Insights, News & Events

EYES ON MICHIGAN: WHAT BUSINESSES NEED TO KNOW ABOUT PENDING CONSUMER PRIVACY AND IDENTITY THEFT LEGISLATION

Insights
Sep 9, 2025

Michigan lawmakers are considering sweeping updates to the state's identity theft protection law while also debating whether Michigan will become one of nearly half the states that have passed a consumer privacy law. Fisher Phillips is closely monitoring both SB 359 and SB 360 to prepare businesses for changes that may be on the horizon on both fronts. This Insight explores the current state of Michigan law, the proposed changes being debated, and some steps your business can take to prepare for new potential obligations.

Overview of Senate Bill 359: The Personal Data Privacy Act

The Personal Data Privacy Act, introduced in June 2025, would create Michigan's first comprehensive consumer privacy framework. We outline the key provisions below.

Applicability Thresholds

Entities covered would be those that conduct business in Michigan or produce products or services that are targeted to residents of Michigan and, during the calendar year, either control or process personal data from over 100,000 consumers or control or process personal data of 25,000 or more consumers and derive any revenue from the sale of personal data. There are also a number of exemptions.

Consumer Rights

If enacted, the law would grant residents new rights to access, correct, delete, and obtain copies of their data. It

Related People

Kate Dedenbach, CIPP/US
Of Counsel
248.901.0301

Jillian Seifrit, CIPP/US
Associate
610.230.6129

would also create new rights related to opting out of processing for targeted advertising, the sale of personal data, and profiling.

Notice Requirements

If enacted, the law would require entities subject to the law to provide a notice to consumers explaining the categories of data they collect, the third parties with whom they sell or chare the data, the purpose for collecting the data, and a description of their rights and how to exercise them.

Data Protection Impact Assessment

Controllers would need to conduct and document a data protection impact assessment (DIPA) for certain processing activities involving personal data including:

- Processing of personal data for targeted advertising
- Sale of personal data
- Processing of personal data for the purposes of profiling if the profiling has certain risks
- Processing of sensitive data
- Any processing activities that involve personal data that present a heightened risk of harm to consumers

The Michigan Attorney General would be able to request a copy of the DIPA, but it would remain confidential and exempt from public requests under FOIA. This is a unique twist that is different than other consumer privacy laws.

Data Broker Registry

The bill proposes that, beginning on February 1, 2026, and every year after that, data brokers register with the attorney general. The list of registered data brokers would be publicly assessable on the Attorney General's website.

If a data broker does not register, there is a proposed fine of $100 per day until registration occurs or an amount equal to the registration fees that were due and not paid.

Geofencing

Michigan proposes to join a minority of states that prohibit geofencing within 1,750 of any mental health facility

Service Focus

Consumer Privacy Team

Data Protection and Cybersecurity

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

Related Offices

Detroit

or reproductive or sexual health facility for the purpose of identifying, tracking, or collecting data from or sending any notification to a consumer regarding the consumer's health data.

Enforcement

There is no private right of action under the proposed bill. Instead, the Attorney General would be solely responsible for enforcement. Before bringing any action, the AG would need to provide notice.

The civil fines are not to exceed $7,500 per violation, unless related to data brokers not registering with the AG. Additionally, if a person does not cooperate with the Attorney General's investigation, the office could issue a maximum fine of $5,000.

Overview of Senate Bill 360: Identity Theft Act

Before examining the potential changes on tap, here's an overview of the current Michigan Identify Theft Act.

- Businesses that own or license data must notify Michigan residents if their unencrypted "personal information" is accessed and acquired by an unauthorized person, or if their encrypted data is accessed and acquired along with the encryption key – unless the business determines that the security breach is not likely to cause substantial loss, injury, or result in identity theft.
- Such notice must be provided "without unreasonably delay."
- There is no requirement to notify the Attorney General. However, if 1,000 or more Michigan residents are affected, the business must notify the Consumer Reporting Agencies (Experian, Equifax, and TransUnion).
- "Personal information" means the first name or first initial and last name linked to one or more of the following data elements: Social Security number, driver license number or state personal identification card number, and demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the individual's financial accounts.

- Businesses that are subject to the GLBA or HIPAA, and comply with the notification requirements under those statutes, are considered to be in compliance with Michigan's law.
- Penalties for failing to notify can reach $250 per violation, capped at $750,000 per breach.

Notice Requirements

SB 360 proposes to add a notification requirement to the Attorney General if 100 or more Michigan residents are affected by a security breach. This notice would need to be provided no later than 45 days after the determination of the breach.

The bill also proposes to add the same notice timeframe of 45 days for notifying individuals.

The threshold for notifying the Consumer Reporting Agencies would remain the same.

Additionally, if the security breach results in a resident's Social Security number or taxpayer identification number being accessed or acquired, or is reasonably believed to have been accessed or acquired, the business would need to offer appropriate identity theft prevention services and, if applicable, identity theft mitigation services that must be provided at no charge to the resident for not less than 24 months.

Personal Information Definition Changes

The proposed law would add additional elements to the definition of "personal information," including:

- passport number
- other unique identification number issued on a governmental document that is used to verify the identity of an individual
- any individually identifiable information contained in the individual's current or historical record of medical history, medical treatment, or diagnosis created by a health care professional
- a health insurance policy number or subscriber identification number and any unique identifier used by a

health insurer to identify an individual

- a username or email address, in combination with a password or security question and answer, that would permit access to an online account that is reasonably likely to contain or is used to obtain personal identifying information
- any genetic information or biometric information that is used to authenticate or ascertain the individual's identity, such as a fingerprint, voice print, retina, or iris image

The proposed addition to the definition of personal information is a growing trend among states. Right now, about half of states require notice to individuals if their health information was impacted by a data breach.

Cybersecurity

The bill adds a new section related to cybersecurity – a new trend that has not yet spread to most other states with data breach laws. Entities that handle personal information would be required to implement and maintain reasonable security procedures to prevent unlawful use or disclosure. These procedures must include appointing a responsible coordinator, identifying internal and external risks, implementing safeguards tailored to those risks, and regularly assessing their effectiveness.

Additionally, service providers would be required to be contractually obligated to follow recognized cybersecurity standards, such as the NIST Cybersecurity Framework 2.0. Security protocols would need to be adaptable to changing circumstances that could affect data protection.

Fines

The bill would add additional potential fines and penalties.

- The failure to notify would remain the same: $250 per person.
- However, the bill adds a $2,000 fine for failure to maintain reasonable security procedures and $2,000 for failing to investigate a breach.
- Finally, the aggregate liability per breach would remain the same and not exceed $750,000.

What's Next?

The bill to amend the existing data breach law (SB 360) seems to have more momentum than the bill to revise the consumer privacy law (SB 359). SB 360 was reported favorably without amendment by both the Committee on Finance, Insurance, and Consumer Protection and the Committee of the Whole, and it's now been referred to the House Committee on Government Operations.

However, the Michigan Chamber of Commerce has come out against both bills. It argues that they would hurt small business, create an additional patchwork of regulations, and lead to confusion for businesses trying to comply.

Both bills must be voted on and passed by the end of the legislative session in December of this year. If either bill is passed, it will be presented to Governor Gretchen Whitmer for her signature in order to become law. The Governor has not expressed a position on either bill.

What Should Businesses Do?

We recommend that businesses continue to monitor the progress of Michigan Senate Bills 359 and 360. The best way to track this legislation is to subscribe to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. Also:

- Consider any necessary changes to your identity theft protection and cyber security practices, particularly focusing on the expanded scope of the definition of personal information and timelines for notification under the proposed bill.
- Conduct regular risk assessments and test your Incident Response Plan.
- Evaluate your current Privacy Policy to determine any changes that may be required if your business needs to comply with Senate Bill 359.

Conclusion

Fisher Phillips will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. You can also visit FP's U.S. Consumer Privacy Hub for additional

resources to help you navigate this area. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber team or our Data Protection and Cybersecurity team.