Cybersecurity in the Insurance Industry:

Navigating the Patchwork of U.S. Data Breach Notification Requirements



By Fred E. Karlinsky, Timothy F. Stanfield, and Christian Brito

In recent years, there have been several major data breaches involving large companies that have exposed and compromised the sensitive personal information of millions of individuals across the United States. Despite record-shattering data breaches, the United States has yet to develop a uniform and comprehensive regulatory scheme for regulating how companies store and protect the personal, nonpublic information of their customers and employees. Instead, cybersecurity regulation is left primarily to individual states, which has led to the creation of a patchwork of varying, and sometimes inconsistent, data protection requirements.

California enacted the first data-breach notification law in 2003. Since then, all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted data breach laws that require individuals to be notified if their information is compromised. These laws have different and sometimes incompatible provisions regarding what categories and types of personal information warrant protection, which entities are covered, and what constitutes a breach. Notification requirements also vary greatly among states.

Navigating this patchwork of requirements can be challenging for companies that operate across state lines; this is especially true for multi-state insurance companies and agencies, which are not only subject to state-wide cybersecurity and consumer protection laws, but are increasingly being required to comply with new and evolving cybersecurity requirements that apply specifically to insurance industry participants. Indeed, legislatures and insurance regulators across the country have taken note of high-profile breaches involving U.S. insurers, and have made cybersecurity and consumer data protection a top priority. As a result, the insurance industry is subject to some of the most recent and comprehensive data protection laws and regulations in the United States.

This article focuses on two key data breach notification requirements applicable to insurance companies and agencies: The New York Department of Financial Services (NYDFS) Cybersecurity Regulation (the NYDFS Regulation) and the National Association of Insurance Commissioners (NAIC) Data Security Model Law (the NAIC Model). This article does not address laws or regulations that require notice to individuals whose personal information has been compromised as a result of a breach. For the most part, individual data security breach notification obligations are tied to the state of residency of the individual whose information is potentially affected, so even though an insurer may only be licensed in certain jurisdictions, notification obligations to any potentially affected individuals are triggered by the individuals' respective state residencies.

Despite record-shattering data breaches, the United States has yet to develop a uniform and comprehensive regulatory scheme for regulating how companies store and protect the personal, nonpublic information of their customers and employees.

New York DFS Cybersecurity Regulation

The New York Department of Financial Services' landmark cybersecurity regulation for insurance companies and financial institutions became effective March 1, 2017, with a two-year implementation period. The NY Regulation requires insurance companies, producers, banks and other financial services companies regulated by the NYDFS (i.e., Covered Entities) to adhere to strict standards to protect consumer data. The rule implements a host of requirements, including requiring that covered entities

This article first appeared in the Spring 2021 issue of *The Demotech Difference*, a publication of Demotech, Inc., www.demotech.com.
To obtain your own copy contact BAlbert@demotech.com.

establish a cybersecurity policy and perform an annual risk assessment to evaluate their cybersecurity policies.

Although planning for cybersecurity breaches is implicit in the requirements, there is a specific requirement for covered entities to prepare incident response plans. These written plans must be prepared in advance based on the risk assessment, and should describe the procedures personnel will follow, and their roles and responsibility to remediate or mitigate the harm caused. Notably, the NY Regulation requires that covered entities provide notice to the superintendent of the NY DFS as promptly as possible, but in no event later than 72 hours from making a determination that a cybersecurity event has occurred; however, it is important to note that this is not a blanket requirement to report every breach. Rather, if a covered entity is required to report the breach to another government agency or supervisory body, such as a state attorney general's office or another insurance department, then notice must also be provided to the superintendent. Covered entities must also report any breaches that "have a reasonable likelihood of materially harming any material part of the normal operation(s)" of a covered entity.

The determination of whether a breach has triggered the reporting requirement under the NY Regulation is a fact-specific exercise that must be made on a case-by-case basis; however, covered entities should keep in mind that it is the NYDFS' interpretation of the reporting requirements, as applied to any particular set of circumstances, that will carry the day. Accordingly, it is important for entities to stay abreast of interpretive guidance published by the NYDFS which can be helpful in understanding how the regulator interprets the requirements. Indeed, the NYDFS has an extensive section on its website that is dedicated exclusively to the NY Regulation, pursuant to which it has indicated that the "notice requirement is intended to facilitate information sharing about serious events that threaten an institution's integrity and that may be relevant to the Department's overall supervision of the financial services industries." The guidance further indicates that the NYDFS "trusts that Covered Entities will exercise appropriate judgment" in determining which attacks must be reported "and does not intend to penalize Covered Entities for the exercise of honest, good faith judgment." As such, good regulatory hygiene requires that covered entities which have been subject to a data breach conduct a thorough investigation of the circumstances leading up to the event and give due consideration to the notification requirement. Where the line blurs and a covered entity is on the fence regarding whether to report, the prudent approach in most cases will be to report the incident.

fizkes/shutterstock.com

NAIC Insurance Data Security Model Law

The NAIC Model was adopted by the NAIC in October 2017 following extensive deliberations and input from state insurance regulators, consumer representatives and the insurance industry. State adoption of the model by state legislatures is critical for state insurance regulators to have the tools they need to better protect sensitive consumer information.

The NY Regulation had a significant impact on the development of the NAIC Model. The model requires insurers and other entities licensed by a state department of insurance to develop, implement, and maintain an Information Security Program (ISP). Importantly, the NAIC Model requires that licensees investigate cybersecurity events and notify the insurance commissioner of cybersecurity events that satisfy certain criteria. The model defines "cybersecurity event" as an event resulting in unauthorized access to, disruption or misuse of, an information system or information stored on such an information system.

Specifically, the NAIC Model requires that all domestic insurers and all home state producers notify the insurance commissioner as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred. This 72-hour notice requirement may also apply to non-domestic (i.e., foreign) insurers and producers if the breach involves the nonpublic information of 250 or more consumers residing in the state and if either of the following is true:

- The insurer or producer is required to provide notice of the breach to any government body, self-regulatory agency or any other supervisory body pursuant to any state or federal law; or

- The breach has a reasonable likelihood of materially harming: (i) any consumer residing in the state; or (ii) any material part of the normal operation(s) of the insurer or producer.

Thus, insurers and producers that are domiciled in states that have adopted the NAIC Model without modification are required to notify the insurance commissioner within 72 hours of determining that a threat actor has gained

access to, disrupted, or misused their information systems. Moreover, nondomestic insurers and producers may also have reporting obligations if the breach has resulted in the access or misuse of the nonpublic information of 250 or more of the state's consumers and one of the above two conditions has been satisfied. Regarding the condition identified in the first bullet above, it is important to remember that the condition is satisfied if the insurer or producer is required to provide notice to any state government body, self-regulatory agency or any other supervisory body pursuant to any state or federal law (i.e., it is not limited to circumstances where the insurer or producer is required to provide notice to another insurance commissioner).

As of the drafting of this article, Alabama, Connecticut, Delaware, Indiana, Louisiana, Michigan, Mississippi, New Hampshire, Ohio, South Carolina and Virginia have adopted the NAIC Model. While most states that have adopted the model included the breach notification requirements with little or no substantive changes, Virginia's version of the NAIC Model includes a more expansive notification requirement for non-domestic insurers and producers. Insurers and producers should be mindful that there may be additional data breach laws in any given state that should be considered. Specifically, notice of a breach is required to the Virginia Commissioner of Insurance within three business days if:

- The licensee reasonably believes that the nonpublic information involved is of 250 or more consumers residing in the Commonwealth or the licensee is required under federal law or the laws of another state to provide notice of the cybersecurity event to any government body, self-regulatory agency or other supervisory body.

Accordingly, if the breach does not involve the nonpublic information of at least 250 Virginia consumers, non-domestic insurers and producers may nonetheless be required to provide notice to the Virginia Commissioner of Insurance if it is determined that the licensee is required to provide notice to another government body, self-regulatory agency or other supervisory body under federal or state law. Thus, a company may be required to report a breach even if the breach did not affect a single Virginia consumer.

Conclusion

One of the primary goals of the NAIC Model is to bring much-needed uniformity to the regulation of cybersecurity for the U.S. insurance industry, but whether the majority of U.S. jurisdictions will enact the NAIC Model remains unclear. Barring universal adoption of the NAIC Model, which is unlikely unless it becomes an accreditation standard, or action at the federal level, insurance companies and other licensees will continue to closely monitor developments at the state level and implement protocols to ensure that their cybersecurity response plans comply with the laws of each state in which they transact insurance.

In developing cybersecurity breach response plans, companies must consider a wide-range of information, including the kinds of information that are protected by individual state breach laws, the conditions that trigger breach notification requirements, and the timeframes within which breach notifications must be made. It is imperative that companies understand their reporting obligations, and have a streamlined incident response plan in place that has been tested via tabletop exercises to ensure they are prepared to handle a cybersecurity event.

Insurance company boards must also be involved in their companies' cybersecurity activities and must go beyond merely "check-the-box" compliance. During the last few years, cybersecurity risk has quickly morphed into enterprise risk, which creates the need for a whole-company approach. This means that cybersecurity is not just a problem for the company's IT department — today, it is everyone's problem, especially the board's.

Greenberg Traurig Shareholder Fred E. Karlinsky is co-chair of the firm's Insurance Regulatory and Transactions Practice Group. Fred has nearly 30 years of experience representing the interests of insurers, reinsurers and a wide variety of other insurance-related entities on their regulatory, transactional, corporate and governmental affairs matters. Fred is a recognized authority on national insurance regulatory and compliance issues and has taken a leadership position in many insurance trade organizations, has led many industry-driven legislative and regulatory initiatives, and is a sought-after thought leader who has spoken and presented to insurance executives and governmental officials, both nationally and internationally.

Timothy F. Stanfield is of counsel at Greenberg Traurig. Timothy is a member of the firm's Florida Government Law & Policy Practice and represents a broad array of private and public-sector clients before the Florida legislature, cabinet, and state agencies.

Christian Brito is an associate at Greenberg Traurig. Christian focuses his practice on national insurance transactional, regulatory and compliance matters. Christian represents a wide variety of insurance industry participants, including insurers, reinsurers, captives, managing general agencies, brokers, third-party administrators, claims administrators and others in connection with regulatory, transactional, corporate and governmental affairs matters.