HINSHAW

Another Cybersecurity Wake Up Call: Connecticut Insurance Department Issues Guidance on Cyber Law Set to go Into Effect

3 min read
Jul 31, 2020

Covered entities received two cybersecurity wake up calls from insurance regulators this month. As we have reported, the New York State Department of Financial Services (DFS) issued its long-awaited first cyber enforcement action pursuant to its groundbreaking and first-in-nation cybersecurity regulation. In addition, the Connecticut Insurance Department issued a Bulletin to all licensees, providing guidance for compliance with the Connecticut Insurance Data Security Law (the Act), which goes into effect on October 1, 2020. The Act was modeled after the National Association of Insurance Commissioners Model Cybersecurity Law, which itself was modeled after the DFS cybersecurity regulation.

In the July bulletin, the Insurance Department highlighted a number of important sections of the Act, including the following requirements:

- **Information Security Program**

  Licensees must develop, implement, and maintain a comprehensive written information security program (ISP) that complies with the Act by October 1, 2020. The ISP must be based on a risk assessment and contain safeguards for the protection of both nonpublic information and the licensee's information systems.

- **Third-Party Service Providers**

  Covered licensees must exercise due diligence in selecting service providers and must, by October 1, 2021, require each service provider to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that is accessible to and held by the service provider.

- **Annual Certification by Domestic Insurers**

Annually, beginning February 15, 2021, non-exempt Connecticut domestic insurers must certify compliance with the Act.

- **Cybersecurity Event Investigations**

  Licensees or an outside service provider must conduct a prompt investigation in accordance with the Act after learning of a "cybersecurity event," which is defined as "an event resulting in any unauthorized access to, or disruption or misuse of, an information system or the nonpublic information stored thereon, except if: (A) The event involves the unauthorized acquisition of encrypted nonpublic information if the encryption process for such information or encryption key to such information is not acquired, released or used without authorization; or (B) the event involves access of nonpublic information by an unauthorized person and the licensee determines that such information has not been used or released and has been returned or destroyed."

- **Notification of a Cybersecurity Event**

  Licensees must provide notice of cybersecurity events to the Insurance Commissioner as promptly as possible, but in no event later than three business days after the date of the event when either (1) Connecticut is, in the case of an insurer, the state of domicile, in the case of a producer, the home state of the producer; or (2) the licensee reasonably believes that the event involves nonpublic information of 250 or more consumers residing in Connecticut and state or federal laws require notification to a government entity, or there is a reasonable likelihood of material harm to Connecticut consumers or the licensee's normal operations.

- **Notification to Consumers**

  Licensees must comply with Connecticut's data breach notification law and also provide a copy of any required notice to the Insurance Commissioner.

- **Notice Regarding Cybersecurity Events of Reinsurers**

  Licensees acting as an assuming insurer must notify affected ceding insurers and its domiciliary regulator of a cybersecurity event involving nonpublic information that is used by such assuming insurer or in its possession, custody or control when it is acting as an assuming insurer with no direct contractual relationship with affected consumers not later than 72 hours after the assuming insurer discovered that the cybersecurity event has occurred.

- **Notice by Insurers to Producers of Record**

  If the cybersecurity event involves nonpublic information that is in the possession, custody or control of an licensee acting as an insurer or a third-party service provider for an insurer, the Act requires the insurer to notify the producer of record for any affected consumer residing in this state who accessed services through an independent insurance producer of the occurrence of such event not later than the

time at which notice is provided to such consumer, provided the insurer has the current producer of record information for such individual consumer.

In light of the recent DFS enforcement action and the upcoming effective date of the Connecticut Act, insurers and other covered entities are urged to assess their compliance with these cyber mandates and implement policies and procedures to achieve and maintain ongoing compliance.

Hinshaw & Culbertson LLP is a U.S.-based law firm with offices nationwide. The firm's national reputation spans the insurance industry, the financial services sector, professional services, and other highly regulated industries. Hinshaw provides holistic legal solutions—from litigation and dispute resolution, and business advisory and transactional services, to regulatory compliance—for clients of all sizes. Visit www.hinshawlaw.com for more information and follow @Hinshaw on LinkedIn and X.

Topics

DFS, Cybersecurity, Regulatory, Regulatory Compliance, Connecticut, Connecticut Insurance Department

Related Capabilities

Consumer Financial Services