OHIO LEGISLATIVE SERVICE COMMISSION

Sub. Bill Comparative Synopsis

Emily E. Wendel

S.B. 220

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

This table summarizes how the latest substitute version of the bill differs from the immediately preceding version and the As Introduced version. It addresses only the topics on which the versions differ substantively. It does not list topics on which the bills are substantively the same.

Topic	Previous Version (As Introduced)	Sub. Version Adopted by Committee (L_132_0943-5)	Sub. Version (L_132_0943-8)
Covered entities and types of information	Specifies that a covered entity for purposes of the bill is a business that accesses, maintains, communicates, or handles personal information. Defines "business" as any limited liability company, limited liability partnership, corporation, sole proprietorship, or nonprofit corporation or unincorporated nonprofit association that operates in Ohio. Specifies that "personal information" has the same meaning as in the Consumer Protection Law,	Specifies that a covered entity for purposes of the bill is a business that accesses, maintains, communicates, or processes personal information in or through one or more systems, networks, or services located in or outside Ohio. Defines "system" to have the same meaning as in the Consumer Protection Law. Defines "business" as any limited liability company, limited liability partnership, corporation, sole proprietorship, association, or other group, however organized and	Specifies that a covered entity for purposes of the bill is 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 Ohio. Defines "business" as any limited liability company, limited liability partnership, 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

Topic	Previous Version (As Introduced)	Sub. Version Adopted by Committee (L_132_0943-5)	Sub. Version (L_132_0943-8)
	which defines that term as 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 several listed data elements, including a Social Security or credit card number, when the data elements are not encrypted, redacted, or altered by any method of technology to make them unreadable *(R.C. 1354.01 and R.C. 1349.19, not in the bill)*.	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. Specifies that "personal information" has the same meaning as in the Consumer Protection Law, which defines that term as 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 several listed data elements, including a Social Security or credit card number, when the data elements are not encrypted, redacted, or altered by any method of technology to make them unreadable *(R.C. 1354.01 and R.C. 1349.19, not in the bill)*.	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. Specifies that "personal information" has the same meaning as in the Consumer Protection Law, which defines that term as 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 several listed data elements, including a Social Security or credit card number, when the data elements are not encrypted, redacted, or altered by any method of technology to make them unreadable. Defines "restricted information" as 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 of technology to make it unreadable.

Topic	Previous Version (As Introduced)	Sub. Version Adopted by Committee (L_132_0943-5)	Sub. Version (L_132_0943-8)
			Specifies that "encrypted" and "redacted" have the same meanings as in the Consumer Protection Law *(R.C. 1354.01 and R.C. 1349.19, not in the bill).*
Affirmative defense	Requires a covered entity seeking a safe harbor under the bill to create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and that meets the bill's requirements, including requirements regarding the features, scale, and scope of the program and a requirement that the program comply with an industry cybersecurity framework listed in the bill. States that a covered entity that implements and maintains a cybersecurity program that complies with an industry cybersecurity framework listed in the bill must be deemed to be in compliance with the section of law that creates the affirmative defense. States that compliance with that section constitutes an affirmative defense to any cause of action sounding in tort that alleges the	Requires a covered entity seeking an affirmative defense under the bill to create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and that meets the bill's requirements, including requirements regarding the features, scale, and scope of the program and a requirement that the program *reasonably* comply with an industry *recognized* cybersecurity framework listed in the bill. States that a covered entity that complies with those requirements 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. Specifies that "data breach" has the same meaning as "breach of the	Requires a covered entity seeking an affirmative defense under the bill to 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* and that meets the bill's requirements regarding the features, scale, and scope of the program and a requirement that the program reasonably comply 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* and that meets the bill's

Topic	Previous Version (As Introduced)	Sub. Version Adopted by Committee (L_132_0943-5)	Sub. Version (L_132_0943-8)
	failure to implement reasonable security controls resulted in a data breach. Specifies that "data breach" has the same meaning as "breach of the security of the system" in the Consumer Protection Law, which defines that term to mean 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 (R.C. 1354.01 and 1354.02 and R.C. 1349.19, not in the bill)*.	security of the system" in the Consumer Protection Law, which defines that term to mean 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 (R.C. 1354.01 and 1354.02 and R.C. 1349.19, not in the bill)*.	requirements regarding the features, scale, and scope of the program and a requirement that the program reasonably comply with an industry recognized cybersecurity framework listed in the bill. States that a covered entity that complies with option 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*. States that a covered entity that complies with option 2 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 or restricted information*.

Topic	Previous Version (As Introduced)	Sub. Version Adopted by Committee (L_132_0943-5)	Sub. Version (L_132_0943-8)
			Specifies that "data breach" 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 person or property *(R.C. 1354.01 and 1354.02).*
Industry recognized cybersecurity frameworks	Defines "NIST Cybersecurity Framework" as the Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology, as updated from time to time, and requires a covered entity seeking an affirmative defense to comply with that framework or another framework listed in the bill *(R.C. 1354.01(E)).* Specifies that a covered entity must be deemed to be in compliance with the section of law that creates the affirmative defense if any of the following apply: - The covered entity's cybersecurity program complies with the NIST Cybersecurity Framework.	Specifies that a covered entity's cybersecurity program, as described in the section of law that creates the affirmative defense, reasonably complies with an industry recognized cybersecurity framework for purposes of that section if either of the following apply: - The cybersecurity program reasonably complies with the current version of any of the following or any combination of the following: o The Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and	Same as L_132_0943-5, but also: Allows a covered entity's cybersecurity program to reasonably comply with both the current version of the Payment Card Industry (PCI) Data Security Standard and the current version of another applicable industry recognized cybersecurity framework in the first list in the column to the left. Specifies that when a final revision to the PCI Data Security Standard is published, a covered entity whose cybersecurity program reasonably complies with that standard must reasonably comply with the revised standard not later than one year after the publication date stated in the revision.

Topic	Previous Version (As Introduced)	Sub. Version Adopted by Committee (L_132_0943-5)	Sub. Version (L_132_0943-8)
	- The covered entity is in substantial compliance with any of the following: ○ 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. - The covered entity is regulated by the state and the federal government and is in substantial compliance with the entirety of any of the following: ○ The security	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 covered entity is regulated by the state, by the federal government, or both, and the cybersecurity program reasonably complies with the entirety of	Provides that if a covered entity's cybersecurity program reasonably complies with a combination of industry recognized cybersecurity frameworks, other than the statutory frameworks listed in the column to the left, and two or more of those frameworks are revised, the covered entity must reasonably comply with all of the revised frameworks not later than one year after the latest publication date stated in the revisions *(R.C. 1354.03).*

Topic	Previous Version (As Introduced)	Sub. Version Adopted by Committee (L_132_0943-5)	Sub. Version (L_132_0943-8)
	requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA); ○ Title V of the Gramm-Leach-Bliley Act of 1999; ○ The Federal Information Security Modernization Act of 2014. Specifies that, following any update to the NIST Cybersecurity Framework, or other industry recognized data security framework, covered entity has a period of one year from the stated effective date as prescribed in the framework to comply with the update *(R.C. 1354.02(D) and 1354.03)*.	the current version of any of the following: ○ The security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA); ○ Title V of the Gramm-Leach-Bliley Act of 1999; ○ The Federal Information Security Modernization Act of 2014. Specifies that when a final revision to a 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. Specifies that when a 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	

Topic	Previous Version (As Introduced)	Sub. Version Adopted by Committee (L_132_0943-5)	Sub. Version (L_132_0943-8)
		framework not later than one year after the effective date of the amended framework *(R.C. 1354.03)*.	
Intent statement	States that the purpose of the bill is to establish a legal safe harbor to be pled as an affirmative defense to a cause of action sounding in tort that alleges the failure to implement reasonable information security controls resulted in a data breach. Provides that the safe harbor applies to all covered entities that implement a cybersecurity program that complies with the Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology, or other industry recognized data security framework. Specifies that the bill must not be read to impose liability upon businesses that do not obtain or maintain practices in compliance with those frameworks *(Section 2 of the bill)*.	States that the purpose of the bill is to establish a legal safe harbor to be pled as an affirmative defense to a cause of action sounding in tort that alleges *or relates to* the failure to implement reasonable information security controls, *resulting* in a data breach. Provides that the safe harbor applies to all covered entities that implement a cybersecurity program that meets the requirements of the bill. Specifies that the bill must not be read to impose liability upon businesses that do not obtain or maintain practices in compliance with the bill *(Section 2 of the bill)*.	Same as L_132_0943-5 *(Section 2 of the bill).*

Topic	Previous Version (As Introduced)	Sub. Version Adopted by Committee (L_132_0943-5)	Sub. Version (L_132_0943-8)
Technical changes	Defines "individual" as a natural person. Defines "person" as an individual, corporation, business trust, estate, trust, partnership, association, or other legal entity that conducts business in Ohio *(R.C. 1354.01(D) and (F))*.	Eliminates the definition of "individual" and substitutes "natural person" for "individual" in the only provision of the bill that uses that term. Removes the definition of "person" because that term is not used in the bill *(R.C. 1354.01(D) and (F) and 1354.02(B)(3))*.	Same as L_132_0943-5, but substitutes "individual" for "natural person" in the only provision of the bill that uses that term *(R.C. 1354.02(B)(3))*.

S0220-8-132.docx/ec