MCINTYRE | LEMON

What Small and Bank-Affiliated Insurance Entities Need to Know About State Exemptions from Insurance Data Security Laws

Chrys Lemon, Arshawn Teymoorian, and Jeff Klein

October 10, 2020

On October 24, 2017, the National Association of Insurance Commissioners ("NAIC")[1] adopted Model Law No. 668, the Insurance Data Security Model Law (the "Model Law").[2]

Generally speaking, the Model Law requires entities regulated by state insurance departments to develop and implement an Information Security Program ("ISP") to protect against cybersecurity breaches, to investigate cybersecurity events, and to notify the appropriate state insurance regulator(s) of such events when they occur. Like other Model Laws the NAIC has adopted, such as the Producer Licensing Model Act, the NAIC hoped that the Model Law would prevent a patchwork of state insurance data security laws and provide a uniform state approach to data security regulation that would reduce compliance costs for regulated entities.

While the NAIC's efforts with respect to state uniformity have been largely successfully to date, as additional states adopt or consider adopting the Model Law, key differences in state approaches to insurance data security regulation are beginning to emerge, especially with respect to the regulation of small and bank-affiliated insurance entities.

This article provides a brief background on the NAIC Model Law and the current status of state adoption. It then analyzes the emerging differences with respect to how these states are choosing to regulate small and bank-affiliated insurance entities.

Who Must Comply?

Generally speaking, the Model Law applies to *licensees*, which is broadly defined as any entity required to be licensed by a state insurance department, including insurance companies, insurance agencies and agents, managing general agents, and third-party administrators, but not purchasing groups or risk retention groups licensed in another state.[3]

What Does Compliance Require?

The NAIC's Model Law has *three* primary requirements. First, it requires licensees to develop and implement an ISP that is conducive to the quantity and sensitivity of nonpublic information used or in possession of the licensee. To accomplish this, licensees are in turn required to first conduct a risk assessment. The ISP developed in response to a licensee's risk assessment must contain "administrative, technical, and physical safeguards for the protection of Nonpublic Information and the Licensee's Information System." [4]

Second, licensees are required to investigate *cybersecurity events*.[5] This generally requires a licensee to determine whether a cybersecurity event has occurred, assess its nature and scope, identify any nonpublic information that may have been involved in the event, and take reasonable measures to restore the security of the compromised information systems to prevent further unauthorizes access. [6]

Finally, as promptly as possible but not later than 72 hours from determining a cybersecurity event has occurred, licensees must notify the insurance commissioner of the domicile or home state of the licensee. Licensee must also notify the insurance commissioners of any other state where the licensee reasonably believes that the nonpublic information involved is of 250 or more consumers residing in the state if (1) such notification is required by federal or state laws that require disclosure of the incident or (2) the event has a reasonable likelihood of materially harming any consumer in the state or the normal operations of the licensee. [7] When notifying an insurance commissioner of a cybersecurity event, licensees are required to provide as much information as possible, including but not limited to, the date of the event, how it was discovered, and a description of the efforts being undertaken to remediate the situation. Licensees are also under a continuing obligation to update and supplement initial and subsequent notifications to the appropriate insurance regulators.

What is the Status of State Adoption?

Since 2017, eleven states have adopted the NAIC's Model Law including Alabama,[8] Connecticut,[9] Delaware,[10] Indiana,[11] Louisiana,[12] Michigan,[13] Mississippi,[14] New Hampshire,[15] Ohio,[16] South Carolina,[17] and Virginia.[18] The States that have adopted the Model Law have generally done so almost verbatim. For example, all eleven States that have adopted the Model Law have also adopted its primary provisions, including the requirement to develop and implement an ISP, to investigate cybersecurity events, and to notify the relevant state insurance regulator(s) about a cybersecurity event. However, as described further below, significant variation is beginning to emerge among states with respect to the scope of their exemption provisions.

Are Small and Bank-Affiliated Insurance Entities Exempt?

While all states generally require licensees to investigate cybersecurity events and notify the appropriate state insurance regulator(s), some states have offered a partial exemption for small and bank-affiliated insurance entities from the more burdensome requirement to develop and implement an ISP. For example, the Model Law, and numerous states that have adopted it, exempts licensees "with fewer than ten employees, including any independent contractors" from the requirement to develop and implement an ISP.[19] Moreover, while not included in the Model Law, a smaller number of States, such as Virginia, have also exempted from the ISP requirement, licensees that are "affiliated with a depository institution that maintains an information security program in compliance with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information" under the Gramm-Leach-Bliley Act.[20] However, while some states have opted to grant preferential treatment to small and bank-affiliated entities through partial exemptions from their insurance data security laws, others have not.

For example, South Carolina exempts licensees with fewer than ten employees, and Michigan exempts licensees with fewer than 25 employees, from the requirement to develop and implement an ISP, but Virginia does not provide any exemption for small entities. The result of these state divergences is that a licensee with 20 employees would be exempt in Michigan, but not in South Carolina or Virginia. Equally important, if a licensee's operations grow and it ceases to qualify for the small-entity exemption, states generally only grant 180 days for the licensee to comply with the state's requirements to develop and implement an ISP.

Where are States Today Regarding Partial Exemptions?

The following table provides a summary of which states currently exempt small or bank-affiliated entities from the requirements to develop and implement an ISP.[21]

State	Are Small Entities Partially Exempt?	Are Bank-Affiliated Entities Partially Exempt?
Alabama	Yes, < 25 employees.[22]	Yes.[23]
Connecticut	Yes, < 10 employees, including independent contractors.[24]	No.[25]
Delaware	Yes, < 15 employees.[26]	No.[27]
Indiana	Yes, < 50 employees, excluding independent contractors.[28]	Yes.[29]
Louisiana	Yes, < 25 employees.[30]	Yes.[31]
Michigan	Yes, < 25 employees, including independent contractors.[32]	No.[33]
Mississippi	Yes, < 50 employees, excluding independent contractors.[34]	Yes.[35]
New Hampshire	Yes, < 20 employees.[36]	Yes.[37]
Ohia	Yes, < 20 employees.[38]	No.[39]
South Carolina	Yes, < 10 employees, including independent contractors.[40]	No.[41]
Virginia	No.[42]	Yes.[43]

Looking Forward

The end result of this patchwork of state laws is that small and bank-affiliated insurance entities will likely be required to develop an ISP eventually, even if they are currently exempt in the states in which they operate. Indeed, the Model Law is currently also under consideration in Illinois (HB 5397), Maine (LD 1995), Minnesota (SF 4269), Oklahoma (SB 1919), Rhode Island (S 2618), and Wisconsin (AB 819).

Notably, while current drafts of all of the legislation put forth in these States provide some form of exemption for small entities, none of them exempt bank-affiliated insurance entities from the requirement to develop and implement an ISP. Small and bank-affiliated insurance entities must carefully review the laws of the states they are operating in not only to ensure they are currently exempt from the requirement to develop and implement an ISP, but that they remain exempt as their businesses grow.

McIntyre & Lemon, PLLC will continue to monitor these issues.

[1] The NAIC is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia, and the U.S. territories.

[2] NAIC, Insurance Data Security Model Law No.668 (2017).

[3] Id. § 3(I).

[4] Id. § 4(A).

[5] The NAIC Model Law defines a cybersecurity event as an "event resulting in unauthorized access to, disruption or misuse of, an Information System or information store on such Information System." Id. § (3)(D).

[6] Id. § 5(B)(1-4).

[7] Id. § 6(A)(1)-(2).

[8] Ala. Code §§ 27-62-1-1.

[9] Conn. Gen. Stat. §§ 38a-38(a)-(i).

[10] Del. Code Ann. tit. 18, §§ 8601-8611.

[11] Ind. Code Ann. §§ 27-2-27-1; -32.

[12] La. R.S. §§ 22:2501-2511

[13] MCLS §§ 500.550-565.

[14] Miss. Code Ann. §§ 83-5-801-825.

[15] N.H. RSA §§ 420-P:1-P:14.

[16] Ohio Rev. Code Ann. §§ 3965.01-11.

[17] S.C. Code Ann. §§ 38-99-10 - 38-99-100.

[18] Va. Code Ann. §§ 38.2-621; - 629.

[19] NAIC, Insurance Data Security Model Law No.668 at § 9(A)(1).

[20] Va. Code Ann. § 38.2-629

[21] Notably, a number of these states, like Mississippi, also provide exemptions for entities that are below certain annual revenue or asset thresholds. See Miss. Code Ann. § 83-5-817(1)(a).

[22] Ala. Code § 27-62-9(a)(1).

[23] Id. § 27-62-9(a)(4).

[24] Conn. Gen. Stat. § 38a-38(c)(10)(A)(i)(II).

[25] Id. § 38a-38(c)(10)(A).

[26] Del. Code Ann. tit. 18, § 8609(a)(1).

[27] Id. § 8609(a).

[28] Burns Ind. Code Ann. § 27-2-27-26(a).

[29] Id. § 27-2-27-26(b)(2).

[30] La. R.S. § 22:2509(A)(1).

[31] Id. § 22:2509(A)(6).

[32] MCLS § 500.565(1).

[33] Id. § 500.565(1)-(4).

[34] Miss. Code Ann. § 83-5-817(1)(a).

[35] Id. § 83-5-817(1)(d).

[36] N.H. RSA § 420-P:9(I)(a).

[37] Id. § 420-P:9(I)(e).

[38] Ohio Rev. Code Ann. § 3965.07(A).

[39] Id. § 3965.07(A)-(C).

[40] S.C. Code Ann. § 38-99-70(A)(1).

[40] Id. § 38-99-70(A)(1)-(3).

[42] Va. Code Ann. § 38.2-629(A)(1)-(3).

[43] Id. § 38.2-629(A)(3).

MCINTYRE | LEMON

Chrys D. Lemon

PARTNER

2202-659-3902

202-296-4202

cdl@mcintyrelf.com

Arshawn Teymoorian

OF COUNSEL

202-659-3906

202-296-4202

ateymoorian@mcintyrelf.com

Jeffrey M. Klein

OF COUNSEL

202-659-5760

202-296-4202

jklein@mcintyrelf.com