Updates
October 06, 2022

2022 Breach Notification Law Update: State and Federal Requirements Continue To Evolve

Overview

Cyberattacks continue to plague businesses, making the fallout of data breach notification and response as critical as ever. This year, like 2021, has been relatively quiet as it relates to state updates to breach notification laws. Much of the excitement has instead been around omnibus privacy laws, some of which cover data security as well. Only Maryland made significant alterations to its general data breach notification law, while several other states made more minor changes, as detailed below.

While the state law front has been relatively muted in 2022, the federal government has issued or proposed several new data security and breach reporting requirements for certain types of entities. Companies should take note of the updates in federal laws and federal guidance demanding cybersecurity measures in order to maintain adequate security posture to best prevent ransomware and other cyberattacks.

We discuss relevant state and federal updates below.

State Breach Law Updates

Maryland

On May 29, 2022, Maryland's governor signed into law a variety of changes to its breach notification law that became effective on October 1, 2022, most of which have relatively minor impact. The changes in HB 962 include the following:

- **Expanded definition of personal information.** The definition of "Personal Information" was altered to include "genetic information."
- **Alterations to notification deadlines.** Changes were made to several requirements:
    - Notice to individuals must be given within 45 days after the business *discovers or is notified of the breach of the security of a system*. (Previously, notice could be given 45 days after the company's investigation was completed.)
    - Businesses that maintain data on behalf of the data owner must notify the data owner within **10 days** of discovery or notification of the breach (previously, this was 45 days).
    - When these notices are delayed by a law enforcement request beyond the 45-day period, they must be provided **seven days** after law enforcement determines notice will not impede its investigation.
- **Content requirements for attorney general notification.** Notice to the Office of the Attorney General must now include the number of affected individuals residing in the state, a description of the breach, "including when and how it occurred," and remediation steps the business has taken or plan to take, along with a copy of the notice.
- **Substitute notice revised.** Notification to a statewide media source is no longer adequate. Instead, notification must be given to major print or broadcast media in geographic areas where the individuals

affected by the breach likely reside.
- ***Additional note: Expanded application of data security requirements.*** HB 962 also included a change to § 14–3503, which requires entities to apply reasonable security to "personal information." The statute will now apply to entities that maintain information, in addition to those that own or license the information.

Other State Breach Law Changes

- **Arizona** House Bill 2146, effective July 22, 2022, requires that in incidents involving more than 1,000 Arizona residents, entities must notify both the attorney general and the director of the Arizona Department of Homeland Security, instead of previously just the former.
- **Indiana** House Bill 1351, effective July 1, 2022, adds a time limit of no more than 45 days after the discovery of the breach to notify individuals and the state attorney general. Indiana did not previously impose a notification deadline, although the attorney general's office encouraged notification within 30 days.
- **Maryland**, **Kentucky**, and **Vermont** each passed a version of the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law, which has been implemented in 18 other states in the past several years. These laws require entities subject to a state's insurance licensing to develop an information security program, investigate cyber events, and notify the state insurance commissioner of material cyber events. The newest laws will go into effect in 2023; similar laws passed last year in Hawaii and Minnesota have just come into effect over summer 2022.

Federal Action: Forthcoming Federal Breach Reporting Requirements

Responding to waves of highly complex and damaging cyberattacks in recent years, two major new requirements are poised to significantly alter incident response for certain covered organizations.

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). On March 15, 2022, President Biden signed CIRCIA into law following attacks on critical infrastructure, such as the May 2021 ransomware attack on Colonial Pipeline and the Russian government attacks against the energy sector. Under CIRCIA, certain "Covered Entities" will be required to report various categories of events, including "covered cyber incidents" (CCIs) and ransom payments. We covered more details regarding the scope of CIRCIA in a previous Update.

CIRCIA requires the Cybersecurity and Infrastructure Security Agency (CISA) director to propose a rule within two years of its enactment. This rulemaking is currently ongoing, with comments due November 16.

SEC Proposes New Cybersecurity Disclosure Rules. On March 9, 2022, the U.S. Securities and Exchange Commission (SEC) issued proposed rules regarding cybersecurity risk management, strategy, governance, and incident disclosure for public companies subject to the reporting requirements of the Securities Exchange Act of 1934. Importantly, the SEC proposed to amend Form 8-K to require disclosure of "material" cybersecurity incidents within four business days. The four-day period would begin after a company determines that a cybersecurity incident was material, and not from the date of the incident itself. For more specifics regarding the proposed Cybersecurity Disclosure Rules, please read this previous Update.

All companies holding data on U.S. residents—including employees—should understand the scope of state notification laws and how they may affect the companies' obligations in response to a breach. Perkins Coie's Security Breach Notification Chart offers a comprehensive and current summary of state laws regarding such requirements. For further questions on state or international breach notification requirements or the federal guidance described above, please contact experienced counsel.

Authors

Amelia M. Gerlicher

Partner
AGerlicher@perkinscoie.com 206.359.3445

Peter Hegel

Counsel
PHegel@perkinscoie.com 312.324.8683

Akua N. Asare-Konadu

Associate
AAsareKonadu@perkinscoie.com 206.359.3252

Explore more in

Privacy & Security Retail & Consumer Products

Related insights

Update

Securities Enforcement Forum DC 2024: Priorities in the Election’s Wake

Update

The New Administration’s Impact on Retailers