OHIO LEGISLATIVE SERVICE COMMISSION

Bill Analysis

Emily E. Wendel

S.B. 220

132nd General Assembly
(As Introduced)

Sens. Hackett and Bacon

BILL SUMMARY

- Creates an affirmative defense to any tort action against a covered entity because of a data breach of personal information, if the entity is accused of failing to implement reasonable information security controls to prevent the breach and the entity has a cybersecurity program that meets the bill's requirements.

Definitions

- Defines "covered entity" as a business or nonprofit entity operating in Ohio that accesses, maintains, communicates, or handles personal information.

- Specifies that "personal information" has the same meaning as in the Consumer Protection Law, and gives "data breach" the same meaning as "breach of the security of the system" in the Consumer Protection Law.

Requirements to qualify for the affirmative defense

- Requires a covered entity, in order to be eligible to use the affirmative defense, to create, maintain, and comply with a written cybersecurity program that contains certain safeguards for the protection of personal information that complies with an industry cybersecurity framework approved by the bill.

- Specifies several requirements for the design, scale, and scope of the cybersecurity program.

- Requires the cybersecurity program to be in substantial compliance with one of several listed industry and government cybersecurity frameworks, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Other provisions

- Specifies that the bill does not provide a private right of action that would allow a person to sue a covered entity for failing to follow the bill's cybersecurity requirements.
- Specifies that the bill's provisions are severable.
- States that the bill is intended to encourage improved cybersecurity through voluntary action and not to create a minimum cybersecurity standard that must be achieved.

CONTENT AND OPERATION

The bill creates an affirmative defense to any tort action against a covered entity because of a data breach of personal information, if the entity is accused of failing to implement reasonable information security controls to prevent the breach. To be eligible to use the affirmative defense, the entity must have a cybersecurity program that meets the bill's requirements. The bill refers to the affirmative defense as a "safe harbor."

(A tort action is a civil lawsuit for a legal wrong or injury, such as negligence, for which the person bringing the lawsuit seeks compensation for damages. An affirmative defense is a factor that, if proven by the defendant, makes the defendant not liable for the damages.)

Definitions

Covered entities

Under the bill, a "covered entity" is a business that accesses, maintains, communicates, or handles personal information. "Business" means any limited liability company (LLC), limited liability partnership (LLP), corporation, sole proprietorship, nonprofit corporation, or unincorporated nonprofit association that operates in Ohio.[1]

Personal information

The bill specifies that "personal information" has the same meaning as in Ohio's Consumer Protection Law. Under that law, personal information means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when

[1] R.C. 1354.01(A) and (B).

the data elements are not encrypted, redacted, or altered by any method or technology to make them unreadable:

- The individual's Social Security number;
- The individual's driver's license or state identification card number;
- The individual's account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to the individual's financial account.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or any of the following media that are widely distributed:

- Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television;
- Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to those news media;
- Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation;
- Any type of media similar in nature to any of those items, entities, or activities.[2]

Data breach

Under the bill, "data breach" has the same meaning as "breach of the security of the system" in the Consumer Protection Law. That term means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of an Ohio resident.

For purposes of that definition, good faith acquisition of personal information by an employee or agent of the person for purposes of the person is not a breach of the security of the system, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure. And, acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or

[2] R.C. 1354.01(G). See also R.C. 1349.19(A)(7), not in the bill.

pursuant to a subpoena, order, or duty of a regulatory state agency, is not a breach of the security of the system.[3]

Requirements to qualify for the affirmative defense

To be eligible to use the bill's affirmative defense, a covered entity must create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information that complies with an industry cybersecurity framework approved by the bill.[4]

Cybersecurity program requirements

The bill requires a covered entity's cybersecurity program to be designed to do all of the following:[5]

- Protect the security and confidentiality of personal information;
- Protect against any anticipated threats or hazards to the security or integrity of personal information;
- Protect against unauthorized access to and acquisition of personal information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

The scale and scope of a covered entity's cybersecurity program is considered appropriate if it is based on all of the following factors:[6]

- The entity's size and complexity of the covered entity;
- The nature and scope of the entity's activities;
- The sensitivity of the personal information to be protected;
- The cost and availability of tools to improve information security and reduce vulnerabilities;
- The resources available to the entity.

---

[3] R.C. 1354.01(C). See also R.C. 1349.19(A)(1), not in the bill.

[4] R.C. 1354.02(A) and (D).

[5] R.C. 1354.02(B).

[6] R.C. 1354.02(C).

Approved cybersecurity frameworks

Under the bill, a covered entity's cybersecurity program also must be in substantial compliance with one of the following industry cybersecurity frameworks:[7]

- The National Institute of Standards and Technology (NIST) Cybersecurity Framework, which is the framework developed by the Institute for improving critical infrastructure cybersecurity, as updated from time to time;
- NIST Special Publication 800-171;
- NIST Special Publications 800-53 and 800-53a;
- The Federal Risk and Authorization Management Program;
- Center for Internet Security Critical Security Controls;
- International Organization for Standardization/International Electrotechnical Commission 27000 Family – Information Security Management Systems.

If the covered entity is regulated by the state and the federal government, the entity instead may be in substantial compliance with the entirety of any of the following:[8]

- The security requirements of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), which governs healthcare;
- Title V of the federal Gramm-Leach-Bliley Act of 1999, which applies to financial institutions;
- The Federal Information Security Modernization Act of 2014, which generally covers federal agencies.

After an update to any of those cybersecurity frameworks, a covered entity has a one-year period from the effective date of the updated framework to comply with the update.[9]

---

[7] R.C. 1354.01(E) and 1354.03(A).

[8] R.C. 1354.03(B).

[9] R.C. 1354.02(D).

Other provisions

No private right of action

The bill specifies that it does not provide a private right of action, including a class action, with respect to any act or practice regulated under those sections. In other words, the bill does not allow a person to sue a covered entity for failing to follow the bill's cybersecurity requirements, unless another law would allow the person to do so.[10]

Severability

The bill specifies that if any of its provisions or the application of those provisions to a covered entity is ruled invalid, the remainder of those provisions and their application to other entities is not affected. (The Revised Code provides generally that this principle of severability applies to all Ohio statutes.)[11]

Legislative intent

The bill states that its purpose is to establish a legal safe harbor to be pled as an affirmative defense, as described above. It also states that the bill is intended to be an incentive and to encourage businesses to achieve a higher level of cybersecurity through voluntary action. It does not, and is not intended to, create a minimum cybersecurity standard that must be achieved, nor may it be read to impose liability upon businesses that do not obtain or maintain practices in compliance with the cybersecurity frameworks referenced in the bill.[12]

HISTORY

ACTION	DATE
Introduced	10-17-17

S0220-I-132.docx/ts

[10] R.C. 1354.04.

[11] R.C. 1354.05. See also R.C. 1.50, not in the bill.

[12] Section 2 of the bill.