OHIO LEGISLATIVE SERVICE COMMISSION

**Bill Analysis**

Emily E. Wendel

# Sub. S.B. 220*

132nd General Assembly
(As Reported by S. Gov't Oversight & Reform)

**Sens.** Hackett and Bacon

## BILL SUMMARY

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

### Definitions

- Defines "covered entity" as a business or nonprofit entity, including a financial institution, that accesses, maintains, communicates, or handles personal information or restricted information.

- Provides definitions for "personal information," "restricted information," and "data breach."

### Requirements to qualify for the affirmative defense

- Requires a covered entity, in order to be eligible for the affirmative defense, to create, maintain, and comply with a written cybersecurity program that contains certain safeguards for the protection of personal information, restricted information, or both.

- Requires the cybersecurity program to meet the bill's design, scale, and scope requirements and to reasonably comply with an industry recognized cybersecurity framework listed in the bill.

---

* This analysis was prepared before the report of the Senate Government Oversight and Reform Committee appeared in the Senate Journal. Note that the list of co-sponsors and the legislative history may be incomplete.

- Allows a covered entity to have a cybersecurity program that protects personal information and therefore to be entitled to assert an affirmative defense to a cause of action involving a data breach concerning personal information.

- Allows a covered entity instead to have a cybersecurity program that protects both personal information and restricted information and therefore to be entitled to assert an affirmative defense to a cause of action involving a data breach concerning personal information or restricted information.

### 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, 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 or restricted information in or through one or more systems, networks, or services located in or outside Ohio. "Business" means any limited liability company (LLC), limited liability partnership (LLP), corporation, sole proprietorship, association, or other group, however organized and whether

operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of Ohio, any other state, the United States, or any other country, or the parent or subsidiary of a financial institution.[1]

## Covered information

### 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 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]

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

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

### Restricted information

Under the bill, "restricted information" means any information about an individual, other than personal information, that can be used to distinguish or trace the individual's identity or that is linked or linkable to an individual, if the information is not encrypted, redacted, or altered by any method or technology to make it unreadable. ("Encrypted" and "redacted" have the same meanings as in the Consumer Protection Law.) [3]

For example, if an unencrypted database contained only an individual's residence address, birthdate, and driver's license number, that information would not be considered personal information under the bill because it did not include the person's name, but it probably would be considered restricted information because it would be possible to identify the person based on the information.

### Data breach

Under the bill, "data breach" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information or restricted 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 person or property.

For purposes of that definition, good faith acquisition of personal information or restricted information by an employee or agent of the person for purposes of the person is not a data breach, provided that the information is not used for an unlawful purpose or subject to further unauthorized disclosure. And, acquisition of personal information or restricted information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency, is not a data breach.[4]

## Requirements to qualify for the affirmative defense

To be eligible to use the bill's affirmative defense, a covered entity must do one of the following:

(1) Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of *personal information*, that meets the bill's design, scale, and scope requirements, and that

[3] R.C. 1354.01(E).

[4] R.C. 1354.01(C).

reasonably complies with an industry recognized cybersecurity framework listed in the bill;

(2) Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of *both personal information and restricted information*, that meets the bill's design, scale, and scope requirements, and that reasonably complies with an industry recognized cybersecurity framework listed in the bill.

A covered entity that meets the requirements under (1) above is entitled to assert an affirmative defense to any cause of action sounding in tort that is brought under the laws of Ohio or in the courts of Ohio and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information. A covered entity that meets the requirements under (2) above is entitled to assert an affirmative defense to any such cause of action involving a data breach concerning personal information or restricted information.[5]

### Cybersecurity program requirements

The bill requires a covered entity's cybersecurity program to be designed to do all of the following with respect to the information it is meant to protect:[6]

- Protect the security and confidentiality of the information;
- Protect against any anticipated threats or hazards to the security or integrity of the information;
- Protect against unauthorized access to and acquisition of the 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:[7]

- The entity's size and complexity of the covered entity;
- The nature and scope of the entity's activities;
- The sensitivity of the information to be protected;

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

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

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

- The cost and availability of tools to improve information security and reduce vulnerabilities;

- The resources available to the covered entity.

### Approved cybersecurity frameworks

Under the bill, a covered entity's cybersecurity program also must reasonably comply with an industry recognized cybersecurity framework. The program meets that requirement if one of the following apply:[8]

- The program reasonably complies with the current version of any of the following or any combination of the following frameworks:

    - The Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology (NIST);

    - NIST Special Publication 800-171;

    - NIST Special Publications 800-53 and 800-53a;

    - The Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework;

    - The Center for Internet Security Critical Security Controls for Effective Cyber Defense;

    - The International Organization for Standardization/International Electrotechnical Commission 27000 Family – Information Security Management Systems.

- The program reasonably complies with both the current version of the Payment Card Industry (PCI) Data Security Standard and the current version of another applicable framework listed above.

- The covered entity is regulated by the state, by the federal government, or both, and the program reasonably complies with the entirety of the current version of any of the following:[9]

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

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

- 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.

When a final revision to a cybersecurity framework in the first list above is published, a covered entity whose cybersecurity program reasonably complies with that framework must reasonably comply with the revised framework not later than one year after the publication date stated in the revision. And, when a statutory framework in the second list above is amended, a covered entity whose cybersecurity program reasonably complies with that framework must reasonably comply with the amended framework not later than one year after the effective date of the amended framework.

Finally, if a covered entity's cybersecurity program reasonably complies with a combination of industry recognized cybersecurity frameworks, other than the statutory frameworks in the second list above, and two or more of those frameworks are revised, the entity must reasonably comply with all of the revised frameworks not later than one year after the latest publication date stated in the revisions.[10]

## 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 the bill. 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.[11]

### 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

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

[11] R.C. 1354.04.

their application to other entities is not affected. (The Revised Code provides generally that this principle of severability applies to all Ohio statutes.)[12]

### 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 bill.[13]

## HISTORY

| ACTION | DATE |
|---|---|
| Introduced | 10-17-17 |
| Reported, S. Gov't Oversight & Reform | --- |

S0220-RS-132.docx/ec

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

[13] Section 2 of the bill.