science, and Transportation on 04/15/2015.

These bills have not been scheduled for a vote but CUNA and the MCUL continue to advocate for additional hearings in the coming months.