mba

Michigan Bankers Association

507 S. Grand Ave.
Lansing, MI 48933
www.mibankers.com

517-485-3600
Fax 517-485-3672

November 28, 2018

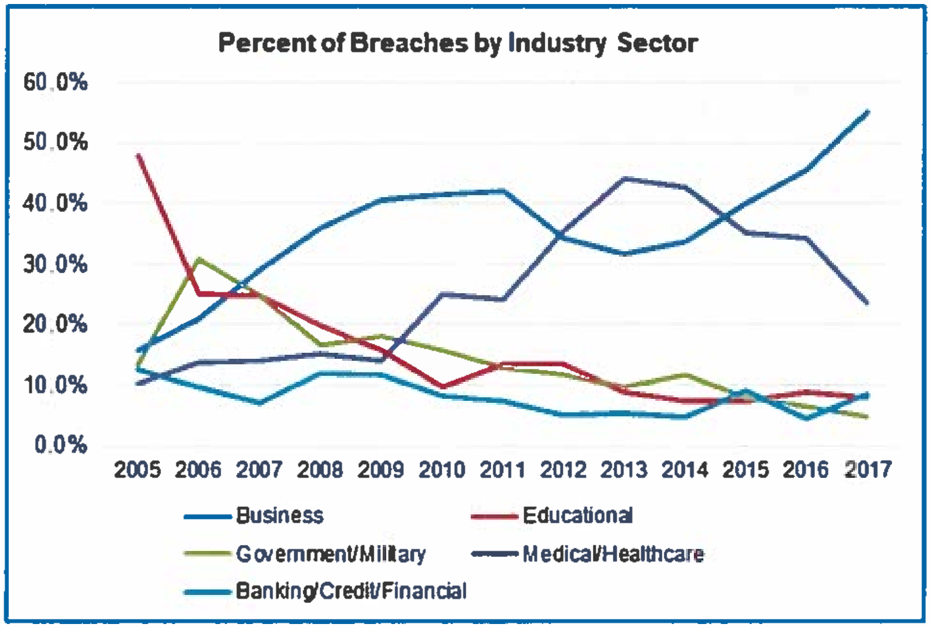
The Honorable Diana Farrington
Chairwoman
Michigan House Financial Services Committee
794 Anderson House Office Building
Lansing, MI 48909

Dear Chair Farrington & Members of the House Financial Services Committee:

Thank you for the opportunity to testify in support of House Bills 4186 and 4187.

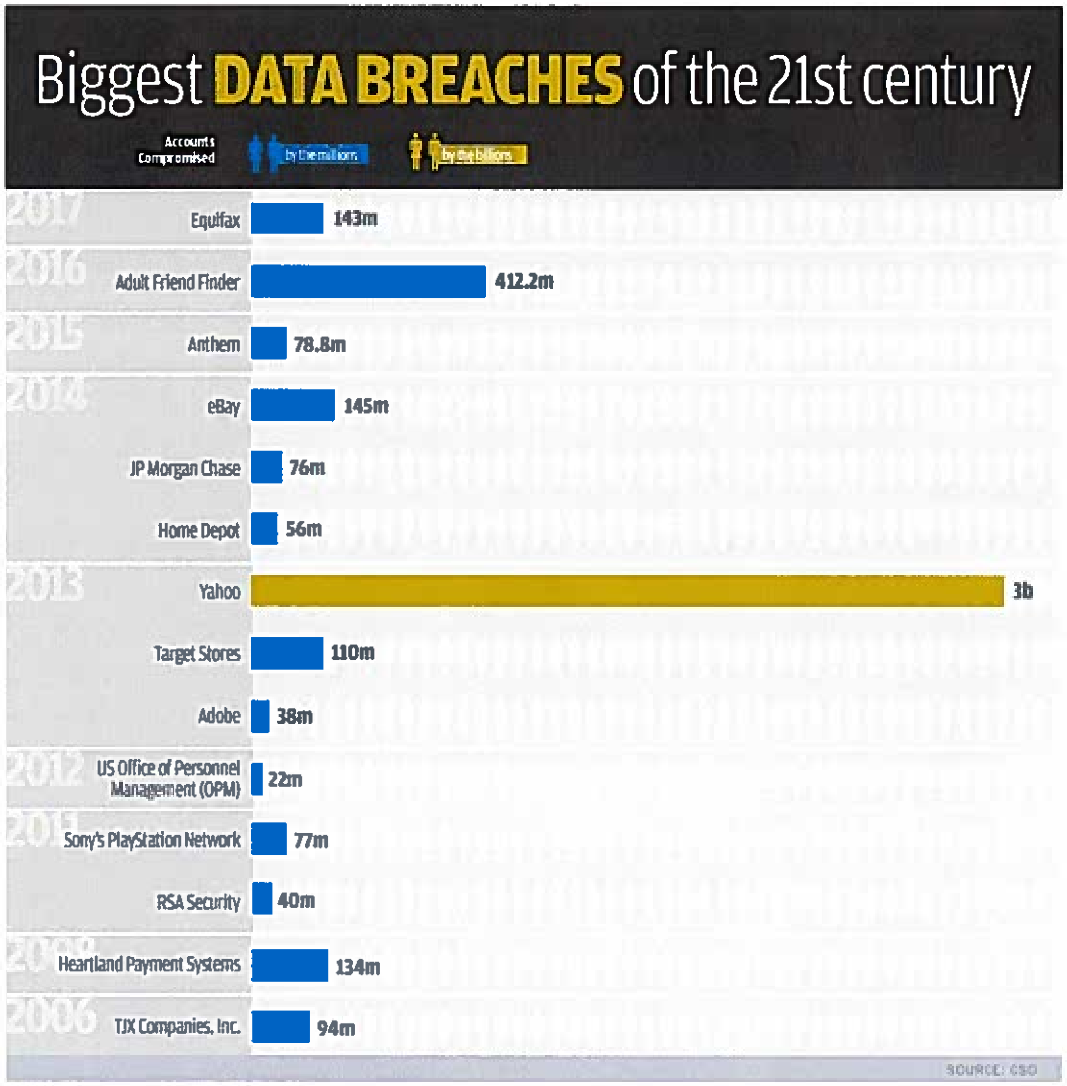
Banks are national leaders in preserving the security of customer data. Our industry dedicates hundreds of millions of dollars annually to data security and adheres to strict regulatory and network requirements. Nevertheless, data breaches in the electronic payments system occur, much of it on the merchant end of the payment system.

The Identity Resource Center reported 1,579 breaches in 2017 – a new record high. The two sectors that reported the highest number of breaches were business (55 percent of breaches – or 870) and the healthcare industry (23.7 percent or 374 breaches). 2017 was only the second time since 2005 that the financial services industry ranked in the top three industry categories (with 8.5 percent or 134 breaches). These numbers and the graph below indicate where criminals are focusing their efforts.



The Federal Trade Commission Consumer Sentinel Network reported that there were 15,028 ID theft complaints. The most common source of these complaints came from government documents and benefits (27 percent) with the second most coming from employment or tax related transactions (26 percent).

Consider the following infographic, which highlights the biggest data breaches of the 21st century:



SOURCE: CSO

[ii]

The infamous Target breach in 2013 impacted 110 million people. It began before Thanksgiving of that year but was not discovered until weeks later. The company had been collecting personally identifiable information (PII) of its customers. This includes full names, addresses, email addresses and telephone numbers. In some cases, they also collected credit card numbers.

One of the earliest and most damaging data breach events involved Heartland Payment Systems in 2008. That event exposed 134 million credit cards. At the time of the breach, Heartland was processing 100 million payment card transactions per month for 175,000 merchants – most small to mid-sized retailers. It wasn't discovered until January 2009, when Visa and MasterCard notified Heartland of suspicious transactions from accounts it had processed. In this case, Heartland ended up paying an estimated $145 million in compensation for fraudulent payments.

As exemplified by the Heartland event, too often our members become aware that a retailer has been breached weeks or months after the event was discovered. During the time between the breach and when we are told of the event, criminals have a distinct advantage as financial institutions are unaware of the heightened risk.

Regardless of where the breach occurred, Michigan banks take a variety of steps to protect the integrity of our customers' accounts. For example, we monitor accounts for indications of suspicious activity and block and reissue cards for affected accountholders. In the event of a confirmed fraudulent transaction, we will make our customers whole as quickly as possible.

The cost of these retail data breaches is significant. Replacement cards can cost up to $10 each to replace. This expense, any fraud losses, time spent mitigating and the lost revenue as customers are without a working debit or credit card is a burden on the financial institution. What is more difficult to determine is the loss of a customer's trust when their card is compromised.

We all have a shared responsibility to protect the integrity of the payments system and by working together we can prevent or at least limit the damage caused by data breaches. Our members will continue to work with the card networks, law enforcement agencies and industry associations to better understand the impact of breaches and determine the best strategies to protect our customers.

However, we must be notified as quickly as possible. Under existing federal law, until we have been notified that a breach has occurred, we cannot share with our customers the reason why they are receiving new cards or are experiencing other anti-fraud procedures. Yes, we can send them a new card. Yes, we can close existing accounts and open new accounts, but until we have been notified, we cannot fully explain why we are taking these actions. Our hands are tied.

When merchants notify financial institutions in a timely manner, we are more quickly able to react to potentially fraudulent activity as a result of a data breach. Our experience has shown, however, that merchants are reluctant to share this information.

To ensure that this policy, when enacted, will benefit all entities involved, there is an amendment that our members ask to be included in the bill. Financial institutions are subject to the federal Gramm-Leach-Bliley Act. This act places stringent requirements on financial institutions in regard to the protection of customer sensitive data, including the requirement of the implementation of the "*safeguards rule.*" In order to make sure there is no conflict between state and federal we ask that standard language exempt institutions subject to Gramm-Leach-Bliley be added to the bill. Specifically, we ask for the following amendment to HB 4187 (as introduced):

Amend page 14, line 11 after "government" by inserting a comma and "including, but not limited to, title V of the Gramm-Leach-Bliley act, Public Law 106-102, 15 USA 6801 to 6827 or the health insurance portability and accountability act of 1996, Public Law 104-191,"

The bills before you continue the conversation on the best ways to inform the public, law enforcement and financial institutions. We look forward to good faith discussions with Michigan retailers and with other concerned parties about their concerns and how we can find a balance that will increase our common customers trust in all our institutions.

Sincerely Yours,

David Q. Worthams
Policy Director

[i] Identity Theft Resource Center, "2017 Annual Data Breach Year-End Review", Accessed November 26, 2018, https://www.idtheftcenter.org/2017-data-breaches/

[ii] CSO From IDG, "The 17 Biggest Data Breaches of the 21st Century, Accessed November 26, 2018, https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html