State Issue Brief

Data Breach Liability & Notification

Background

Over the past few years, large and small retailers have 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 and costing credit unions over $30 million.

In 2016, Wendy's had a massive data breach impacting hundreds of thousands of Michigan credit union members and in 2017 Arby's had a similar breach. Additional breaches have also occurred at national retailers, including Home Depot, Neiman Marcus and Michaels.

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. With federal inaction on this important issue, number of states have passed laws designed to ensure that retailers provide timely notification when a breach occurs, and incentives to invest in controls designed to prevent breaches in the first place.

Cost of data breaches

Data breaches have both direct and indirect costs. Direct costs include an estimate $6.38 to replace each credit or debit card. This amount includes member service costs, increased call center volume and actual card replacement. In addition to card replacement, credit unions also must pay for an fraudulent activity that occurs prior to card replacement.

Indirect costs include serious reputation risks associated with each data breach. Because financial institutions are prohibited from disclosing the source of a breach, and retailer breach announcements are frequently vague and infer that financial institutions are responsible, consumers understandably often assume their credit union caused the breach, undermining confidence in the institution.

Wendy's data breach hits Michigan hard

The Wendy's breach impacted more than 100 of their locations across Michigan. Wendy's customers who used a card at affected locations between December 2015 and June of 2016 had their plastic compromised. Hundreds of thousands of Michigan credit union members have been impacted and Michigan credit unions continue to bear the costs of this breach. Wendy's corporate, franchise owners, along with Visa and Master Card, failed to notify card-issuing institutions until months after the breach, causing millions of dollars in preventable fraud losses. For example, one Michigan credit union had to pay out nearly $780,000 in provisional credit, a direct expense to the credit union's bottom line and reprint over 18,000 cards.

EMV card (pin and chip) technology

Retailers have mistakenly touted "chip and pin" cards as a total solution to the fraud problem. While EMV has reduced in person or "point of service" (POS) fraud by preventing stolen card data to be burned onto counterfeit cards for POS transactions, it does not prevent the compromised data from being used in

State Issue Brief

online “card not present” transactions, which have become a major source of fraud. Hackers get the card data by bypassing EMV protections when they install malware on retailer terminals, giving them a conduit to any payment credentials run through the devices. While it’s not advisable for states to mandate specific technology standards given the rapid pace of technology change, it is appropriate to require that those who participate in the payment system be held to a common set of standards as it relates to protecting consumer data; to fairly allocate breach costs to responsible parties; and require timely notification to avoid unnecessary fraud losses.

Current Legislation

As currently drafted, SB 633 requires the individual, agency or business to provide all financial institutions effected by a breach of their systems notification of said breach within a three day period of acknowledging that a breach has occurred. If the entity that has been breached fails to do so then civil action can be commenced against the entity by the financial institution. This legislation also incorporates language creating a “gold standard”. This “gold standard” provides a safe harbor for entities that are taking certain precautions to ensure the safety and security of their data. If an entity meets the requisite requirements of the “gold standard” and notifies all financial institutions effected within three days of acknowledging a breach has occurred then the entity would be shielded from a civil legal action.

Senate Bill 632 formally establishes who the Governor can appoint to the State of Michigan’s cyber security council. Two of the eleven member council will be representatives from the financial sector.

MCUL Position

In early October 2017, data breach legislation (SB 632-633) was introduced in the State Senate by Senate Banking Committee Chairman Darwin Booher. The MCUL Supports this legislation as an important step in tightening state notification requirements and providing an avenue to bring civil action against those who fail to notify and/or do not meet the “gold standard” data security requirements.

MCUL
MICHIGAN CREDIT UNION LEAGUE & AFFILIATES