Senate Fiscal Agency
P.O. Box 30036
Lansing, Michigan 48909-7536

BILL ANALYSIS

Telephone: (517) 373-5383
Fax: (517) 373-1986

Senate Bills 360 through 364 (as introduced 6-5-25)
Sponsor: Senator Rosemary Bayer (S.B. 360)
Senator Ed McBroom (S.B. 361)
Senator John N. Damoose (S.B. 362)
Senator Sue Shink (S.B. 363)
Senator Mary Cavanagh (S.B. 364)
Committee: Finance, Insurance, and Consumer Protection

Date Completed: 6-10-25

INTRODUCTION

The bills would require private and State entities that had access to State residents' personal information to maintain security procedures for the protection of that information. These procedures would include the assignment of a security coordinator and the implementation of appropriate safeguards to protect the information, among other things. In the case of a security breach, the bills would require an entity to notify affected residents and provide specific information concerning consumer protections and actions taken to rectify the breach. If a breach affected more than 100 residents, the entity would have to notify the Attorney General. The bills would prescribe civil fines for failing to comply with the bills' requirements.

FISCAL IMPACT

Senate Bill 360 could have a positive fiscal impact on the State and local units of government. The bill would impose civil fines ranging from a low of $250 up to a maximum fine of $750,000. Revenue collected from civil fines is used to support local libraries. Additionally, $10 of the civil fine would be deposited into the State Justice System Fund. This Fund supports justice-related activities across State government in the Departments of Corrections, Health and Human Services, State Police, and Treasury. The Fund also supports justice-related issues in the Legislative Retirement System and the Judiciary. The amount of revenue to the State or for libraries is indeterminate and dependent on the number of violations and fines imposed.

The bills would enhance notice requirements for private and public entities, including State departments and educational institutions, whenever a data breach was discovered. Depending on the size of the data breach and how many residents were affected, these notice requirements could have a significant, though indeterminate, fiscal impact on State agencies. The bills also would enhance security procedures for State agencies that housed or accessed personal information. These security enhancements could vary based on the amount of personal information used or stored by a particular State agency. State departments and education institutions could have increased but indeterminate costs to meet the requirements. The bills would empower the Attorney General to investigate and prosecute data breach violations and provide for voluntary payments to offset the costs of investigation and attorney fees. While this would offset many costs, it is possible the Attorney General would require additional appropriations and full-time equivalents to pursue data breach violations, depending on the volume of investigations and prosecutions sought.

MCL 445.75 et al. (S.B. 360); 487.2142 (S.B. 361); 750.159g (S.B. 362); 8.9 (S.B. 363); 762.10c (S.B. 364)

Legislative Analyst: Nathan Leaman
Fiscal Analyst: Joe Carrasco, Jr.
Michael Siracuse

CONTENT

Senate Bill 360 would amend the Identity Theft Protection Act to do the following:

-- Expand the Act's definition of personal information, as protected under the Act.
-- Require a person or an agency that owned, possessed, collected, or accessed personal information to implement and maintain reasonable security procedures to protect and safeguard personal information from unlawful use.
-- Prescribe the security procedures required and how to determine their reasonableness.
-- Require a person or an agency that owned or licensed data that was included in a database that determined a security breach or received notice of a security breach to provide a notice to those affected, and if more than 100 residents were affected, require the person or agency to provide a notice to the Attorney General.
-- Prescribe the information that the notices would have to contain.
-- Prescribe actions that the Attorney General could take to remedy violations of the Act, including executing an assurance of discontinuance, serving a written demand to a suspected person or agency, and bringing a civil action against a person or agency that could result in civil fines.

Senate Bill 361 would amend the Deferred Presentment Service Transactions Act to modify an MCL reference to the Identity Theft Protection Act.

Senate Bill 362 would amend the Michigan Penal Code to modify an MCL reference to the Identity Theft Protection Act.

Senate Bill 363 would amend the Revised Statutes of 1846 to modify an MCL reference to the Identity Theft Protection Act.

Senate Bill 364 would amend the Code of Criminal Procedure to modify an MCL reference to the Identity Theft Protection Act.

Senate Bills 361 through 364 are tie-barred to Senate Bill 360, which is described in greater detail below.

Definitions

"Data" currently means computerized personal information. The bill would include in the definition personal information contained in any other medium.

"Personal information" means the first name or first initial and last name linked to one or more of the following data elements of a State resident: 1) a Social Security number; 2) a driver license number or a State personal identification number; 3) a demand deposit or other financial account information. Under the bill, the term also would include the following:

-- A passport number or other unique identification number issued on a government 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 term would not include the following:

-- Any information about an individual that had been lawfully made public by a Federal, State, or local government record or widely distributed media.
-- Any information that was truncated, encrypted, secured, or modified by any other method or technology that removed elements that personally identify an individual or that otherwise rendered the information unusable, including encryption of the data or device containing the information, unless the person or agency knew or reasonably believed that the encryption key or security credential that could render the personal information readable or usable had been accessed or acquired with the information.

"Security breach" would mean the unauthorized acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency. The term would not include unauthorized access to data by an employee or other individual if the access met all the following:

-- The employee or other individual acted in good faith in accessing the data.
-- The access was related to the activities of the agency or the person.
-- The employee or other individual did not misuse any personal information or disclose any personal information to an unauthorized person.

"Third-party agent" would mean either of the following:

-- A person that maintains a database that includes personal information that the person does not own or license.
-- A person that is otherwise permitted to access personal information owned or licensed by another person or agency in connection with providing services under an agreement with the other person or agency.

Requirements for the Protection of Personal Information

Under the bill, a person or an agency that owned, possessed, collected, or accessed personal information would have to implement and maintain reasonable security procedures to protect and safeguard personal information from unlawful use or disclosure by doing all the following:

-- Identify at least one owner, manager, or employee that would coordinate the person's or agency's security procedures.
-- Identify internal and external risks for security breaches.
-- Include appropriate safeguards for personal information that would be designed to address the external risks.
-- Provide for assessments of the effectiveness of the safeguards.
-- Contractually require each service provider of the person or agency to maintain appropriate safeguards for personal information by adhering to the National Institute of Standards and Technology’s Cybersecurity Framework 2.0 or another industry standard cybersecurity framework.
-- Evaluate and adjust security procedures to account for changes in circumstances affecting the security of personal information.

(The Act defines "person" as an individual, partnership, corporation, limited liability company, association, or other legal entity. "Agency" means a department, board, commission, office, agency, authority, or other unit of State government. The term includes State institutions of higher education and does not include courts.)

The reasonableness of the security procedures would have to be determined by considering all the following:

-- The size of the person or agency.
-- The amount of personal information owned, possessed, collected, or accessed by the person or agency.
-- The type of activities for which the personal information was owned, possessed, collected, or accessed by the person or agency.
-- The cost to implement and maintain the security procedures compared to the person's or agency's resources.

A person or agency that reasonably conformed to an industry recognized cybersecurity framework would be considered to be in compliance if the cybersecurity program was the current version of the National Institute of Standards and Technology's Cybersecurity Framework 2.0, or the person or agency was regulated by the State, the Federal government, or both, or otherwise conformed to any of the following laws or regulations:

-- The security requirements of the Health Insurance Portability and Accountability Act.
-- Title V of the Gramm-Leach-Bliley Act.
-- The Federal Information Security Modernization Act of 2014.
-- The Health Information Technology for Economic and Clinical Health Act.

If a person or an agency that owned or licensed personal information determined that a security breach had or was reasonably believed to have occurred, the person or agency would have to conduct a good-faith and prompt investigation that included all the following:

-- Assessment of the nature and scope of the security breach.
-- Identification of the personal information that was involved in the security breach and the identity of the individuals whose personal information was involved in the security breach.
-- Determination of whether the personal information identified had been acquired or was reasonably believed to have been accessed or acquired by an unauthorized person.
-- Identification and implementation of measures to restore the security and confidentiality of any system compromised in the security breach.

Security Breach Notice Requirements

Under the Act, unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents of the State, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach must provide a notice of the security breach to each resident of the State who meets one or more of the following:

-- That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person.
-- That resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key.

The bill would modify this provision as described below.

Under the bill, if, on or after the bill's effective date, a third-party agent discovered a security breach that involved data that was owned or licensed by another person or agency, the third-party agent would have to provide immediately upon determination a notice of the security breach to the person or agency and provide any other information that was necessary for the person or agency to comply with the notice requirements under the bill.

A person or an agency that owned or licensed data that was included in a database that discovered a security breach or received notice of a security breach on or after the bill's effective date would have to provide a notice of the security breach to each resident of the State who met one or more of the following criteria, if the person or agency knew, should know, or should have known that the security breach had or could have resulted in identity theft or fraud affecting the resident:

-- That resident's unencrypted and unredacted personal information was or could have been accessed and acquired by an unauthorized person.
-- That resident's personal information was accessed or could have been accessed or acquired in encrypted form by a person with unauthorized access to the encryption key.

The Act provides that unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents of the State, a person or agency that maintains a database that includes data that the person or agency does not own or license that discovers a breach of the security of the database must provide a notice to the owner or licensor of the information of the security breach. In determining whether a security breach was likely to cause substantial loss or injury to, or result in identity theft for, one or more State residents, a person or agency must act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances. The bill would delete these provisions.

Instead, under the bill, if a person or an agency was required to provide notice under the Act to 100 or more residents of the State, the person or agency would also have to provide written notice of the security breach to the Attorney General before the date of the notice or receipt of notice.

The written notice to the AG would have to include all the following:

-- A synopsis of the events surrounding the security breach.
-- The approximate number of residents of the State that the person or agency was required to notify.
-- A description of the timing, distribution, and content of the notice.
-- The steps taken to investigate the security breach.
-- The steps taken to prevent a similar security breach.
-- A description of any services related to the security breach that the person or agency was offering and a description of the information being provided.
-- A description of how a resident of the State could obtain additional information about the security breach from the person or agency.

In the case of a security breach, the Act requires a notice to an affected State resident to meet all the following:

-- Be clear and conspicuous.
-- Describe the security breach in general terms.
-- Describe the type of personal information subject to the breach.
-- Describe the action the agency or person has taken to protect data from further breach.
-- Include a telephone number for further assistance or information.

The bill also would require the notice to meet the following requirements:

-- If the Social Security number or taxpayer identification number of a resident were accessed or acquired or was reasonable believed to have been accessed or acquired in the security breach, the notice would have to offer appropriate identity theft prevention services and, if applicable, identity theft mitigation services, which would have to be provided at no charge to the resident for not less than 24 months.
-- The notice would have to provide any information necessary for a resident to enroll in the identity theft prevention services and identity theft mitigations services, as applicable.
-- The notice would have to provide information on how a resident could place a credit freeze on the resident's credit file.

Under the Act, a person who knowingly fails to provide any notice of a security breach may be ordered to pay a civil fine of no more than $250 for each failure to provide notice. The Attorney General or a prosecuting attorney may bring an action to recover the civil fine. The aggregate liability of a person for these civil fines for multiple violations that arise from the same security breach may not exceed $750,000. The bill would delete these provisions.

For the purposes of the bill, residency would be determined by the principal mailing address of an individual, as determined by a record of the person or agency.

Assurance of Discontinuance

Under the bill, if the Attorney General had authority to institute a civil action or proceeding under the bill, the Attorney General could accept an assurance of discontinuance of a method, act, or practice that was alleged to be unlawful from the person or agency that was alleged to have engaged, be engaging, or be about to engage in the method, act, or practice.

The assurance of discontinuance would not constitute an admission of guilt and could not be introduced in any other proceeding. The assurance of discontinuance would have to include a stipulation for any of the following:

-- The voluntary payment by the person for the costs of investigation and reasonable attorney fees.
-- An amount to be held in escrow pending the outcome of an action.
-- An amount for restitution to any aggrieved person.

The assurance of discontinuance would have to be in writing and could be filed with the circuit court of Ingham County, and the clerk of the court would have to maintain a record of the filings. Unless rescinded by the parties or voided by a court for good cause, the assurance of discontinuance could be enforced in the circuit court by the parties to the assurance of discontinuance. The assurance of discontinuance could be modified by the parties by a written agreement signed by all parties or by a court for good cause.

Investigations of and Fines for Violations

If the Attorney General had reasonable cause to believe that a person or an agency had information or was in possession, custody, or control of any document or object that was relevant to an investigation of a violation of the Act, the Attorney General could, before bringing any action, serve the person with a written demand to do one of the following:

-- Appear and be examined under oath.
-- Answer interrogatories.
-- Produce the document or object for inspection and copying.

The demand would have to contain all the following:

-- A description of the conduct constituting the violation of the Act being investigated by the Attorney General.
-- A summary of a person's right to petition for a protective order to modify a demand.
-- If the demand required the appearance of the person, the demand would also have to include a reasonable time and place for the appearance, and a notice that the person could file an objection to or reason for not complying with the demand with the Attorney General on or before that time.
-- If the demand required written interrogatories, the demand also would have to include a copy of the written interrogatories and a reasonable time within which the person would have to answer the written interrogatories.

If the demand required the production of a document or object, the demand also would have to include all the following:

-- A description of the document or object with sufficient definiteness to permit the document or object to be fairly identified by the person.
-- A reasonable time and place for production of the document or object.
-- A notice that the person could file an objection to or reason for not complying with the demand with the Attorney General on or before that time.
-- The name of the person that would be the custodian of the document or object.

At any time before the return date or not later than 10 days after receiving the demand, whichever was earlier, a person subject to the demand could petition the circuit court of Ingham County for a protective order to do any of the following:

-- Extend the return date for a reasonable time.
-- Modify the demand.
-- Set aside the demand.

If a person filed a petition, the person would be required to give the Attorney General at least 10 days' notice of any hearing on the petition and the Attorney General would have to receive an opportunity to respond to the petition.

If a person did not secure a protective order and the person did not comply with the demand by the return date, the Attorney General, with notice to the person, could apply to a court for an order compelling the person's compliance with the demand.

If the Court contemplating the order found that there was reasonable cause to believe that the Act was being, had been, or was about to be violated, that the person subject to the demand was the person that was committing, had committed, or was about to commit the violation or was the person that possessed information, document, or object that was relevant to the investigation by the Attorney General, that the person had left the State or was about to leave the State, and that the order was necessary for the enforcement of the Act, the Court could do either or both of the following:

-- Require the person to comply with the demand.
-- Forbid the removal, concealment, withholding, destruction, mutilation, falsification, or alteration of any document or object that was in the possession, custody, or control of the person.

A person subject to a demand or court order, that with the intent to avoid, evade, or prevent compliance with the demand or order, in whole or in part, removed, concealed, withheld,

destroyed, mutilated, falsified, or by any other means altered any document or object in the possession, custody, or control of the person could be ordered to pay a maximum civil fine of $25,000.

Any testimony, answer, document, or object received by the Attorney General in accordance with a demand or order under the Act would be confidential and not subject to disclosure until the time that an enforcement action was brought by the Attorney General.

The Attorney General could disclose any testimony, answer, document, or object if confidentiality were waived by the following:

-- The person subject to the demand.
-- The person being investigated by the Attorney General.

A person or agency to whom a written demand was served would have to comply with the terms of the demand unless otherwise provided by the order of the Circuit Court.

A person that did any of the following could be ordered to pay a maximum civil fine of $25,000:

-- Knowingly and without good cause failing to appear when served with a demand.
-- Knowingly avoiding, evading, or preventing compliance, in whole or in part, with an investigation, including, the removal from any place, concealment, destruction, mutilation, alteration, or falsification of documentary material in the possession, custody, or control of a person subject to the demand.
-- Knowingly concealing relevant information.

The Attorney General could file a petition in the Circuit Court of the county in which the person was established or conducted business or, if the person were not established in the State, in the Circuit Court of Ingham County for an order to enforce compliance with the bill. A violation of a final order entered under the bill would have to be punished as civil contempt.

If the Attorney General had reasonable cause to believe that a person or an agency had violated the bill, the Attorney General could bring a civil action seeking one or more of the following, as applicable, together with reasonable attorney fees and costs of investigation and litigation:

-- Injunctive relief.
-- If the person or an agency knowingly failed to implement and maintain reasonable security procedures, a civil fine of not more than $2,000.
-- If the person or an agency knowingly failed to investigate a security breach, a civil fine of not more than $2,000.
-- If the person or an agency knowingly failed to provide a notice of a security breach, a civil fine of not more than $250 for each failure to provide the notice, except that the aggregate liability under the bill for multiple violations that arose from the same security breach could not exceed $750,000.

On the petition of the Attorney General, the Circuit Court could enjoin a person from doing business in the State if the person persistently and knowingly evaded or prevented compliance with an injunction issued under the Act.

PREVIOUS LEGISLATION

(This section does not provide a comprehensive account of previous legislative efforts on this subject matter.)

Senate Bills 360 through 364 are respectively reintroductions of Senate Bills 888 through 892 of the 2023-2024 Legislative Session. Senate Bills 888 through 892 passed the Senate and were referred to the House Committee on Government Operations but received no further action.

Legislative Analyst: Nathan Leaman

SAS\S2526\s360sa

This analysis was prepared by nonpartisan Senate staff for use by the Senate in its deliberations and does not constitute an official statement of legislative intent.