



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



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

Senate Bill 198 (Substitute S-1)
Sponsor: Senator Sam Singh
Committee: Regulatory Affairs

Date Completed: 12-2-25

INTRODUCTION

The bill would enact a new law to protect certain types of vehicle dealer data, such as consumers' personal and financial data and motor vehicle diagnostic data (protected dealer data). The bill would prohibit a manufacturer or a third party from accessing, sharing, or using protected dealer data without prior written consent from the dealer. The bill also would prohibit a manufacturer or third party from barring or otherwise limiting a dealer's ability to protect, share, or use protected dealer data, such as by imposing a fee to access or share protected dealer data. Furthermore, the bill would prohibit a manufacturer from leveraging a program, standard, or policy to gain prior written consent from a dealer. The bill specifies the purposes for which a manufacturer could use *legally required* manufacturer data obtained from a dealer's data system, such as for vehicle recall notices and paying incentives.

The bill also would require a dealer's data vendor to adopt and make available a standardized framework for the exchange and retrieval of protected dealer data by a third party contracted with a manufacturer (an authorized integrator). An authorized integrator could only access this framework to the extent agreed upon with the dealer and the dealer data vendor. The bill also would require data vendors, dealers, manufacturers, and other participants of a data exchange to adhere to applicable data security standards (star standards).

FISCAL IMPACT

Although it is not specifically stated in the bill, it is assumed that the Attorney General and local prosecutors would be responsible for enforcing the regulatory framework outlined in the bill. These costs are indeterminate and are not accounted for in the bill, either by appropriation or with language in the bill that would cover any litigation costs.

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

CONTENT

The bill would enact the "Motor Vehicle Dealer Data Collection Act" to do the following:

- Prohibit a third party and a manufacturer from accessing protected dealer data without prior express written consent, engaging in acts of cyber ransom, and barring or limiting a dealer's access to protected dealer data.**
- Prohibit a manufacturer or a manufacturer's selected third party from requiring a dealer to pay a fee for sharing required manufacturer data.**
- Allow a manufacturer to use required manufacturer data obtained from a dealer data system for specified purposes.**
- Prohibit prior express written consent from being a condition of or factor for consideration or eligibility for any manufacturer program, standard, or policy.**
- Require a dealer data vendor to adopt and make available a standardized framework for the exchange and retrieval of protected dealer data.**
- Allow a dealer data vendor or an authorized integrator to access, use, store, or share protected dealer data or any other data from a dealer data system only to the extent allowed in a written agreement between the dealer data vendor or authorized integrator and the dealer.**
- Establish requirements for such an agreement between a dealer data vendor, authorized integrator, and dealer, such as the transmission of protected dealer data if a party to an agreement were to terminate that agreement.**
- Require a manufacturer, authorized integrator, or other third party to indemnify a dealer for any claim or damages resulting from a violation of the bill for accessing, providing access to, or using protected dealer data, if certain circumstances applied.**

Definitions

Under the bill, "third party" would mean a service provider, vendor, dealer data vendor, authorized integrator, or any other person other than a dealer, a government entity acting under Federal, State, or local law, an entity acting pursuant to a valid court order, or a manufacturer.

"Manufacturer" would mean that term as defined in the Michigan Vehicle Code: a person, firm, corporation or association engaged in the manufacture of new motor vehicles, trailers or trailer coaches or semi-trailers, as a regular business.

"Dealer" would mean that term as defined in Section 11 of the Michigan Vehicle Code: a person who, in a 12-month period, 1) engaged in the business of purchasing, selling, or dealing in vehicles required to be titled under the Code or the salvageable parts of five or more vehicles, or 2) engaged in the business of buying five or more vehicles to sell vehicle parts or process into scrap metal. The term also includes a person engaged in the actual remanufacturing of engines or transmissions.

"Protected dealer data" would mean any of the following types of data:

- Personal, financial, or other data relating to a consumer that a consumer provides to a dealer or that a dealer otherwise obtains and that is stored in the dealer's dealer data system.
- Motor vehicle diagnostic data that is stored in a dealer data system and used to fulfill a dealer's obligation to provide warranty, repair, or service work to consumers.

- Other data regarding a dealer's business operations that is stored in the dealer data system.

The term would not include data that was otherwise publicly available or that a manufacturer or third party obtained through another source.

"Star standards" would mean the current applicable security standards published by the Standards for Technology in Automotive Retail.

"Authorized integrator" would mean a third party that a dealer enters a contractual relationship with to perform a specific function for the dealer that allows the third party to access protected dealer data or to write data to a dealer data system, or both, to carry out the specified function.

"Required manufacturer data" would mean data that is required to be obtained by the manufacturer under Federal or State law, data that is required to complete or verify a transaction between the dealer and the manufacturer, motor vehicle diagnostic data, and data that is reasonably necessary and used in compliance with the Motor Vehicle Franchise Act to do any of the following:

- To satisfy a safety, recall, or other legal notice obligation.
- To process and complete the sale and delivery of a new motor vehicle or a certified used motor vehicle to a consumer.
- To validate and pay consumer or dealer incentives.
- A claim for dealer supplied services relating to warranty parts or repairs.
- To evaluate a dealer's performance, including a dealer's monthly financial statements, sales, service, or consumer satisfaction with the dealer through direct consumer contact or consumer surveys.
- Dealer and market analytics.
- To identify the dealer that sold or leased a specific motor vehicle and the date of the transaction.
- Marketing purposes designed for the benefit of or to direct leads to dealers.
- Motor vehicle diagnostic data.
- To develop, evaluate, or improve the manufacturer's products or services.

The term would not include consumer data on a consumer credit application or a dealer's notes about a consumer that were not related to a transaction.

"Dealer data system" would mean a software, hardware, or firmware system that is owned, leased, or licensed by a dealer and includes a system of web-based applications, computer software, or computer hardware, located at the motor vehicle dealership or a remote location, that stores or provides access to protected dealer data including, dealership management systems and consumer relations management systems.

"Dealer data vendor" would mean a third-party dealer management system provider, third-party consumer relationship management system provider, or other third-party vendor providing similar services that permissibly stores protected dealer data under a contract with the dealer.

"Prior express written consent" would mean consent from a dealer contained in a document that is separate from any other consent, contract, franchise agreement, or other writing that contains 1) the dealer's express consent to the data sharing and identification of the parties with whom the data may be shared and 2) all details required by the dealer relating to the

scope and nature of the data to be shared, including the data fields and the duration for which the sharing is authorized.

Dealer Data Sharing with Manufacturer or Third Party

Under the Act, a manufacturer or a third party could not require a dealer to grant the manufacturer, the third party, or any person acting on behalf of the manufacturer or third party, direct or indirect access to the dealer's dealer data system. A dealer could submit or push data or information to a manufacturer or third party through a widely acceptable electronic file format or protocol that complied with star standards or other generally accepted cybersecurity standards that were at least as comprehensive as star standards.

Third Party Restrictions

The bill would prohibit a third party from doing any of the following:

- Copying, using, or transmitting protected dealer data without prior express written consent.
- Engaging in an act of cyber ransom.¹
- Accessing or permitting access to protected dealer data without prior express written consent (see Prior Express Written Consent).

Additionally, a third party could not take an action by contract, technical means, or any other means to prohibit or limit a dealer's ability to protect, share, or use protected dealer data, including any of the following actions:

- Imposing a fee or other restriction on a dealer or an authorized integrator for accessing or sharing protected dealer data or for writing data to a dealer data system, including a fee on a dealer that submitted or pushed data or information to a third party; a charge would be considered a fee unless a third party disclosed the charge to the dealer and justified the charge by documentation of the costs associated with access and, on written request by the dealer, provided the dealer with documentation that the charges were agreed to in writing by the dealer or provided for in the contract for service or goods.²
- Prohibiting a third party that was compliant with star standards or other generally accepted cybersecurity standards that were at least as comprehensive as star standards and that the dealer had identified as an authorized integrator from integrating into the dealer's dealer data system.
- Placing an unreasonable restriction on integration by an authorized integrator or a third party that the dealer wished to be an authorized integrator.

The bill would provide the following examples of an unreasonable restriction:

- An unreasonable limitation or condition on the scope or nature of the protected dealer data that was shared with an authorized integrator.
- An unreasonable limitation or condition on the ability of the authorized integrator to write data to a dealer data system.

¹ "Cyber ransom" would mean to encrypt, restrict, or prohibit or threaten or attempt to encrypt, restrict, or prohibit a dealer's or an authorized integrator's access to protected dealer data to obtain payment not agreed to by the dealer or the authorized integrator in a written contract for services or goods.

² "Fee" would mean a charge for access to protected dealer data beyond any direct costs incurred by the dealer data vendor in providing protected dealer data access to an authorized integrator or allowing an authorized integrator to write data to a dealer data system.

- An unreasonable limitation or condition on a third party that accessed or shared protected dealer data or that wrote data to a dealer system.
- A requirement of unreasonable access to sensitive, competitive, or other confidential business information of a third party as a condition for access to protected dealer data or sharing protected dealer data with an authorized integrator.

Manufacturer Restrictions and Requirements

The bill would prohibit a manufacturer from doing any of the following:

- Accessing, using, transmitting, or requiring a dealer to share or provide access to protected dealer data beyond the required manufacturer data without prior express written consent.
- Engaging in an act of cyber ransom.
- Taking an action by contract, technical means, or any other means to prohibit or limit a dealer's ability to protect, store, copy, share, or use protected dealer data.

The bill would prohibit a manufacturer or a manufacturer's authorized integrator from requiring a dealer to pay a fee for sharing required manufacturer data if the following applied:

- The manufacturer required the dealer to provide the required manufacturer data through a specific third party that the manufacturer selected.
- The required manufacturer data was in a format that was compatible with the file format required by the manufacturer.
- The third-party vendor satisfied or followed the star standards or other generally accepted cybersecurity standards that were at least as comprehensive as the star standards.

The bill *would* allow a manufacturer to charge a dealer the manufacturer's actual third-party costs for providing access to protected dealer data to a dealer, authorized integrator, or other third party if the manufacturer did the following:

- Disclosed the charge to the dealer in writing.
- On written request by the dealer, provided to the dealer documentation that the charges were agreed to in writing by the dealer or provided for in the contract for services or goods.

The Act would not restrict or limit a manufacturer's right to obtain required manufacturer data, use required manufacturer data for the purposes previously identified, or use or control data that was proprietary to the manufacturer, created by the manufacturer, obtained from a source other than the dealer, or that was public information.

A manufacturer, authorized integrator, or other third party would have to indemnify a dealer for any claims or damages if the claims or damages result from a violation of the bill for accessing, providing access to, using, or disclosing protected dealer data, and any of the following applied:

- The claims or damages directly resulted from a violation of the bill by the third party from whom the dealer was seeking indemnification.
- The claims or damages directly resulted from a violation of the bill by a vendor or contractor as an agent acting on behalf of the third party from whom the dealer was seeking indemnification.
- The claims or damages directly resulted from a violation of the bill by a vendor or other service provider that the third party from whom the dealer was seeking indemnification required the dealer to use.

A dealer bringing cause of action against a manufacturer, authorized integrator, or other third party for a violation of the bill would have the burden of proof.

Prior Express Written Consent

The bill would prohibit prior express written consent from being a condition of or factor for consideration or eligibility for any manufacturer program, standard, or policy, including one that offered a bonus, incentive, rebate, or other payment or benefit to a dealer. If the bonus, incentive, rebate, or other payment program required the delivery of information that was considered protected dealer data to qualify for the program and receive the program benefits, a dealer would have to supply the information to participate in the program.

Prior express written consent could be unilaterally revoked or amended by a dealer without cause with a 60-day notice or immediately for cause.

The bill would not require a manufacturer to pay a benefit to a dealer if the dealer refused to provide data that was reasonably necessary to participate in a bonus, incentive, rebate, or other program.

Dealer Data Vendor Requirements

The bill would require a dealer data vendor to adopt and make available a standardized framework that allowed both the following:

- The exchange, integration, and sharing of protected dealer data from a dealer data system with an authorized integrator.
- The retrieval of protected dealer data by an authorized integrator using star standards or a standard that was compatible with star standards.

The bill also would require a dealer data vendor to provide open application programming interface access to an authorized integrator. If the application program interfaces were not the reasonable commercial or technical standard for secure data integration, the dealer data vendor could provide a similar open access integration method if that method provided the same or better access as an application programming interface and that method used the required standardized framework.

The bill would allow a dealer data vendor or an authorized integrator to access, use, store, or share protected dealer data or any other data from a dealer data system *only* to the extent allowed in a written agreement between the dealer data vendor or authorized integrator and the dealer. An agreement regarding access to, sharing or selling of, copying, using, or transmitting protected dealer data would have to be terminable within 90 days after a dealer data vendor or authorized integrator received notice from the dealer. On notice of the dealer's intent to terminate such an agreement, a dealer data vendor or an authorized integrator would have to ensure a secure transition of all protected dealer data to a successor dealer data vendor or authorized integrator by doing the following:

- Providing access to, or an electronic copy of, all protected dealer data and all other data stored in the dealer data system in a commercially reasonable time and format that a successor dealer data vendor or authorized integrator could access and use.
- Deleting or returning all protected dealer data to the dealer before the termination of the agreement in accordance with any written directions of the dealer.

On request by a dealer, a dealer data vendor or an authorized integrator would have to provide the dealer with a list of any entity the dealer data vendor or authorized integrator was sharing protected dealer data with or any entity to whom the dealer data vendor or authorized integrator had allowed access to protected dealer data.

A dealer data vendor or an authorized integrator would have to allow a dealer to audit the dealer data vendor's or authorized integrator's access to and use of any protected dealer data.

Violations

A person that violated the Act would be subject to a civil fine of up to \$5,000 per violation.

Additionally, the bill would require a manufacturer to compensate a dealer for a third-party claim asserted against or damages incurred by the dealer to the extent caused by access to, use of, or disclosure of protected dealer data in violation of the Act by the manufacturer or a third party acting on behalf of a manufacturer to whom the manufacturer had provided the protected dealer data.

Exemptions

The Act would not govern, restrict, or apply to data that existed outside of a dealer data system, including data that was generated by a motor vehicle or by a device that a consumer connected to a motor vehicle.

The Act also would not authorize a dealer or a third party to use data that was obtained from a person in a manner inconsistent with an agreement with that person or with the purposes for which that person provided the data to the dealer or third party.

The Act would not prevent a dealer, manufacturer, or third party from discharging the obligations of the dealer, manufacturer, or third party as a service provider, an obligation under Federal or State law to protect and secure protected dealer data or to otherwise limit those responsibilities.

Lastly, the Act would not grant a dealer ownership of motor vehicle diagnostic data or rights to share or use motor vehicle diagnostic data except as necessary to fulfill the dealer's obligation to provide warranty, repair, or service to a consumer.