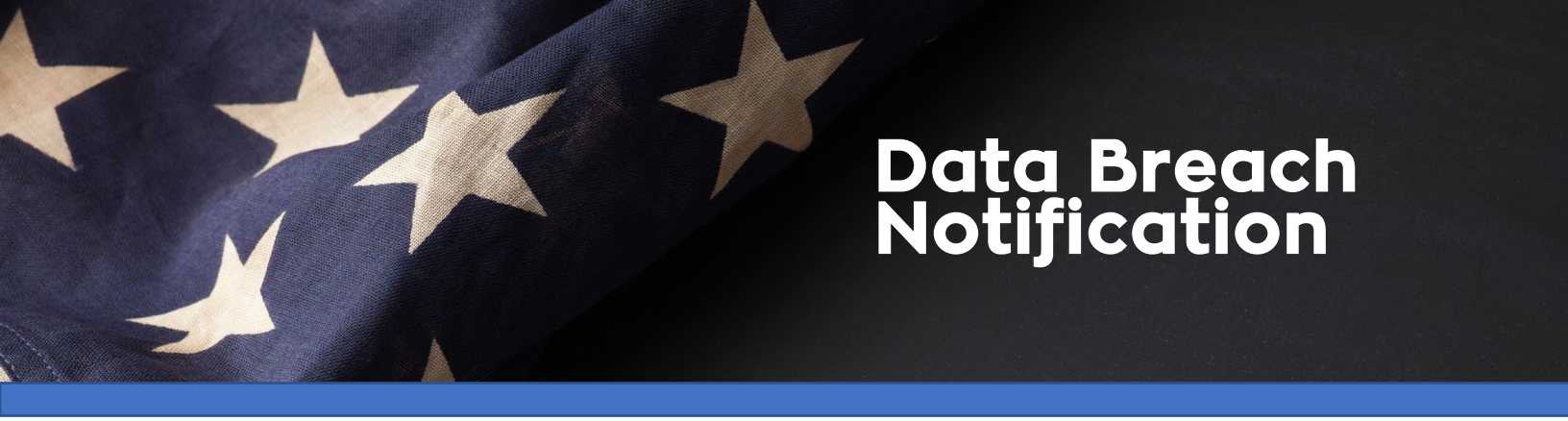

Data Breach Notification

Background

The number of retailers who have reported data breaches has skyrocketed in recent years. During the 2013 holiday season, Target experienced one of the largest compromises, exposing the payment card and personal identifying information of nearly 70 million consumers and 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, and a massive breach at Equifax affected nearly 150 million consumers. A late year announcement last year from Marriott reported more than 500 million consumers' information had been breached over several years prior to discovery of the security event. Additional large-scale breaches have occurred at Facebook, Home Depot, Neiman Marcus, Michaels, Saks Fifth Avenue and others.

While credit unions have been subject to strict federal privacy requirements for more than 20 years, retailers have no similar requirements to protect customer transactional data. With federal inaction, the nation relies on state-specific legislation to ensure that retailers provide timely notification when a breach occurs and incentives to invest in preventative controls.

Impact on Credit Union Members and Consumers

The biggest impact of data breach events falls on the millions of consumers whose data is compromised. The headaches associated with replacing cards, updating autopay accounts and monitoring their personal information are very real. While 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 over-drafting their account when these unauthorized charges come in. They may be unable to pay for groceries or medicine because their card has been blocked and they have yet to receive a new one. Depending on what information is compromised, their problems can get even worse. The consumers—our members—are the ones that truly suffer as a result of 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. Indirect costs include serious reputational 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, along with hundreds of thousands of Michigan credit union members. Card-issuing institutions were not notified 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 total solution to electronic card fraud. EMV cards do help reduce in-person or "point of sale" (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 online in "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 retailers' terminals, giving them a conduit to any payment credentials run through the devices.

Current Legislation

Legislation introduced last session will has been reintroduced. HB 4186-4187 provides for an entirely new data breach notification act. Its key provisions include various levels of notification based on the size of a breach and 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 Budget (DTMB) must also be notified within the 45-day period. If more than 1,000 residents may have been affected by the breach the notification must go to the residents, DTMB and all credit-reporting agencies must be notified within 45 days. The legislation creates new data security guidelines for retailers operating in Michigan to provide consumers with added security when using their electronic payment cards in this state.

New to the legislation this year is an expected provision to exempt small businesses, defined as having 50 or fewer employees. These small businesses would still be required to comply with the current requirements to notify "without unreasonable delay."

Status

Our team continues to work with the sponsor and interested parties on this legislation to ensure that it provides comprehensive data security standards to protect Michigan consumers. The legislation has had an initial hearing in the House Financial Services committee and is expected to be voted on in short order. The legislation then will be heard by the House Ways and Means committee before being sent to the floor.

Key Message Points

MCUL supports requiring breached retailers to notify the residents of this state by a certain date.

MCUL is reviewing the "small business" exception included in the newest version of the bill to determine its overall impact on consumer protection.

MCUL also supports creating guidelines for retailers regarding securing customer data, and for investigating breaches appropriately when they are discovered.

Please encourage your lawmaker to support these reasonable data security reforms that will better protect Michigan consumers' personal and financial information.