OHIO LEGISLATIVE SERVICE COMMISSION

Bill Analysis

Yosef Schiff

Sub. S.B. 273*

132nd General Assembly
(As Re-reported by H. Rules and Reference)

Sens. Hackett, Hottinger, Brown, Burke

BILL SUMMARY

Insurance rating agency

- Defines "insurance rating agency" for the purposes of the Revised Code as any rating agency certified or approved by a national entity that has an approval process that meets specified criteria.

Cybersecurity

- Requires insurers to implement an information security program based on the results of a risk assessment in order to safeguard certain business and personal information.
- Requires insurers to develop a formal incident response plan to respond to a cybersecurity event.
- Requires insurers to certify compliance to the Superintendent of Insurance and gives compliant insurers an affirmative defense to certain actions.
- Requires insurers to investigate cybersecurity events.
- Requires insurers to notify certain parties of a cybersecurity event.
- Provides that certain information relating to a cybersecurity event is confidential, privileged, and not subject to disclosure except under limited circumstances.

* This analysis was prepared before the report of the House Rules and Reference Committee appeared in the House Journal. Note that the list of co-sponsors and the legislative history may be incomplete.

- Exempts certain small insurers from the information security program requirements and deems HIPAA-compliant insurers as meeting those requirements.

Motor vehicle ancillary product protection contracts

- Merges the motor vehicle tire or wheel road hazard contract provisions in the motor vehicle ancillary product protection (MVAPP) contract provisions.
- Adds a contract for key replacement as a type of MVAPP contract.
- Allows MVAPP contracts to provide for incidental payment of indemnity under limited circumstances including towing, rental, and emergency road services.
- Exempts a contract that is only for prepaid routine, scheduled maintenance from the definition of a consumer goods service contract.

Surplus lines insurance

- Authorizes domestic insurers to offer surplus lines insurance products as domestic surplus lines insurers.
- Exempts domestic surplus lines insurers from most insurance laws.
- Allows surplus lines brokers to obtain coverage for a person from a domestic surplus lines insurer.

Cancellation of certain insurance policies

- Allows an insurer to include a notice of cancellation of certain insurance policies for nonpayment of premium with a billing notice.

Regulatory authority of the Superintendent of Insurance

- Specifies that nothing in the Health Care Contract Law provisions relating to the termination of health care contracts is to be construed to expand the regulatory authority of the Superintendent of Insurance over vision care providers.

TABLE OF CONTENTS

CONTENT AND OPERATION

Definition of "insurance rating agency"

The bill defines "insurance rating agency" for the purposes of the Revised Code as A.M. Best Rating Services, Inc., Demotech, Inc., or another rating agency certified or approved by a national entity that engages in an approval process that includes all of the following:

- A requirement for the rating agency to register and provide an annual updated filing;
- Record retention requirements;
- Financial reporting requirements;
- Policies for the prevention of misuse of material, nonpublic information;

- Management of conflicts of interest, including prohibited conflicts;
- Prohibited acts and practices;
- Disclosure requirements;
- Required policies, practices, and internal controls;
- Standards of training, experience, and competence for credit analysts.[1]

The bill specifies that any reference in the Revised Code to an insurance rating agency named in the bill is to be construed as a reference to any insurance rating agency as defined by the bill. Any reference in the Revised Code to a specific entity that is *not* named above, but that otherwise meets the definition of "insurance rating agency," is to be construed as a reference to an insurance rating agency as defined by the bill. [2]

The term "insurance rating agency" does not currently appear in the Revised Code. But, the term "rating agency" currently appears in the following provisions of the Revised Code:

- R.C. 126.11(E)(2) provides that, with the exception of certain specified information required to be communicated in offering or disclosure documents, direct communication is permitted between an issuer of public obligations and a rating agency concerning an issuance of public obligations or matters associated with that issuance.[3]
- R.C. 133.22(D)(9) provides exceptions to the requirement that any maximum interest rates set by a political subdivision's taxing authority on anticipatory securities must not exceed the estimated average annual interest rate on the bonds anticipated by those securities. One such exception is the existence of an interest rate swap agreement to the contrary between the subdivision and another person, the obligations of which person are rated in one of the two highest rating categories of a national rating agency. An "anticipatory security" is a security issued in anticipation of the issuance of another security. An "interest rate swap agreement" is an agreement in which one stream of future interest

[1] R.C. 1.65(A).

[2] R.C. 1.65(B).

[3] R.C. 126.11(E)(2), not in the bill.

payments is exchanged for another based on a specified principal amount.[4]

- R.C. 183.51 allows the Treasurer of State to invest certain moneys associated with the Tobacco Master Settlement Agreement in guaranteed investment contracts with providers in the three highest rating categories by two nationally recognized rating agencies. A "guaranteed investment contract" is an insurance contract that guarantees the owner principal repayment and a fixed or floating interest rate for a predetermined period of time.[5]

- R.C. 3901.62 allows a ceding insurer to take credit for any reinsurance ceded as either an asset or a reduction of liability only if at least one listed condition applies. One such condition is that the reinsurance is ceded to an assuming insurer that has been certified by the Superintendent of Insurance as a reinsurer in Ohio and that maintains financial strength ratings from two or more rating agencies that meet the Superintendent's criteria.[6]

- R.C. 3916.13 prohibits certain entities including rating agencies or companies from disclosing a viator or insured's identity or financial or medical condition absent certain circumstances. A "viator" is the owner of a group life insurance policy who sells that policy to another person at a price greater than the cash surrender value but less than the net death benefit. In addition to paying the viator a lump sum, the buyer assumes responsibility for paying the premiums on the plan and receives the death benefits when the viator dies.[7]

- R.C. 3942.02 requires a transportation network company driver to be covered by a primary automobile insurance policy that meets certain requirements. If the policy is purchased from an insurer not holding an Ohio license, the insurer must meet certain criteria. One of those criteria is the insurer must have a credit rating of not less than "A-" from A.M. Best or "A" from Demotech or a similar rating from another rating agency

[4] R.C. 133.01(B) and 133.22(D)(9), not in the bill; Investopedia, *Interest rate swap*, https://www.investopedia.com/terms/i/interestrateswap.asp (accessed April 2, 2018).

[5] R.C. 183.51(D), not in the bill; Investopedia, *Guaranteed investment contract*, https://www.investopedia.com/term/g/guaranteedinvestmentcontract.asp (accessed April 2, 2018).

[6] R.C. 3901.62(D)(1)(c), not in the bill.

[7] R.C. 3916.13 and R.C. Chapter 3916., not in the bill.

recognized by the Department of Insurance. A transportation network company is a business entity operating in Ohio that uses a digital network to connect transportation network company riders to transportation network company drivers who provide transportation network company services. Uber is an example of a transportation network company.[8]

- R.C. 4123.35 requires certain public employers applying for the status of self-insuring employer for workers' compensation purposes to hold a debt rating of Aa3 or higher according to Moody's Investors Service, Inc., or a comparable rating by an independent rating agency similar to Moody's.[9]

- R.C. 4928.23 allows an electric distribution utility to apply to the Public Utilities Commission for a financing order authorizing recovery of certain phase-in and financing costs, including rating agency fees.[10]

Adoption of rules

The bill requires the Superintendent of Insurance, when adopting or amending a rule related to an insurance rating agency, to give consideration to the inclusion of the definition of the term "insurance rating agency" provided above. This includes rules adopted in relation to Health Insuring Corporations.[11]

Cybersecurity

Information security program

The bill requires a licensee (an insurer authorized to do business in Ohio but excluding a purchasing or risk retention group chartered and licensed in another state and an assuming insurer domiciled in another state) to develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment. An information security program is the set of safeguards a licensee uses to handle nonpublic information (business and personal information the disclosure of which would harm the business or expose certain personal details of a customer, e.g., health information, financial information, or certain identifiers like a social security or bank account number). Such a program must be commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities including its

[8] R.C. 3942.01(F) and 3942.02(C)(2)(b), not in the bill.

[9] R.C. 4123.35(B)(2)(g), not in the bill.

[10] R.C. 4928.23 and 4928.231(A)(2)(b), not in the bill.

[11] R.C. 3901.91.

use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control. The risk assessment upon which the program is based must examine the nature and likelihood of any threats posed to the nonpublic information held by the licensee. In particular, the program must be designed to do the following:

- Protect the security and confidentiality of nonpublic information and the security of the information system;
- Protect against any threats or hazards to the security or integrity of nonpublic information and the information system;
- Protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to any consumer; and
- Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed.[12]

Licensee's duties with respect to the program

The bill requires the licensee to do all of the following:

- Designate a party to act on behalf of the licensee and be responsible for the information security program;
- Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including threats to the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers;
- Assess the likelihood and potential damage of the threats described in the above bullet point based on the sensitivity of the nonpublic information;
- Assess the sufficiency of safeguards in place to manage the threats described above;
- Implement information safeguards to manage the threats identified in its ongoing assessment; and
- Not less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.[13]

[12] R.C. 3965.01 and 3965.02(A) and (B).

Risk assessment

The bill requires the licensee to do the following based on its risk assessment:

- Design its information security program to mitigate the identified risks;
- Determine which security measures are appropriate and implement such measures. These measures may include restricting information access to specific parties, identifying and managing important information, encrypting information, testing and monitoring certain important systems, protecting information from physical damage, or establishing audit trails to reconstruct a cybersecurity event (an event resulting in unauthorized access to, disruption of, or misuse of an information system or nonpublic information stored on an information system that has a reasonable likelihood of materially harming any consumer residing in this state or any material part of the normal operations of the licensee).
- Include cybersecurity risks in the licensee's enterprise risk management process;
- Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and
- Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in the risk assessment.[14]

Duties of the board of directors

If the licensee has a board of directors, the board must do the following:

- Require the licensee's executive management or its delegates to develop, implement, and maintain the licensee's information security program;
- Require the licensee's executive management or its delegates to report in writing at least annually:
    - The status of the information security program and the licensee's compliance with the bill; and

[13] R.C. 3965.02(C).

[14] R.C. 3965.02(D).

- Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events or violations and management's responses thereto, and recommendations for changes in the information security program.

- If executive management delegates any responsibilities related to the information security program, it must oversee the delegates' performance of those responsibilities and require the delegates to submit a report that complies with the requirements in the above bullet point.[15]

Third-party service providers

The bill requires a licensee to exercise due diligence in selecting its third-party service provider. A third-party service provider is a person that contracts with a licensee to maintain, process, or store nonpublic information, or is otherwise permitted access to nonpublic information, through its provision of services to the licensee. The bill requires a licensee to require a third-party service provider to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that are accessible to, or held by, the third-party service provider.[16]

Additional considerations

The bill requires a licensee to consider and adjust its information security program in light of changes in technology, the sensitivity of its nonpublic information, threats to information, and its own changing business relationships.[17]

Incident response plan

The bill requires a licensee, as part of the licensee's information security program, to establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromises nonpublic information in the licensee's possession, the licensee's information systems, or the continuing functionality of any aspect of the licensee's business or operations. The bill requires the plan to address all of the following:

---

[15] R.C. 3965.02(E).

[16] R.C. 3965.01 and 3965.02(F).

[17] R.C. 3965.02(G).

- The internal process for responding to a cybersecurity event;
- The goals of the incident response plan;
- The definition of clear roles, responsibilities, and levels of decision-making authority;
- External and internal communications and information sharing;
- Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
- Documentation and reporting regarding cybersecurity events and related incident response activities;
- The evaluation and revision as necessary of the incident response plan following a cybersecurity event.[18]

Compliance certification and affirmative defense

The bill requires each insurer domiciled in Ohio to submit to the Superintendent of Insurance a written statement certifying compliance with all of the above information security program requirements. It requires an insurer to maintain records supporting such certificate for at least five years. To the extent an insurer has identified areas that require material improvement, the insurer shall document the identification and the remedial efforts to address these areas. This documentation must be available for inspection by the Superintendent. The bill allows an insurer domiciled and licensed exclusively in Ohio and no other state to submit a written statement certifying compliance as part of its corporate governance annual disclosure.[19]

The bill provides that a licensee meeting all its requirements relating is deemed to have implemented a cybersecurity program that reasonably conforms to an industry-recognized cybersecurity framework, thus giving the licensee an affirmative defense to any cause of action sounding in tort that is brought under the laws of Ohio or in an Ohio court and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information or restricted information.[20]

---

[18] R.C. 3965.02(H).

[19] R.C. 3965.02(I).

[20] R.C. 3965.02(I); R.C. Chapter 1354., not in the bill.

Investigation of a cybersecurity event

The bill requires a licensee or an outside vendor or service provider designated to act on behalf of the licensee to conduct a prompt investigation when the licensee learns that a cybersecurity event has or may have occurred. At a minimum, the licensee, vendor, or provider must do as much of the following as possible:

- Determine whether a cybersecurity event has occurred;
- Assess the nature and scope of the cybersecurity event;
- Identify any nonpublic information that may have been involved in the cybersecurity event; and
- Perform or oversee reasonable measures to restore the security of the information systems compromised in the cybersecurity event in order to prevent further unauthorized acquisition, release, or use of nonpublic information in the licensee's possession, custody, or control.[21]

If a licensee learns that a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, the bill requires the licensee to take the actions mentioned above or confirm and document that the third-party service provider has done so. The bill requires a licensee to maintain records concerning all cybersecurity events for a period of at least five years from the date of the cybersecurity event and to produce those records upon demand of the Superintendent of Insurance.[22]

Notice of a cybersecurity event

Notice to Superintendent of Insurance

The bill requires each licensee to notify the Superintendent as promptly as possible after a determination that a cybersecurity event involving nonpublic information in the possession of the licensee has occurred, but in no event later than three business days after that determination, when either of the following criteria has been met:

- Both of the following apply:
  - Ohio is the licensee's state of domicile, in the case of an insurer, or the licensee's home state, in the case of an independent insurance agent (an

[21] R.C. 3965.03(A) and (B).

[22] R.C. 3965.03(C) and (D).

insurance agent who is neither employed nor controlled solely by an insurer, whose agency contract with an insurer provides that upon termination of the contract, the ownership of the property rights of all expiration information vests in the agent or the agent's heirs or assigns, and whose agency contract with an insurer permits the agent to represent concurrently other insurers of the agent's choice); and

- The cybersecurity event has a reasonable likelihood of materially harming a consumer or a material part of the normal operations of the licensee.

- The licensee reasonably believes that the nonpublic information involved relates to 250 or more consumers residing in this state and the cybersecurity event is either of the following:

  - An event of which notice is required to be provided to any authority under state or federal law;

  - An event that has a reasonable likelihood of materially harming an Ohio consumer or any material part of the licensee's normal operations.[23]

The bill provides that if a licensee discovers a cybersecurity event in a system maintained by a third-party service provider, the licensee must treat the event as it would if the event occurred in a system maintained by the licensee. Any deadline would begin on the day after the third-party service provider notifies the licensee of the cybersecurity event or the licensee otherwise has actual knowledge of the cybersecurity event, whichever is sooner. The bill specifies that nothing in the bill abrogates an agreement between a licensee and any other party to fulfill the bill's investigation or notice requirements.[24]

As part of this notification, the bill requires a licensee to provide as much of the following as possible:

- The date of the cybersecurity event;

- A description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of any third-party service providers;

[23] R.C. 3965.04(A); R.C. 3905.49(A). not in the bill.

[24] R.C. 3965.04(D).

- How the cybersecurity event was discovered;
- Whether any lost, stolen, or breached information has been recovered and if so, how this was done;
- The identity of the source of the cybersecurity event;
- Whether the licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when such notification was provided;
- A description of the specific types of information acquired without authorization. "Specific types of information" means particular data elements, including types of medical information, types of financial information, or types of information allowing identification of the consumer.
- The period during which the information system was compromised by the cybersecurity event;
- The number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the superintendent and update this estimate with each subsequent report to the superintendent pursuant to this section.
- The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;
- A description of efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur;
- A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event; and
- The name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.[25]

The bill requires the licensee to provide this information in electronic form as directed by the Superintendent. It also specifies that a licensee has a continuing

[25] R.C. 3965.04(B)(1).

obligation to update and supplement initial and subsequent notifications to the Superintendent regarding material developments relating to the cybersecurity event.[26]

Continuing law requires a person to notify any Ohio resident whose computerized personal information was breached if the breach is likely to cause a material risk of identity theft or other fraud. The bill requires a licensee to provide a copy of each such notice to the Superintendent when the licensee is also required to submit the above notification of a cybersecurity event.[27]

Notice to ceding insurer, affected consumers, and the insurance authority of another state or jurisdiction

The bill provides that in the case of a cybersecurity event involving nonpublic information used by or in the possession, custody, or control of a licensee that is acting as an assuming insurer (an insurance company that accepts all or part of the risk underwritten by another insurer for purposes of reinsuring that other insurer), including an assuming insurer domiciled in another state, and that does not have a direct contractual relationship with the affected consumers, both of the following apply:

- The assuming insurer shall notify each affected ceding insurer (an insurance company that transfers all or part of the risk it underwrites to an assuming insurer) and the insurance commissioner of its state or jurisdiction of domicile within three business days of making the determination that a cybersecurity event has occurred.

- The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill all consumer notification requirements under the bill and other state or federal law.[28]

The bill provides similar requirements when the cybersecurity event involved a licensee's third-party service provider. Specifically:

- The assuming insurer must notify each affected ceding insurer and the insurance commissioner of its state or jurisdiction of domicile within three business days of receiving notice from its third-party service provider that a cybersecurity event has occurred.

---

[26] R.C. 3965.04(B)(2).

[27] R.C. 3965.04(C).

[28] R.C. 3965.04(E)(1); R.C. 3901.61, not in the bill.

- The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill all consumer notification requirements under the bill and other state or federal law.[29]

The bill provides that a licensee acting as an assuming insurer has no other notice obligations relating to a cybersecurity event or other data breach under "**Notification to Superintendent of Insurance**," above.[30]

Notice to independent insurance agents

The bill provides that in the case of a cybersecurity event involving nonpublic information used by or in the possession, custody, or control of a licensee that is an insurer or its third-party service provider, that was obtained by the insurer from a consumer accessing the insurer's services through an independent insurance agent, and for which disclosure or notice is required under the continuing law provision addressing the breach of computerized personal information, the insurer shall notify the independent insurance agents of record of all affected consumers.[31]

The bill excuses an insurer from this obligation for any independent insurance agents who are not authorized by law or contract to sell, solicit, or negotiate on behalf of the insurer, and for those instances in which the insurer does not have the current independent insurance agent of record information for an individual consumer.[32]

Superintendent's powers

The bill gives the Superintendent of Insurance power to examine and investigate into the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of the cybersecurity provisions of the bill. Whenever the superintendent has reason to believe that a licensee has been or is engaged in conduct in this state that violates the cybersecurity provisions of the bill, the bill allows the Superintendent to take any necessary or appropriate action to enforce those provisions.[33]

---

[29] R.C. 3965.04(E)(2).

[30] R.C. 3965.04(E)(3).

[31] R.C. 3965.04(F).

[32] R.C. 3965.04(F).

[33] R.C. 3965.05.

The bill also allows the Superintendent to adopt rules as necessary to carry out the bill's provisions and requires the Superintendent to consider the nature, scale, and complexity of licensees in doing so.[34]

Confidentiality and sharing of documents

The bill provides that the following information – including when in the possession or control of National Association of Insurance Commissioners (NAIC) or any vendor, third-party consultant to NAIC, or a third-party service provider – is confidential and privileged, not a public record, prohibited from release, not subject to subpoena, and not subject to discovery or admissible in evidence in any private civil action. It also provides that neither the Superintendent nor any person who received such information while acting under the authority of the Superintendent be permitted or required to testify in any private civil action concerning the information:

- The licensee's incident response plan described in "**Incident response plan**," above;
- The licensee's certification of compliance described in "**Compliance certification and affirmative defense**," above;
- The following information identified in "**Notice to Superintendent of Insurance**," above:
    - A description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of any third-party service providers;
    - How the cybersecurity event was discovered;
    - Whether any lost, stolen, or breached information has been recovered and if so, how this was done;
    - The identity of the source of the cybersecurity event;
    - The period during which the information system was compromised by the cybersecurity event;
    - The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed; and

[34] R.C. 3965.10 and 3965.11.

- A description of efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur.[35]

The bill provides that notwithstanding the confidential nature of these documents, the Superintendent of Insurance may use them in furtherance of any regulatory or legal action brought as a part of the Superintendent's duties. The bill also allows the Superintendent to do any of the following in performing its duties:

- Notwithstanding the confidential nature of the information described above, share such information, and any other information, with regulatory agencies, NAIC and its affiliates and subsidiaries, and law enforcement authorities;

- Receive any information, confidential or not, from NAIC and its affiliates and subsidiaries, and from regulatory and law enforcement officials of other jurisdictions. The bill requires the Superintendent to maintain as confidential or privileged any information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the information.

- Share the confidential information identified above with a third-party consultant or vendor if the consultant or vendor agrees in writing to maintain the confidentiality and privileged status of the information.

- Enter into agreements governing sharing and use of information consistent with the bill's requirements.[36]

The bill provides that disclosure of information to the Superintendent does not constitute a waiver of any applicable privilege or claim of confidentiality in the information.[37]

The bill provides that nothing in the bill prohibits the Superintendent from releasing decisions related to final, adjudicated actions that are open to public inspection pursuant to Ohio's Public Records Law to a database or other clearinghouse service maintained by NAIC or its affiliates or subsidiaries.[38]

---

[35] R.C. 3965.06(A), (B), and (F), 3965.02(H) and (I), and 3965.04(B)(1)(b), (c), (d), (e), (h), (j), and (k).

[36] R.C. 3965.06(C).

[37] R.C. 3965.06(D).

[38] R.C. 3965.06(E).

Exemption from information security program requirements

The bill exempts a licensee from the requirements in "**Information security program**," above if it meets any of the following criteria:

- It has fewer than 20 employees.
- It has less than $5 million in gross annual revenue.
- It has less than $10 million in assets, measured at the end of the licensee's fiscal year.

The bill also provides that a licensee that is subject to and compliant with the privacy and security rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is deemed to meet the bill's requirements, except for those requirements under "**Notice of a cybersecurity event**," above. The bill requires such a licensee to submit a certification of its HIPAA-compliance to the Superintendent and retain all records relating to that certification for a period of five years. To the extent an insurer has identified any areas requiring material improvement, the insurer must document any improvement efforts and make such documentation available to the Superintendent.[39]

The bill requires that notwithstanding any other provision of the bill, a licensee subject to HIPAA must comply with the requirements of any subsequent amendments to HIPAA in the timeframe established in the applicable amendments to HIPAA (see **COMMENT**).

The bill exempts an employee, agent, representative, independent contractor, or designee of a licensee, who is also a licensee, from the requirements in "**Information security program**," above to the extent that the employee, agent, representative, independent contractor, or designee is covered by the information security program of the other licensee. The bill provides that if a licensee ceases to qualify for an exemption, the licensee shall have 180 days after the date it ceases to qualify to comply with requirements in "**Information security program**," above.[40]

Affirmative defense

The bill provides that a licensee that satisfies the bill's provisions is entitled to an affirmative defense to any cause of action sounding in tort that is brought under the laws of Ohio or in an Ohio court and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning nonpublic

[39] R.C. 3965.07(A) and (B); 45 Code of Federal Regulations Parts 160 and 164, not in the bill.

[40] R.C. 3965.07(D).

information. The bill specifies that this affirmative defense does not limit any other affirmative defense available to a licensee.[41]

Exclusive state standards

The bill provides that notwithstanding any other provision of law, the provisions of the bill and any rules adopted pursuant to the bill constitute the exclusive state standards and requirements applicable to licensees regarding cybersecurity events, the security of nonpublic information, data security, investigation of cybersecurity events, and notification to the superintendent of cybersecurity events.[42]

Effective dates

The bill gives licensees two years from the bill's effective date to implement the provisions described in "**Third-party service providers**," above.[43]

Industry-recognized cybersecurity framework

The bill specifies that it is intended to enact an industry-recognized cybersecurity framework for the purposes of Chapter 1354. of the Revised Code, which gives a covered entity – a business that accesses, maintains, communicates, or processes personal information or restricted information in or through one or more systems, networks, or services located in or outside this state – an affirmative defense to any cause of action sounding in tort that is brought under the laws of Ohio or in an Ohio court and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information or restricted information.[44]

Definitions

"**Consumer**" means an individual who is a resident of this state and whose nonpublic information is in a licensee's possession, custody, or control. "Consumer" includes an applicant, policyholder, insured, beneficiary, claimant, and certificate holder.[45]

---

[41] R.C. 3965.08.

[42] R.C. 3965.09.

[43] Section 2 of the bill.

[44] Section 3 of the bill; R.C 1354.01 and Chapter 1354., not in the bill.

[45] R.C. 3965.01.

"**Cybersecurity event**" means an event resulting in unauthorized access to, disruption of, or misuse of an information system or nonpublic information stored on an information system that has a reasonable likelihood of materially harming any consumer residing in this state or any material part of the normal operations of the licensee. "Cybersecurity event" does not include the unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization. "Cybersecurity event" does not include an event with regard to which the licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.[46]

"**Information system**" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic nonpublic information, as well as any specialized system such as industrial and process controls systems, telephone switching and private branch exchange systems, and environmental control systems.[47]

"**Insurer**" means any person engaged in the business of insurance, guaranty, or membership, an inter-insurance exchange, a mutual or fraternal benefit society, or a health insuring corporation. "Insurer" does not include any agency, authority, or instrumentality of the United States, its possessions and territories, the Commonwealth of Puerto Rico, the District of Columbia, or a state or political subdivision of a state.[48]

"**Licensee**" means any person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this state. "Licensee" includes an insurer. "Licensee" does not include a purchasing group or a risk retention group chartered and licensed in another state or a licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction.[49]

"**Nonpublic information**" means information that is not publicly available information and is one of the following:

- Business-related information of a licensee the tampering with, unauthorized disclosure of, access to, or use of which, would cause a

[46] R.C. 3965.01.

[47] R.C. 3965.01.

[48] R.C. 3965.01; R.C. 3901.32, not in the bill.

[49] R.C. 3965.01.

material adverse impact to the business, operation, or security of the licensee;

- Information concerning a consumer that because of the name, number, personal mark, or other identifier contained in the information can be used to identify that consumer in combination with any one or more of the following data elements:
    - Social security number;
    - Driver's license, commercial driver's license, or state identification card number;
    - Account, credit card, or debit card number;
    - Any security code, access code, or password that would permit access to the consumer's financial account;
    - Biometric records.
- Any information or data, except age or gender, that is in any form or medium created by or derived from a health care provider or a consumer, that can be used to identify a particular consumer, and that relates to any of the following:
    - The past, present, or future physical, mental, or behavioral health or condition of the consumer or a member of the consumer's family;
    - The provision of health care to the consumer;
    - Payment for the provision of health care to the consumer.[50]

"**Publicly available information**" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from federal, state, or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state, or local law. For the purposes of the bill, a licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine both of the following:

- That the information is of the type that is available to the general public;

[50] R.C. 3965.01.

- Whether a consumer can direct that the information not be made available to the general public and, if so, that the consumer has not done so.[51]

Motor vehicle ancillary product protection contracts

Motor vehicle tire or wheel road hazard contracts

The bill merges the motor vehicle tire or wheel road hazard contract (road hazard contract) provisions into the motor vehicle ancillary product protection (MVAPP) contract provisions. Under continuing law, all road hazard and MVAPP contracts are subject to certain requirements. For example, such a contract must be covered by a reimbursement insurance policy. It must contain certain items, including a disclosure that the contract is not insurance, a disclosure that the obligations are guaranteed under a reimbursement insurance policy, and the contract holder's rights under that policy. The reimbursement policy must include certain statements regarding procedures for contract holders (those who purchased the road hazard or MVAPP contract) to collect under the provider's policy and protections in the event of cancellation of the policy. Finally, the sale or issuance of road hazard or MVAPP contracts is subject to the Consumer Sales Practices Act.[52]

The bill repeals the existing provisions for road hazard contracts and merges these provisions into MVAPP provisions by classifying a contract for the repair or replacement of tires or wheels damaged because of a road hazard as an MVAPP contract. The bill also incorporates existing road hazard contract provisions that are not applicable to other MVAPPs. For example, a road hazard contract in which the provider is a tire manufacturer is exempt from the reimbursement insurance requirements if the contract contains certain items including a statement that the contract is not insurance, that any obligations are the responsibility of the provider, contact information for the provider and any contract administrators, and the procedure for making a claim.[53]

The bill merely merges the road hazard contract provisions into the MVAPP provisions; it does not make any substantive changes to the requirements for road hazard contracts.[54]

---

[51] R.C. 3965.01.

[52] R.C. 3905.425 and 3905.426.

[53] R.C. 3905.426(J) and R.C. 3905.425 (repealed); conforming change in R.C. 3905.423(A)(3)(d).

[54] R.C. 3905.426(A)(3)(a)(iv).

Other MVAPP provisions

The bill adds a contract for the replacement of a lost, stolen, or inoperable key or key fob as a type of MVAPP contract.[55]

The bill also provides that an MVAPP contract may, but is not required to, provide for incidental payment of indemnity under limited circumstances, including towing, rental, and emergency road services (an expansion from merely applying to road hazard contracts as under current law).[56]

Under continuing law, unless issued by an Ohio insurer, an MVAPP contract is not considered insurance. Under the bill, a contract explicitly excluded from the definition of an MVAPP contract does not constitute a contract substantially amounting to insurance, or the contract's issuance the business of insurance.[57]

Also, the bill revises the list of contracts that are not considered MVAPP contracts. Under the bill, the excluded contracts are:

- A contract to perform or pay for motor vehicle repairs due to defects, normal wear and tear, or part failures that is effective for a specified duration and paid for by means other than the purchase of a motor vehicle (continuing law, but defined as a "motor vehicle service contract" under the bill);
- A vehicle protection product warranty (continuing law);
- A home service contract (continuing law);
- A consumer goods service contract (continuing law);
- A contract for prepaid routine, scheduled maintenance only (added by the bill).[58]

In addition to exempting a contract for prepaid routine, scheduled maintenance from the definition of an MVAPP contract, the bill also exempts it from the definition of a consumer goods service contract (a contract to perform or pay for repairs, replacement, or maintenance of consumer goods due to a defect in materials or

[55] R.C. 3905.426(A)(3)(a)(v).

[56] R.C. 3905.426(A)(3)(b).

[57] R.C. 3905.426(H).

[58] R.C. 3905.426(A)(3)(c).

workmanship, normal wear and tear, power surges, or accidental damage from handling, that is effective for a specified duration and paid for by means other than the purchase of the consumer goods).[59]

Motor vehicle service contracts

Under existing law, a contract to perform or pay for motor vehicle repairs due to defects, normal wear and tear, or part failures that is effective for a specified duration and paid for by means other than the purchase of a motor vehicle is excluded from the definition of "consumer goods service contract" and "motor vehicle ancillary product protection (MVAPP) contract." The bill keeps these exclusions in place, but identifies such a contract as a "motor vehicle service contract" (MVSC). In the definition, the bill specifies that an MVSC may, but is not required to, provide for incidental payment of indemnity under limited circumstances including towing, rental, and emergency road services.[60]

Definitions

"**Motor vehicle ancillary product protection contract**" means a contract or agreement that is effective for a specified duration and paid for by means other than the purchase of a motor vehicle, or its parts or equipment, to perform any one or more of the following services:

- Repair or replacement of glass on a motor vehicle necessitated by wear and tear or damage caused by a road hazard (continuing law);
- Removal of a dent, ding, or crease without affecting the existing paint finish using paintless dent removal techniques but which expressly excludes replacement of vehicle body panels, sanding, bonding, or painting (continuing law);
- Repair to the interior components of a motor vehicle necessitated by wear and tear but which expressly excludes replacement of any part or component of a motor vehicle's interior (continuing law);
- Repair or replacement of tires or wheels damaged because of a road hazard (added by the bill as part of merging the road hazard contract provisions into the MVAPP contract provisions);

[59] R.C. 3905.423(A)(3)(e).

[60] R.C. 3905.426(A)(4); conforming changes in R.C. 3905.423(A)(3)(a) and 3905.426(A)(3)(c)(i).

- Replacement of a lost, stolen, or inoperable key or key fob (added by the bill).[61]

"**Road hazard**" means a condition that may cause damage or wear and tear to a tire or wheel on a public or private roadway, roadside, driveway, or parking lot or garage, including potholes, nails, glass, road debris, and curbs. "Road hazard" does not include fire, theft, vandalism or malicious mischief, or other perils normally covered by automobile physical damage insurance.[62]

Surplus lines insurance

Background

The bill authorizes a domestic insurer to be designated as a domestic surplus lines insurer,[63] thereby allowing it to offer surplus lines insurance products. Under current law, domestic insurers must meet the various requirements of the Ohio insurance laws in order to transact the business of insurance in Ohio. The requirements are such that domestic insurers might not offer certain high-risk products because those products do not comply with existing regulations. These high-risk products are known as surplus lines products. By definition, they are products that a person seeks but cannot find within Ohio because of the risk associated with the product, but can find elsewhere.[64] If the person could find such a product in Ohio, then it would not be a surplus lines product because it would not be so high-risk as to not comply with existing regulations.

The bill authorizes a domestic insurer to offer these high-risk products by exempting such an insurer from many of the Ohio insurance laws. The bill does this by defining such an insurer as an *unauthorized* insurer, or an insurer that, although offering a product to an Ohio resident and coming under the jurisdiction of Ohio courts, is not regulated under the Ohio insurance laws.[65]

---

[61] R.C. 3905.426(A)(3)(a).

[62] R.C. 3904.426(A)(6).

[63] R.C. 3905.332.

[64] R.C. 3905.33(B).

[65] R.C. 3901.17, not in the bill; R.C. 3905.33(A)(3) and 3905.332(C), (D), (E), and (G); *Akron Co. v. Fidelity General Ins. Co.*, 229 F. Supp. 397, 400 (1964).

Conditions

Under the bill, in order to become a domestic surplus lines insurer, all of the following conditions must be met:

- The domestic insurer must possess minimum capital and surplus of at least $15 million;
- The domestic insurer must seek to become a domestic surplus lines insurer pursuant to a resolution adopted by its board of directors; and
- The Superintendent of Insurance must authorize the designation of the insurer as a domestic surplus lines insurer in writing.[66]

Taxes

Under the bill, a person who obtains a surplus lines product from a domestic surplus lines insurer is subject to a tax of 5% of the gross premium, if any, after a deduction for return premium, if any.[67]

Under the bill, a domestic surplus lines insurer is not subject to the annual franchise tax on the privilege of being an insurance company.[68]

Exemptions from specific insurance laws

The bill exempts domestic surplus lines insurers from the provisions of the Ohio Insurance Guaranty Association Act, which provides a mechanism for the payment of covered claims under certain insurance policies and protects claimants and policyholders from the effects of an insurer's insolvency. In particular, the bill exempts domestic surplus lines insurers from the protection of the Association's accounts.[69]

The bill exempts domestic surplus lines insurers in the same manner as surplus lines policies issued by nondomestic insurers from all statutory requirements relating to the following:

- Insurance rating and rating plans;
- Policy forms; and

---

[66] R.C. 3905.332(B).

[67] R.C. 3905.332(F); R.C. 3905.36, not in the bill.

[68] R.C. 3905.332(F); R.C. 5725.18, not in the bill.

[69] R.C. 3905.332(H) and 3955.05(S).

- Policy cancellation and renewal.[70]

The bill subjects domestic surplus lines insurers to all financial, reserve, and solvency requirements under the Ohio insurance laws from which the insurers are not specifically exempted.[71]

Licensed surplus lines brokers

The bill allows licensed surplus lines brokers to obtain insurance from a domestic surplus lines insurer.[72] It also prohibits any person who is not so licensed from obtaining liability insurance from a domestic surplus lines insurer on behalf of a purchasing group located in Ohio.[73]

Cancellation of certain insurance policies

Current law allows an insurer to include a notice of cancellation of an automobile insurance policy for nonpayment of premium with a billing notice. Such a cancellation must be effective at least ten days after the notice was mailed. The bill additionally allows such a notice to be sent for a policy of commercial property insurance, commercial fire insurance, commercial casualty insurance other than fidelity or surety bonds, or medical malpractice insurance.[74]

The bill also applies these provisions to a notice of cancellation of a personal lines insurance policy, defined as "any policy of insurance issued to a natural person for personal or family protection, including basic property, dwelling fire, homeowner's, tenant's, inland marine, personal liability, and personal umbrella liability coverage." In addition, the bill specifies that, subject to the ten-day effective date mentioned above, a cancellation is effective on or after the due date of the bill.[75]

---

[70] R.C. 3905.332(I).

[71] R.C. 3905.332(J).

[72] R.C. 3905.30(C).

[73] R.C. 3960.11(D).

[74] R.C. 3937.25(B) and (D)(2); R.C. 3937.28(C).

[75] R.C. 3937.47.

Regulatory authority of the Superintendent of Insurance

The bill specifies that nothing in the Health Care Contract Law provisions relating to the termination of health care contracts is to be construed to expand the regulatory authority of the Superintendent of Insurance over vision care providers.[76]

COMMENT

As noted in "**Exemption from information security program requirements**," above, a licensee subject to HIPAA must comply with the requirements of any subsequent amendments to HIPAA in the timeframe established in the applicable amendments to HIPAA. This provision raises questions concerning the General Assembly's ability to delegate its legislative authority.[77]

HISTORY

ACTION	DATE
Introduced	03-15-18
Reported, S. Insurance and Financial Institutions	06-05-18
Passed Senate (32-0)	06-27-18
Reported, H. Insurance	12-06-18
Re-reported, H. Rules and Reference	---

S0273-RRH-132.docx/ec

[76] R.C. 3963.02(E)(5).

[77] Ohio Const., art. II, sec. 26; *State v. Gill*, 63 Ohio St.3d 53.