ACCEL LAW GROUP

WHITE PAPER

The Developing Landscape of Cybersecurity Regulations:

Clarifying the Cybersecurity Requirements for Insurance Intermediaries

BACKGROUND

As more states begin to adopt comprehensive cybersecurity regulations, insurance agencies and producers must determine their cybersecurity compliance obligations among varying standards and requirements. The first cybersecurity regulation of private sector entities was adopted in 2017 by the New York Department of Financial Services ("NYDFS"), and soon after the National Association of Insurance Commissioners ("NAIC") adopted the Insurance Data Security Model Law 668 ("Model Law").

Since 2017, several states have adopted the Model Law, or a variation thereof, while New York has adopted its own extensive set of requirements. New York's Cybersecurity Regulation, 23 NYCRR §500 ("New York's Cybersecurity Regulation" or "Part 500") requires all "Covered Entities," to submit a certification of material compliance with all/or certain parts of New York's Cybersecurity Regulation. Contrast this with the Model Law which requires only "insurers" to submit a certification of material compliance, but nevertheless requires "licensees" to comply with certain other cybersecurity requirements.

With New York imposing the most demanding cybersecurity standards, and other states deferring to New York's Cybersecurity Regulation, where does this leave insurance intermediaries and their cybersecurity programs? This White Paper outlines certain cybersecurity and filing requirements under New York's Cybersecurity Regulation and those states that have adopted the Model Law, or a variation thereof.

IMPORTANT DEFINITIONS

Covered Entity

Under the New York Cybersecurity Regulation, "Covered Entity" is defined as "any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law."[1]

Licensee

Under the Model Law, "Licensee" is defined as "any Person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State but shall not include a purchasing group or a risk retention group chartered and licensed in a state other than this State or a licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction."[2]

CYBERSECURITY REGULATIONS BY STATE

New York's Cybersecurity Regulation

As mentioned above, the New York Cybersecurity Regulation applies to Covered Entities, which includes insurance intermediaries licensed in New York. The regulation entails an extensive list of requirements including, but not limited to, the following: implementing and maintaining a cybersecurity policy, developing and implementing written policies and procedures for vulnerability management, conducting periodic risk assessments, and maintaining audit trails, to name a few.[3]

New York recently amended this regulation with the intent of tailoring the cybersecurity requirements based on the size and type of entity that is operating under the Banking Law, the Insurance Law, or the Financial Services Law. The size and type of entity are key factors in determining whether the Covered Entity must comply with all or certain parts of New York's Cybersecurity Regulation. A Covered Entity's classification is directly related to the requirement under 23 NYCRR §500.17 (b) to annually certify compliance with all or certain parts of the regulation.

(a) Certification of Material Compliance

The ***Certification of Material Compliance*** under New York's Cybersecurity Regulation requires a Covered Entity to certify to the NYDFS that they are in compliance with all or certain parts of the regulation during the prior calendar year (Certification of Material Compliance)[4]. The Certification of Material Compliance is due annually by April 15 and must be based on data

and documentation sufficient to accurately determine and demonstrate such material compliance. However, if a Covered Entity is not in material compliance with New York's Cybersecurity Regulation, it is required to submit a Written Acknowledgement of Noncompliance.[5]

For more information on submitting a compliance filing see NYDFS Cybersecurity Resource Center.[6]

(b) Full and Limited Exemptions

Full Exemptions

Based on a Covered Entity's size and entity classification, a Covered Entity may be subject to (a) a limited exemption or (b) a full exemption from compliance with the regulation. A Covered Entity may claim a full exemption if they fall under one of the following categories: (a) employees, agents, or wholly owned subsidiaries of another DFS-regulated business if they are fully covered by the Cybersecurity Program of another DFS-regulated business; (b) inactive individual insurance brokers; or (c) a charitable annuity society, or risk retention group not chartered in NY.[7]

If a Covered Entity determines it qualifies for a full exemption, then a Notice of Exemption[8] must be submitted to the NY Department of Financial Services. Once a Notice of Exemption is filed it remains valid until terminated. However, a Covered Entity should be mindful to re-evaluate its exemption status annually.

Limited Exemptions

If a Covered Entity does not qualify for a full exemption, it may qualify for a limited exemption. A Covered Entity may claim a limited exemption if it falls under one of the following categories: (a) a small business; (b) a Covered Entity that does not directly or indirectly control, own, access, maintain or utilize any Information Systems and nonpublic information; or (c) a captive insurance company that does not directly or indirectly control, own, or access nonpublic information.[9]

If the Covered Entity qualifies for a limited exemption, then the Covered Entity is required to submit (1) a Notice of Exemption and (2) a Certification of Material Compliance (certifying compliance to the applicable sections based on its exempt status) with the NYDFS.

Insurance intermediaries should reference the New York Cybersecurity Regulation for specific exemption requirements or seek advice from counsel to determine their exemption status.

NAIC Insurance Data Model Law

The NAIC's Model Law is largely based on the New York Cybersecurity Regulation. The Model Law generally requires "insurers and other entities licensed by the department of insurance to develop, implement, and maintain information security program, investigate any cybersecurity events and notify the state insurance commissioner of such events."[10]

In addition to maintaining an information security program, the Model Law requires insurers to submit an annual certification of compliance with the requirements set forth in the Model Law. The Model Law distinguishes "insurers" from "licensees" making it clear that only "insurers" are subject to the certification requirements. Thus, insurance intermediaries are not subject to this requirement. However, insurance intermediaries should remain aware that they are considered "licensees" and therefore subject to certain other cybersecurity requirements under the Model Law.

As of January 5, 2024, 23 states have adopted the Model Law[11] and 4 states have pending legislation to adopt the Model Law.[12] Although a majority of the states have chosen to adopt the Model Law, or a variation thereof, insurance intermediaries should continue to monitor the states in which they are licensed or desire to be licensed in the event that states enact cybersecurity standards similar to that of New York (i.e., certification of compliance for insurance intermediaries or stricter security protocols).

(a) Vermont and New Hampshire

Although New Hampshire and Vermont have adopted the Model Law, they each provide a safe harbor for New York regulatory compliance. Both states provide that a "licensee" in compliance with the New York Cybersecurity Regulation is in compliance with New Hampshire's and Vermont's cybersecurity requirements provided that the licensee submits a written statement to the commissioner certifying compliance.[13] This standard demonstrates deference to New York's higher standard and thus, insurance intermediaries should consider this when developing and implementing their cybersecurity programs.

CONCLUSION

Overall, as insurance intermediaries review or implement their cybersecurity programs, they should remain aware of New York's higher standard imposed on insurance intermediaries as compared to states that have adopted the Model Law. Under the current cybersecurity landscape, compliance with the New York standard satisfies the Model Law standard and the current standards adopted by the other states. However, there is always the possibility that

states will adopt new or different standards that must be followed. As such, insurance intermediaries should seek further legal advice to determine the most appropriate path for compliance and to determine how varying state regulations apply.

ABOUT ACCEL Compliance

ACCEL Compliance provides comprehensive compliance services and software to insurance agents and brokers. We focus on ensuring insurance intermediaries meet their regulatory obligations while freeing their resources to focus on growth. Learn more at ACCELCompliance.com.

ABOUT ACCEL Law Group

ACCEL Law Group specializes in advising insurance agents and brokers on complex mergers, acquisitions and regulatory matters. Learn more at ACCELLawGroup.com.

NOTES

1 See 23 NYCRR §500.1(c).

2 See Insurance Data Security Model Law 668.

3 See 23 NYCRR §500.3, §500.5, §500.6 & §500.9.

4 See Instructions on How to File a Certification of Material Compliance for Entities & Instructions on How to File Certification of Material Compliance for Individual Licensees.

5 See Instructions on How to File Acknowledgement of Noncompliance for Entities & How to File to Acknowledgement of Noncompliance for Individual Licensees.

6 See NYDFS Cybersecurity Resource Center ("Submit a Compliance Filing").

7 See 23 NYCRR §500.19(b), (e), & (g).

8 See instructions How to File a Notice of Exemption.

9 See 23 NYCRR §500.19(a), (c), & (d).

10 See NAIC State Legislative Brief: The NAIC Insurance Data Security Model Law (January 2024).

11 According to the NAIC State Legislative Brief the following states have adopted the Model Law: Alabama, Connecticut, Delaware, Hawaii, Illinois, Indiana, Iowa, Kentucky, Louisiana, Maine, Maryland, Michigan, Minnesota, Mississippi, New Hampshire, North Dakota, Ohio, Pennsylvania, South Carolina, Tennessee, Vermont, Virginia, and Wisconsin.

12 According to the NAIC State Legislative Brief the following states have pending legislation: Alaska, Nebraska, New Jersey, and Oklahoma.

13 See NH RSA 420-P:11; Vt. Stat. Ann. tit. 8 § 4728(b)(4).