State Issue Brief

Data Breach Liability & Notification

Background
The number of retailers who have reported data breaches has skyrocketed in recent years. During the holiday season of 2013, Target had one of the largest compromises, exposing payment cards and personal identifying information of nearly 70 million consumers, costing credit unions more than $30 million. In 2016, Wendy's had a massive data breach impacting hundreds of thousands of Michigan credit union members. In 2017, Arby's had a similar breach impacting hundreds of Michigan financial institutions. Within the last year, additional large-scale breaches have occurred at Equifax, Facebook, Home Depot, Neiman Marcus, Michaels, Saks Fifth Avenue and others.

While credit unions have been subject to strict federal privacy requirements since 1999, retailers have no similar requirements designed to protect customer transactional data. With federal inaction, at least 25 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.

Impact on Consumers
While there is a financial and reputational risk that financial institutions bear as card issuers, there is a bigger impact felt by the millions of consumers who are affected by these breaches. Consumers have the most to lose when their data is breached. The headaches that come from having to get new cards, update autopay information and monitor their information are very real. While the consumers do not have to pay for these unauthorized charges on their account, they do have to deal with not being able to pay a bill or overdrafting their account when these unauthorized charges come in. They can't pay for groceries because their card has been blocked as result of these charges and haven't yet received a new one. Depending on what info is compromised, their problems can get even worse. The consumers — our members — are the ones that truly suffer from data breaches.

Cost of Data Breaches
Data breaches have both direct and indirect costs. Direct costs include an estimated $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 must also pay for any 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 frequent, vague and imply that financial institutions are responsible, consumers often assume their credit union caused the breach, undermining confidence in the institution.

Wendy's Data Breach Hit Michigan Hard
The Wendy's breach impacted more than 100 of their locations across Michigan. Hundreds of thousands of Michigan credit union members were impacted and Michigan credit unions continue to bear the costs of this breach. Wendy's corporate and franchise owners, along with Visa and Mastercard, 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 was tasked with reprinting more than 18,000 cards.

EMV Card (Pin and Chip) Technology
Retailers have mistakenly touted "chip and pin" cards as a solution to electronic card fraud. EMV cards do help reduce in-person or "point of service" (POS) fraud by keeping stolen card data from being burned onto counterfeit

cards for POS transactions. They do not, however, prevent the compromised data from being used in 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.

Current Legislation

There are currently two separate data breach legislation packages pending in the state legislature. The first is SB 632 and 633, sponsored by Senator Darwin Booher (R-Evart). As currently drafted, SB 633 requires the individual, agency or business to provide financial institutions affected by a breach with notification within a three-day period. If the breached entity fails to do so, then a civil action can be commenced against the entity by the financial institution. This legislation also creates a "gold standard" by providing a safe harbor for entities that take certain precautions to ensure the safety and security of their data. If an entity meets the requirements of the "gold standard" and notifies their card processor within three days of acknowledging a breach has occurred, then the entity would be shielded from civil action. SB 632 creates the State of Michigan's Cyber Security Council.

The second package, HB 6405 sponsored by Representative Diana Farrington (R-Utica) and HB 6406 sponsored by Representative Joe Graves (R-Argentine Twp.), provides for an entirely new data breach notification act. This legislation would provide for various levels of notification based on the size of the breach. The bills require notification within 45 days of the breach to residents of the state that may have been affected. If more than 750 residents may have been affected, then the Department of Technology, Management and the Budget (DTMB) must also be notified within that 45-day period. If more than 1,000 residents have been notified because they may be affected by the breach, then the DTMB and all credit reporting agencies must be notified within the 45-day period. This legislation also creates new data security guidelines for retailers operating in the State of Michigan to provide consumers with added security when using their electronic payment cards at retailers of all sizes in the state.

Status

SB 632-633 have had multiple hearings in the Senate Banking and Finance Committee. This legislation was met with harsh opposition from the retail community, and MCUL and other stakeholders continue to try to address the concerns of these groups to allow the legislation to move forward.

HB 6405-6406 were recently voted out of the House and have been referred to the Senate Finance Committee.

Key Message Points: Senate Bills

- Requires breached retailers to notify card processors within three days of discovering that a breach has occurred.
- Creates a civil cause of action if the notification is not provided within the requisite statutory time period.
- Provides the framework for a Cyber Security Council comprised of members of the retail, financial and business sectors to create comprehensive data security standards for Michigan businesses.

Key Message Points: House Bills

- Requires retailers who are breached to notify the residents of the state within 45 days of confirmation. If the breach affected 750 residents, then the retailer must also notify the DTMB in writing. If the breach affected 1,000 residents, then the retailer must, in addition to the DTMB, also notify all credit reporting agencies.
- Creates guideline measures for retailers for securing their customers' data.
- Encourage your lawmaker to support these reasonable data security reforms, to better protect Michigan consumers' personal and financial information.