Eye on the Experts

CYBERSECURITY UPDATE: NYDFS, NAIC, AND WHAT'S GOING ON IN AL, SC, OH, MI, AND MS?

July20, 2019

By *Theodore P. Augustinos and Ben FrazziniKendrick*

The cybersecurity regulation of the New York Department of Financial Services (the "DFS Regulation") took effect recently, requiring subject financial institutions, including insurance companies, ("Covered Entities") to among other things adopt written information security programs to address the protection of nonpublic information and information systems.[1]

The National Association of Insurance Commissioners ("NAIC"), which had separately been preparing a model cybersecurity law, adopted a model law that closely resembled the DFS Regulation. A version of the NAIC model law was first enacted in South Carolina, with Ohio, Michigan, and Mississippi following suit.[2]

Alabama's Governor signed a similar bill;[3] Connecticut recently passed a version of the NAIC model law; and additional bills are pending in New Hampshire and Nevada.[4]

However, none of the laws as enacted were exactly the same as each other, and none precisely followed the NAIC model.

So What's Going On?

In concept, the laws are substantially similar.

Each requires Covered Entities to adopt cybersecurity programs and policies to protect information systems and nonpublic information.

Further, they require each Covered Entity to perform a risk assessment and base its programs and policies thereon, to develop an incident response plan, and to investigate and report data breaches to regulatory authorities in their respective states.

Finally, the laws provide for some limited exemptions from having to comply with their requirements based on compliance with, for example, the Health Insurance Portability and Accountability Act ("HIPAA"), or based on the size of the licensee.

Each law differs in some respects.

For example, the DFS Regulation and NAIC model law differ as to their definitions of what constitutes a cybersecurity event and what triggers a cybersecurity event notification requirement.

Ohio adopted a cybersecurity event definition based on, but slightly different from, the NAIC model law.

Alabama's law, unlike each of the other laws, excludes business information from its definition of nonpublic information that must be protected.

Further, the laws differ as to their deadlines for providing notification of cybersecurity events.

The DFS Regulation and the NAIC model law both require notification within 72 hours. Michigan requires notification within 10 days, and Alabama, Ohio, and Mississippi require notification "as promptly as possible," but no later than three business days.

The laws also differ with respect to the nature and scope of exemptions and particular requirements for written policies. Covered Entities should be attuned to these differences when developing compliance programs.

The following is a summary of some of these differences.

	NY DFS Cybersecurity Regulation	NAIC Model	South Carolina	Ohio	Michigan	Mississippi	Alabama
Cybersecurity Event – Definition	"[A]ny act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System."[5]	"[A]n event resulting in unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System." Excludes any event where the data has been encrypted and the key has not been stolen, as well as events in which the Licensee has determined that the Nonpublic Information accessed has not been used or released and has been returned or destroyed.[6]	Same definition and exclusions as the NAIC model.[7]	"[A]n 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." Same exclusions as NAIC model.[8]	Same definition and exclusions as NAIC model.[9]	Same definition and exclusions as NAIC model.[10]	Similar definition and exclusions as NAIC model, except that the Alabama act does not include business information in its definition of "nonpublic information," which may narrow the scope of incidents constituting cybersecurity events.[11]
Entities subject to the law	"[A]ny entity operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under [New York's] Banking Law, Insurance Law or the Financial Services Law."[12]	Insurance licensees of a state.	Entities licensed under the insurance laws of South Carolina.[13]	Entities licensed under the insurance laws of Ohio.[14]	Entities licensed under the insurance laws of Michigan.[15]	Entities licensed under the insurance laws of Mississippi.[16]	Entities licensed under the insurance laws of Alabama.[17]

	NY DFS Cybersecurity Regulation	NAIC Model	South Carolina	Ohio	Michigan	Mississippi	Alabama
Third Party Service Provider Policy	Each Covered Entity must develop and implement a policy addressing the identification of each third party service provider, an assessment of their risk, due diligence with respect to each third party service provider, minimum cybersecurity practices third party service providers must maintain in order for the covered entity to continue to do business with them, and contractual representations and warranties that the covered entities contracts with third party service providers should contain. [18]	Insurance licensees must provide oversight of third party service provider arrangements including due diligence and requiring third party service providers to implement appropriate technical and physical measures to secure Information Systems and Nonpublic Information. [19]	Same as NAIC model.[20]	Same as NAIC model.[21]	Same as NAIC model.[22]	Same as NAIC model.[23]	Same as NAIC model. [24] Note, however, that the Alabama law contains a different definition of "nonpublic information" from the NAIC model, which may narrow the number of entities that must be addressed in a third party service provider policy.

	NY DFS Cybersecurity Regulation	NAIC Model	South Carolina	Ohio	Michigan	Mississippi	Alabama
Certification	All Covered Entities must certify compliance with the Superintendent of the Department of Financial Services annually and not later than February 15.	Licensees domiciled within a state must provide certification of compliance with risk assessment, cybersecurity program, and third party service provider requirements to the state's insurance commissioner annually by Feb. 15.[25]	Same as NAIC model with respect to insurance licensees domiciled in South Carolina.[26]	Same with respect to insurance licensees domiciled in Ohio. However, also allows insurance companies domiciled and licensed in Ohio to submit a written statement certifying compliance with the requirements of Ohio Stat. § 3965.02 as part of the insurer's corporate governance annual disclosure.[27]	Same as NAIC model with respect to insurance licensees domiciled in Michigan.[28]	Same as NAIC model with respect to insurance licensees domiciled in Mississippi.[29]	Substantially same as NAIC model with respect to insurance licensees domiciled in Alabama.[30]
Breach Notification – Deadline	72 hours from the determination that a cybersecurity event has occurred.[31]	72 hours after determining that a cybersecurity event has occurred.[32]	Same as NAIC Model.[33]	As promptly as possible, but no later than 3 business days after a determination that a cybersecurity event has occurred[34]	"[A]s promptly as possible but not later than 10 days after a determination that a cybersecurity event involving nonpublic information that is in the possession of a licensee has occurred."[35]	Same as Ohio's law.[36]	Same as Ohio's law.[37]

	NY DFS Cybersecurity Regulation	NAIC Model	South Carolina	Ohio	Michigan	Mississippi	Alabama
Breach Notification –Triggering Events	Either of the following: 1. Cybersecurity event impacting covered entity for which notice is required to be provided to any government or regulatory body; 2. Cybersecurity events that have a reasonable likelihood of harming any material part of the normal operations of the covered entity. [38]	When either of the following criteria has been met: 1. The state is the licensee's state of domicile or home state, or 2. The licensee reasonably believes that the nonpublic information involved is of more than 250 or more consumers residing in the state, and either of the following are met: a. The event requires notice to be provided to a government body, self-regulatory agency, or any other body under state or federal law, or b. The event has a reasonable likelihood of materially harming:	Same as NAIC Model. [40]	When either of the following criteria has been met: 1. Both of the following apply: a. Ohio is the licensee's state of domicile or home state, and b. The cyber-security event has a reasonable likelihood of harming a consumer or a material part of the normal operation of the licensee, or 2. The licensee reasonably believes that the nonpublic information involved relates to 250 or more consumers residing in Ohio and the cybersecurity event is either of the following:	When either of the following criteria has been met: 1. Michigan is the licensee's state of domicile or home state, and the cybersecurity event has a reasonable likelihood of materially harming either of the following: a. A consumer residing in Michigan, or b. Any material part of a normal operation of the licensee, or 2. The licensee reasonably believes that the nonpublic information involved is of 250 or more consumers residing in Michigan and is either of the following:	Substantially the same as Michigan's law.[43]	Substantially the same as Ohio's law.[44]

	NY DFS Cybersecurity Regulation	NAIC Model	South Carolina	Ohio	Michigan	Mississippi	Alabama
Breach Notification –Triggering Events (continued)		i. Any consumer residing in the state, or ii. Any material part of the operations of the licensee. [39]		a. A cybersecurity event impacting the licensee of which notice is required to be provided to any government, self-regulatory agency, or any other supervisory body pursuant to any state or federal law, or b. A cybersecurity event that has a reasonable likelihood of materially harming either of the following: i. Any consumer in Ohio, or ii. Any material part of the normal operations of the licensee. [41]	a. A cybersecurity event impacting the licensee of which notice is required to be provided to any agency or body under state or federal law, or b. A cybersecurity event that has a reasonable likelihood of materially harming either of the following: i. Any consumer residing in this state, or ii. Any material part of the normal operation of the licensee. [42]		
Exceptions – Size	Fewer than 10 employees, or with gross annual revenue less than $5 million, or year-end total assets less than $10 million.	Fewer than 10 employees. No revenue or asset threshold.[45]	Same as NAIC model.[46]	Same as NY Regulation. [47]	Fewer than 25 employees. No revenue or asset threshold.[48]	The licensee has fewer than 50 employees, or has less than $5 million in gross annual revenue, or has less than $10 million in year-end total assets, or is an insurance producer or adjuster.[49]	Fewer than 25 employees, less than $5 million in gross annual revenue, or less than $10 million in year-end total assets.[50]

	NY DFS Cybersecurity Regulation	NAIC Model	South Carolina	Ohio	Michigan	Mississippi	Alabama
Exceptions	Covered entities who are subject to the cybersecurity programs of another covered entity are not required to adopt their own cybersecurity programs (e.g., subsidiaries of larger parent companies).[51]	An employee, agent, or designee of a licensee who is also a licensee is exempt from the information security program portions of the Model Act and need not develop its own Information Security program to the extent that it is covered by the information security program of another licensee.[52]	Substantially the same as the NAIC model.[53]	Substantially the same as the NAIC model.[54]	Substantially the same as the NAIC model.[55]	Substantially the same as the NAIC model.[56]	Substantially the same as the NAIC model.[57]
Exceptions –Compliance with HIPAA	The NY DFS regulation does not contain an exemption for entities subject to and in compliance with HIPAA.	A licensee subject to HIPAA that has established and maintains an information security program pursuant to HIPAA will be considered to meet the information security program requirements of the Model Act.[58]	A licensee subject to HIPAA will be considered to meet the requirements of S.C. Code of Laws § 38-99-20.[59]	Substantially the same as the NAIC model.[60]	Substantially the same as the NAIC model.[61]	Substantially the same as the NAIC model.[62]	Substantially the same as the NAIC model.[63]

Notes

[1] See 23 NYCRR Part 500.

[2] Mississippi (Senate Bill No. 2831) approved by Governor Phil Bryant on April 3.

[3] Alabama Senate Bill 54, assigned Act No. 2019-98.

[4] Connecticut's version of the NAIC model law was passed as part of its omnibus budget bill, Public Act 19-117, Section 230. Similar laws are pending in other states, including New Hampshire (Senate Bill 194-FN) and Nevada (Senate Bill 21).

[5] 23 NYCRR 500.01(d) (emphasis added).

[6] Model 668, § 3.D.

[7] S.C. Code of Laws § 38-99-10(3).

[8] Ohio Rev. Code § 3965.01(E) (emphasis added).

[9] Mich. Comp. Laws § 500.553(c).

[10] Miss. SB 2831, § 3(d).

[11] Ala. Act 2019-98, §§ 3(4) and 3(11).

[12] 23 NYCRR 500.01(c).

[13] S.C. Code of Laws § 38-99-10(9)

[14] Ohio Rev. Code § 3965.01(M).

[15] Mich. Comp. Laws § 500.553(g).

[16] Miss. SB 2831, § 3(i).

[17] Ala. Act No. 2019-98, § 3(9).

[18] 23 NYCRR 500.11.

[19] Model 668, § 4(F).

[20] S.C. Code of Laws § 38-99-20(F).

[21] Ohio Rev. Code § 3965.02(F).

[22] Mich. Comp. Laws § 500.555(6).

[23] Miss. SB 2831, § 4(6).

[24] Ala. Act 2019-98, § 4(f).

[25] Model 668, § 4(I).

[26] S.C. Code of Laws § 38-99-20(I).

[27] Ohio Rev. Code § 3965.02(I). Further, the Ohio statute provides that a licensee that meets the risk assessment, cybersecurity program, and other requirements of Ohio Rev. Code 3965.02 "shall be deemed to have implemented a cybersecurity program that reasonably conforms to an industry-recognized cybersecurity framework for the purposes of Chapter 1354 of the Ohio Revised Code."

[28] Mich. Comp. Laws § 500.555(9).

[29] Miss. SB 2831, § 4(9).

[30] Ala. Act 2019-98, § 4(i).

[31] 23 NYCRR 500.17(a).

[32] Model 668, § 6.

[33] S.C. Code of Laws § 38-99-40(A).

[34] Ohio Rev. Code § 3965.04(A).

[35] Mich. Comp. Laws § 500.559(1).

[36] Miss. SB 2831, § 6(1).

[37] Ala. Act 2019-98, § 6(a).

[38] 23 NYCRR 500.17(a).

[39] Model 668, § 6(A).

[40] S.C. Code of Laws § 38-99-40(A).

[41] Ohio Rev. Code § 3965.04(A)(1).

[42] Mich. Comp. Laws §§ 500.559(1)(a) and (b). The Michigan statute also contains a provision regarding the notification of consumers that none of the other statutes contain. See Mich. Comp. Laws § 500.561.

[43] Miss. SB 2831, §§ 6(1)(a) and (b).

[44] Ala. Act 2019-98, § 6(a).

[45] Model Act 668, § 9(A)(1).

[46] S.C. Code of Laws § 38-99-70(A)(1).

[47] Ohio Rev. Code § 3965.07(A).

[48] Mich. Comp. Laws § 500.565(1).

[49] Miss. SB 2831, § 9(1)(a) (emphasis added).

[50] Ala. Act 2019-98, § 9(a)(1).

[51] 23 NYCRR § 500.19(b).

[52] Model Act 668, § 9(A)(3).

[53] S.C. Code of Laws § 38-99-70(A)(2)

[54] Ohio Rev. Code § 3965.07(C).

[55] Mich. Comp. Laws § 500.565(3).

[56] SB 2831, § 9(c)

[57] Ala. Act 2019-98, § 9(3).

[58] Model Act 668, § 9(A)(2).. Licensees must still meet the breach investigation and reporting requirements of the Model Act.

[59] The South Carolina Department of Insurance has clarified that, despite the circular and unclear language of the statute, it interprets this provision of the statute to provide licensees subject to HIPAA with an exemption from complying with the information security provisions of §§ 38-99-20(A) through (H), but not the notification provisions of 38-99-20(I), or the cybersecurity event investigation and reporting requirements of §§ 38-99-30 and 38-99-40.

[60] Ohio Rev. Code § 3965.07(B).

[61] Mich. Comp. Laws § 500.565(2).

[62] SB 2831, Section 9(1)(b). The Mississippi proposed law also contains an exemption for a licensee affiliated with a depository institution that maintains an information security program in compliance with interagency guidelines promulgated under the Gramm-Leach-Bliley Act. SB 2831, Section 9(1)(d). Such exemption does not appear in the NAIC model law or similar laws adopted by other states.

[63] Ala. Act. 2019-98, § 9(2).

About the Authors

Theodore P. Augustinos is a partner at **Locke Lord LLP** advising clients in various industries on privacy and data protection, cybersecurity compliance and incident preparedness, and breach response. He may be contacted at ted.augustinos@lockelord.com.

Ben FrazziniKendrick is an associate at **Locke Lord LLP** and a member of the firm's Privacy & Cybersecurity Practice Group advising clients in various industries, including financial services, healthcare and education, with respect to their obligations under various privacy and data protection requirements. He may be contacted at benjamin.frazzinikendrick@lockelord.com.

NOTE: The content posted to this account from ***The Insurance Coverage Law Center*** is current to the date of its initial publication. There may have been further developments of the issues discussed since the original publication.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting or other professional service. If legal advice is required, the services of a competent professional person should be sought.