



## BACKGROUND

Over the past few years, several 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 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. Additional breaches have also 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.

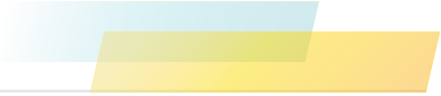
While credit unions have been subject to strict federal privacy requirements since 1999, retailers have no similar obligation to invest in systems designed to protect their customer transaction data.

## COST OF DATA BREACHES

When a data breach occurs Michigan credit unions are confronted with numerous costs. According to CUNA, on average, credit unions pay \$6.38 to replace each credit or debit card. This amount includes member service costs, increased call center volume, and actual card replacement; however it does not include the cost of actual fraud. Credit unions oftentimes also experience a reputational cost when a data breach occurs. Vague wording in the communications sent to consumers by retailers make it seem as though the financial institution is responsible for the breach.

## WENDY'S DATA BREACH HITS MICHIGAN HARD

The Wendy's breach impacted more than 100 of their locations across Michigan. The breach affected customers who dined at Wendy's between December 2015 and June of 2016, and included locations outside of Michigan as well. 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, Visa, and Master Card failed to notify card issuing institutions until very late in the game. One 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.



Until retailers are required to invest in robust data security measures, credit unions will continue to pay the price for retailer data breaches.

## EMV CARD (PIN AND CHIP) TECHNOLOGY

---

Retailers have hailed Europay MasterCard Visa (EMV or chip and pin) cards as a fix to make the system safer, but it is not a panacea. EMV technology represents an improvement in payment technology but it only covers one aspect of the payment process. States should not prescribe a static technology standard that will become easily outdated. Instead states must ensure all of those who participate in the payments system are held to the same standards to protect consumer data, share the costs associated with breaches, and notify those impacted in a timely fashion.

## MCUL POSITION

---

MCUL supports legislation that creates a strong, robust, and comprehensive data security system for all parties that handle personally identifying information. Inaction at the federal level has prompted MCUL to seek a solution at the state level. MCUL has been working with credit union experts and officials throughout the first quarter of 2017 to draft legislation that includes the following principles:

- Reimbursement for all costs that credit unions experience as a result of a breach. The costs of a data breach should ultimately be borne by the entity that incurs the breach such as the costs of:
  - Cancelling and reissuing debit and credit cards
  - Closing accounts and stopping payments
  - Refunding cardholders to cover the costs of unauthorized transactions
  - Notifying members
- Strong notification standards that would require the individual, agency, or business to disclose a breach in the security of the system that includes personal information to a resident of Michigan and the relevant financial institution in the most expedient time possible and without unreasonable delay. The notification would include:
  - A requirement to disclose that the individual's, agency's, or business's systems were breached
  - A list of the types of personal information that were or are reasonably believed to have been subject to the breach
  - Date the breach occurred, the date range within which the breach occurred, or the estimated date of the breach
  - Whether the notification was delayed as a result of a law enforcement investigation if that is possible to determine at the time the notice is provided
  - The toll free telephone numbers and addresses of major credit reporting agencies
  - An offer to provide identity theft prevention and mitigation services for a maximum of 12 months
  - Information about what the individual, agency, or business has done to protect individuals whose information has been breached
  - Advice on steps that the person whose information has been breached may take to protect himself or herself