MEMORANDUM

To: Members of the House Financial Services Committee

From: Dan Papineau – Michigan Chamber of Commerce, Delaney McKinley – Michigan Manufacturers Association, Amy Drumm – Michigan Retailers Association, Brian O'Connell – General Motors, Alexa Kramer – Grand Rapids Area Chamber of Commerce, Amanda Fisher – NFIB, Auday Arabo – Midwest Independent Retailers Association, Jason Puscas – Detroit Chamber, Kurt Berryman – Auto Dealers of Michigan, Connor Spaulding – Michigan Restaurant and Lodging Association

Date: February 20, 2019

Subject: HB 4187 – Critical and Reasonable Amendments to Data Breach Notification Legislation

---

The purpose of this memo is to share our collective opposition to HB 4187, legislation that will mandate notification requirements in the event of a data breach. While the introduced version presents untenable mandates, with a few minor yet critical changes, our respective organizations could support HB 4187.

Cybersecurity is a growing issue for both businesses and individuals throughout the world. Over the last few years we have seen unprecedented breaches of both public and private computer systems releasing millions of records containing sensitive personal information. There is no denying that this developing issue deserves attention and HB 4187 is a great place to begin the conversation.

We compliment the sponsor for introducing a practical and comprehensive cybersecurity bill. The business community represented on this letter appreciates the bill sponsor's efforts in putting forth a real solution to a serious problem.

With the following changes, which reflect the compromise agreed to by all interested parties last year, we would be supportive of HB 4187:

1. For merchants utilizing a credit card gateway, allow for an additional 30-day notification period upon proving the additional time is needed for good cause.
2. For businesses not utilizing a credit card gateway, allow for a notification period of 75 days.
3. If a third-party agent incurs a data breach, the covered entity could require them to be responsible for the notification mandates under the act.
4. As a matter of statewide concern, disallow local cybersecurity ordinances.
5. Make requirements less prescriptive to allow for greater flexibility in investigations to match the severity and risk of each incident.
6. Add a requirement that state or federal law enforcement agencies send a written or electronic notice when asking for a delay in providing the notice required under the act.
7. Also allow substitute notification (online and via the media) if the breach impacts more than 500,000 state residents.

With the above-mentioned changes, the legislation would reflect a compromise reached last session with the Michigan Bankers Association and the Michigan Credit Union League. After tireless negotiations with interested parties we hope you can support the business community's compromise. With the suggested changes, the proposal would benefit Michigan residents while ensuring Michigan business can comply with these new mandates.