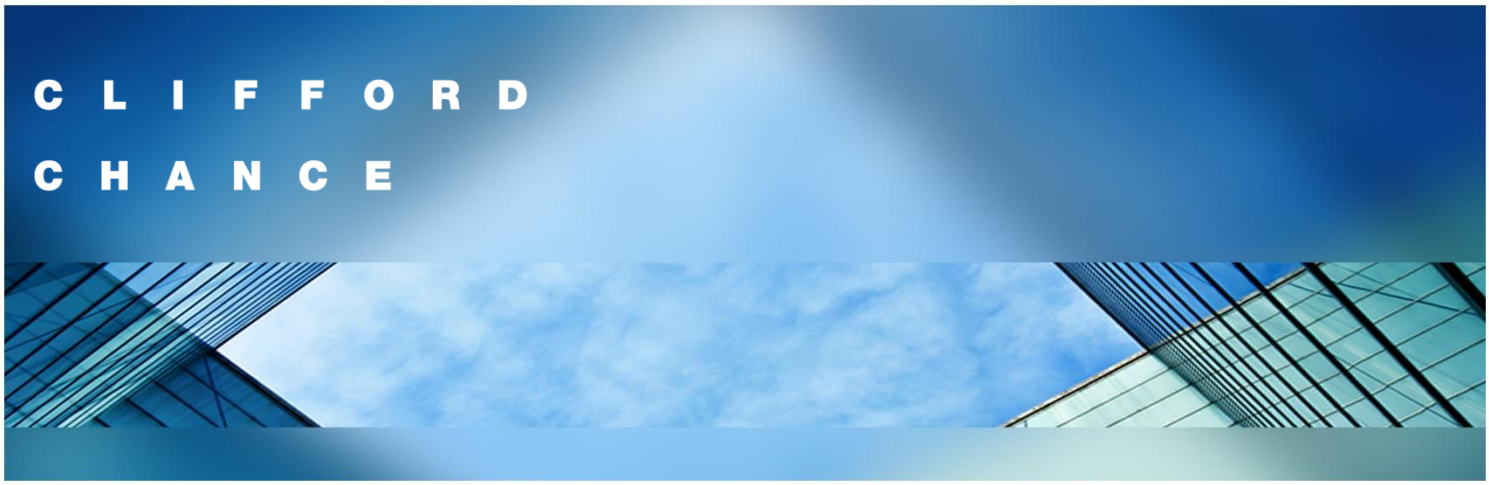

NAIC ADOPTS MODEL CYBERSECURITY LAW

The Cybersecurity (EX) Working Group and the Innovation and Technology (EX) Task Force of the National Association of Insurance Commissioners ("**NAIC**"), at the NAIC Summer 2017 National Meeting in Philadelphia, approved the Insurance Data Security Model Law (the "**Model Law**"). This is a significant step in cybersecurity regulation. The Model Law closely parallels the comprehensive and first-in-the-nation New York Department of Financial Services ("**DFS**") Cybersecurity Requirements for Financial Services Companies regulation that took effect on March 1, 2017 (the "**NYDFS Cybersecurity Regulation**"). The Model Law will now be considered by the NAIC Executive Committee and, if approved, will be presented to the Joint Meeting of the Executive Committee and Plenary for final approval. Capitalized terms used and not defined herein have the meanings set forth in the Model Law.

The Model Law is a noteworthy development because, first, it follows the comprehensive and prescriptive approach of the NYDFS Cybersecurity Regulation and, second, it will likely be adopted in some form in most states, which signals a national approach to cybersecurity for the insurance industry.

This is a significant step in cybersecurity regulation. The Model Law closely parallels the comprehensive and first-in-the-nation New York Department of Financial Services Cybersecurity Requirements for Financial Services Companies regulation that took effect on March 1, 2017. The Model Law is a noteworthy development because, first, it follows the comprehensive and prescriptive approach of the New York cybersecurity regulation and, second, it will likely be adopted in some form in most states, which signals a national approach to cybersecurity for the insurance industry.

KEY REQUIREMENTS OF THE MODEL LAW AND THE NYDFS CYBERSECURITY REGULATION

The Model Law substantially follows the DFS' approach of requiring a security program based on a risk-assessment appropriate to the size and complexity of the insurance company. In addition, in both the Model Law and the NYDFS Cybersecurity Regulation, responsibility for an adequate cybersecurity program resides with the company's board. At the NAIC Summer 2017 National Meeting, the NAIC assured attendees that any insurer in compliance with the NYDFS Cybersecurity Regulation will be in compliance with the Model Law.

Key Requirements under the Model Law

The Cybersecurity (EX) Working Group of the NAIC has been working towards adopting a model cybersecurity law since the spring of 2016. The current version contains the following key provisions:

- The Model Law, as adopted, will apply to all "Licensees," defined as "any Person licensed, authorized to operate, or registered, or required to be

licensed, authorized, or registered pursuant to [the insurance laws of the state enacting the Model Law] but shall not include a purchasing group or a risk retention group chartered and licensed in a state other than [the state enacting the Model Law] or a Licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction."

- A "Cybersecurity Event" is defined as "an event resulting in unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System." The term "Cybersecurity Event" does not include "the unauthorized acquisition of Encrypted Nonpublic Information if the encryption, process or key is not also acquired, released or used without authorization" or "an event with regard to which the Licensee has determined that the Nonpublic Information accessed by an unauthorized person has not been used or released and has been returned or destroyed."
- Under the Model Law, commensurate with the size and complexity of the Licensee, the nature and scope of the Licensee's activities, including the Licensee's use of third parties to maintain, process, store or otherwise have access to Nonpublic Information through such third party's provision of services to the Licensee ("**Third-Party Service Providers**"), and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody or control, each Licensee is required to develop, implement, and maintain a comprehensive written Information Security Program based on the Licensee's Risk Assessment and that contains administrative, technical, and physical safeguards for the protection of Nonpublic Information and the Licensee's Information System.
- The Licensee is required to perform a Risk Assessment as set forth in the Model Law and, based on its Risk Assessment, the Licensee must (1) design its Information Security Program to mitigate the identified risks, commensurate with the size and complexity of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody or control, and (2) determine which of several security measures listed in the Model Law are appropriate to implement.
- The Model Law further provides for oversight by the Licensee's Board of Directors or an appropriate committee thereof.
- Licensees are required to exercise due diligence in selecting Third-Party Service Providers. In addition, Licensees must require Third-Party Service Providers to implement appropriate administrative, technical, and physical measures to protect and secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider.
- As part of its Information Security Program, each Licensee is required to establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event that compromises the confidentiality, integrity or availability of Nonpublic Information in the

Licensee's possession, the Licensee's Information Systems, or the continuing functionality of any aspect of the Licensee's business or operations.

- Annually, each insurer domiciled in the state enacting the Model Law must submit to the chief insurance regulatory official of the state enacting the Model Law (the "**Commissioner**") a written statement by February 15, certifying that the insurer is in compliance with the Information Security Program requirements set forth in the Model Law. Insurers are further required to maintain for examination by the applicable insurance regulatory body all records, schedules and data supporting the certification for a period of five years. To the extent an insurer has identified areas, systems or processes that require material improvement, updating or redesign, the insurer is required to document the identification and the remedial efforts planned and underway to address such areas, systems or processes.
- Each Licensee is required to conduct an investigation if the Licensee learns that a Cybersecurity Event has or may have occurred. Each Licensee must notify the Commissioner as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred when either of the following criteria has been met: (1) the state enacting the Model Law is the Licensee's state of domicile, in the case of an insurer, or the state enacting the Model Law is the Licensee's home state, in the case of a producer; or (2) the Licensee reasonably believes that the Nonpublic Information involved is of 250 or more Consumers residing in the state enacting the Model Law and that is either of the following: (a) a Cybersecurity Event impacting the Licensee of which notice is required to be provided to any government body, 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: (i) any Consumer residing in the state enacting the Model Law; or (ii) any material part of the normal operation(s) of the Licensee.
- The Model Law dictates notice procedures relating to Cybersecurity Events (1) affecting systems maintained by Third-Party Service Providers; (2) affecting reinsurers; and (3) required to be reported to producers of record.
- The Commissioner has enforcement powers under the Model Law. Additionally, the Model Law includes confidentiality protections to protect certain information that is provided to an insurance regulatory body pursuant to the Model Law or as a result of an investigation or examination pursuant to the Model Law from disclosure requests under applicable state freedom of information, "open records", "sunshine" and other appropriate laws.

The drafters of the Model Law specified that they intend that if a Licensee is in compliance with the NYDFS Cybersecurity Regulation, such Licensee is also in compliance with the Model Law.

Key Requirements under the NYDFS Cybersecurity Regulation

The NYDFS Cybersecurity Regulation requires Covered Entities to adopt a cybersecurity program and policies or procedures, which are based on the Covered Entities' risk assessment. "Covered Entity" is defined in the NYDFS Cybersecurity Regulation as any person "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, Insurance Law or Financial Services Law." The risk assessment must be carried out in accordance with written policies and procedures, which must include (i) criteria for evaluation and categorization of threats, (ii) criteria for assessment of confidentiality, integrity, security and availability of the Covered Entity's information systems and nonpublic information, and (iii) requirements describing risk mitigation or acceptance.

Based on the risk assessment, the NYDFS Cybersecurity Regulation requires each Covered Entity to establish a cybersecurity program designed to ensure the confidentiality, integrity, and availability of the Covered Entity's information systems. The program must be designed to identify cyber risks, implement policies and procedures, detect and respond to cybersecurity events, recover from cybersecurity events and restore normal operations, and comply with all regulatory reporting obligations, among other requirements.

The cybersecurity policy must be approved by the Covered Entity's board of directors or equivalent governing body, or by a Senior Officer (as defined in the NYDFS Cybersecurity Regulation) of the Covered Entity.

Other requirements of the NYDFS Cybersecurity Regulation include the following:

- Each Covered Entity must designate a qualified individual to serve as the Covered Entity's Chief Information Security Officer ("**CISO**").
- The cybersecurity program for each Covered Entity must provide for monitoring and testing developed as a result of the Covered Entity's risk assessment.
- Based on its risk assessment, Covered Entities must maintain systems that (i) are designed to reconstruct material financial transactions, and (ii) include audit trails designed to detect and respond to a Cybersecurity Event that have a reasonable likelihood of materially harming any material part of the normal operation of the Covered Entity.
- All personnel within each Covered Entity would be required to attend regular cybersecurity awareness training sessions.
- Any individual accessing the Covered Entity's internal systems from an external network of non-public information must pass a "Multi-Factor Authentication" system, unless the CISO has approved the use of at least equivalent access controls.
- The NYDFS Cybersecurity Regulation requires Covered Entities to implement written policies and procedures designed to ensure security of information systems and nonpublic information that are accessible to, or held by, third-party service providers.

- If a Covered Entity identifies any cybersecurity events presenting material risk of imminent harm relating to its cybersecurity program, the Covered Entity must notify the Superintendent of the DFS within 72 hours and include such items in its annual report.
- Each Covered Entity would have to submit to the Superintendent of the DFS an annual certification by February 15 of each year, certifying that the Covered Entity is in compliance with the requirements set forth in the NYDFS Cybersecurity Regulation.

DFS CONTINUES TO LEAD ON CYBERSECURITY REGULATION

Continuing its leading role in cybersecurity regulation, the DFS issued a press release on July 31, 2017 which announced the launch of a new online portal to securely transmit in real time all notifications required by Covered Entities under the NYDFS Cybersecurity Regulation. According to Superintendent Maria T. Vullo, "With DFS's leading cybersecurity regulation, the DFS cyber portal will allow New York's financial institutions to quickly, easily, and securely report cybersecurity events and file required certifications of compliance, ensuring that the necessary safeguards are in place to protect New York consumers and financial institutions as the threat of cyber-attacks continues to increase."

Clifford Chance will track further developments with respect to the Model Law and future actions by states relating to the Model Law.

AUTHORS

Alice Kane
Senior Counsel

T +1 212 878 8110
E alice.kane
@cliffordchance.com

Analisa Dillingham
Associate

T +1 212 878 3326
E analisa.dillingham
@cliffordchance.com

Ryan Buffkin
Associate

T +1 212 878 8179
E ryan.buffkin
@cliffordchance.com

ADDITIONAL CONTACTS

Gary Boss
Partner

T +1 212 878 8063
E gary.boss
@cliffordchance.com

Joseph Cosentino
Partner

T +1 212 878 3149
E joseph.cosentino
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Nick Williams
Partner

T +1 212 878 8010
E nick.williams
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Bangkok • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • Jakarta* • London • Luxembourg • Madrid • Milan • Moscow • Munich • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

*Linda Widyati & Partners in association with Clifford Chance.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.