Updates
September 30, 2024
2024 Breach Notification Law Update: Unique New State Obligations and Widespread New Federal Obligations

Overview

Amid intense focus on AI and a flurry of consumer privacy law updates, legislative activity has continued to change data breach notification requirements in a variety of ways. Similar to 2023, a handful of changes to generally applicable state breach notification statutes were accompanied by steady sectoral activity at the state level and significant updates at the federal level, including new obligations from both the Federal Trade Commission (FTC) and the U.S. Securities and Exchange Commission (SEC).

For businesses and organizations subject to state and federal data breach notification obligations, understanding the magnitude of these changes, as well as when the changes take effect, will be crucial for compliance. Below is a summary of some of the major changes and amendments for 2024.

State Breach Laws Updates

Pennsylvania

For the second year in a row, Pennsylvania tops the list with a series of short yet substantial updates to its data breach notification statute. Senate Bill 824 took effect on September 26, 2024. Certain updates included in this bill (detailed below) are unique, and it is possible that this may influence nationwide compliance going forward.

- **Regulator notice.** Entities notifying more than 500 Pennsylvania residents must now notify the attorney general. The report must include a summary of the incident, the date of the breach, and both the number of Pennsylvania residents affected and the total affected overall. The law does not specify how the report is to be made or if the attorney general's office will make it public.

- **Assumption of costs requirement for entities.** Pennsylvania adds two unique provisions related to credit reports to its law.
    - First, if a breach of security affects Social Security numbers, driver's license numbers, *or bank account numbers*, the entity must provide credit monitoring free of charge for 12 months. Although other states require credit monitoring, they do so only for breaches involving Social Security numbers or other tax identification numbers.
    - Second, entities must also assume all costs and fees in providing affected individuals "access to one independent credit report from a consumer reporting agency if the individual is not eligible to obtain an independent credit report from a consumer reporting agency for free." The statute is silent on how an entity would identify or confirm which consumers would require a free credit report or if the obligation can be satisfied with the credit monitoring offer.
- **Narrowed definition of personal information.** Only last year, Pennsylvania expanded the definition of "personal information" that triggers notification to include "medical information." However, Pennsylvania's new law narrows its scope, requiring notification only for medical information "in the possession of a State agency or State agency contractor."
- **Decreased threshold for consumer reporting agency notice.** Mirroring the numerical threshold for a regulator notification seen above, Pennsylvania lowered its threshold to notify consumer reporting agencies from 1,000 to 500 persons.

Utah

Expanding on last year's Cybersecurity Amendments creating the "Utah Cyber Center," Utah's Governor Spencer J. Cox signed Senate Bill 98. Senate Bill 98 went into effect on May 1, 2024, and, among other things, amended the Protection of Personal Information Act in two important ways for private organizations:

- **Confidential and classified information.** First, the amendments clarify that information an entity submits to the attorney general or Utah Cyber Center "may be deemed confidential and classified as a protected record" as long as certain conditions are met. Furthermore, "information produced by the Office of the Attorney General or the Utah Cyber Center in providing coordination or assistance to the person providing notification" may also be deemed confidential and classified.
- **New reporting requirements.** Second, the amendments add requirements for the content of the notification to the attorney general and the Utah Cyber Center. The notice must now include:
    - The date the breach of system security occurred.
    - The date the breach of system security was discovered.
    - The total number of people affected by the breach of system security, including the total number of Utah residents affected.
    - The type of personal information involved in the breach of system security.
    - A short description of the breach of system security that occurred.

Other Relevant State Legislative Updates

Although only a few states revised their respective breach notification statutes, three other key trends are taking hold at the state level that will affect an organization's security obligations.

- **Security obligations in comprehensive privacy laws.** Riding on the tidal wave of momentum in the privacy sphere, seven more states passed comprehensive privacy laws in 2024: Kentucky, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, and Rhode Island. Some, although not all, include general security provisions requiring companies to appropriately secure all personal data. Uniquely, California is in the process of finalizing regulations requiring comprehensive cybersecurity audits of

certain companies, and it is anticipated that final regulations may be effective by the end of 2024.
- **Insurance data security requirements.** Following momentum from prior years, Alaska and Oklahoma each passed state laws focused on insurance licensees. Both the Oklahoma Insurance Data Security Act and Alaska's Senate Bill 134 are based on the National Association of Insurance Commissioners model data security law and similarly require organizations to develop and maintain a data security program and implement reporting obligations for cybersecurity events. The Oklahoma Insurance Data Security Act became effective on July 1, 2024, and certain portions of the Alaska Insurance Data Security provisions related to data breach notification are retroactively effective as of January 1, 2024.

Finally, in addition to these general trends highlighted above, there continues to be significant activity regulating security requirements for state agencies and other government entities. Most notably, Utah amended the Utah Technology Governance Act to significantly expand the definition of "data breaches" that government entities must report to the Utah Cyber Center.

Federal Action

The year 2024 saw major action on the federal front, with significant action from the FTC in finalizing its Health Breach Notification Rule (HBNR) and amendments to the Safeguards Rule applicable to nonbank financial institutions, and the SEC in finalizing rules applicable to broker dealers and investment advisors and putting its amended disclosure rules for public companies into effect.

Health Breach Notification Rule (FTC)

On April 26, 2024, the FTC finalized updates to its Health Breach Notification Rule. The HBNR largely parallels the HIPAA breach notification rule but applies to health apps and related technologies. There are two key features to this update:

- **Expanded entities in scope.** The updated rule expands definitions of both the covered information and the relevant entities such that it covers a greater variety of apps and websites with some connection to health issues. In particular, the FTC intentionally swept in services related to such wellness issues as fitness, sleep, and diet.
- **Expanded definition of breach of security.** In addition to traditional security incidents, the rule sweeps in traditional privacy issues, such as a company's intentional but unauthorized disclosure of consumers' information to third-party companies. This expansion is consistent with the FTC's recent enforcement actions related to health information sharing, such as GoodRx and Easy Healthcare.

For additional information, please see our previous publication, FTC Expands Health Breach Notification Rule.

Safeguards Rule (FTC)

On October 27, 2023, the FTC announced an amendment to the Gramm-Leach-Bliley Act's (GLBA) Safeguards Rule, which includes a new notification obligation for a broad range of nonbank financial institutions. Covered institutions must notify the FTC of incidents involving more than 500 people. There is no individual notice requirement, but the FTC has indicated it will make the notice public.

The notification obligation is significantly broader than state breach notification laws in three key ways. First, it applies to all nonpublic, personally identifiable financial information (also known as "NPI") that is maintained about a "customer," which is a consumer with whom the institution has a continuing relationship to provide financial products or services for personal, family, or household purposes. This could include information as

basic as just customers' names.

Second, notice is required for any "notification event," which, similar to the FTC's HBNR (see above), includes not only data breaches and security incidents as traditionally understood but also voluntary and/or intentional sharing of customer information by a financial institution if done without the customer's authorization.

Third, *all* "notification events" must be disclosed if 500 people are affected—even those with no risk of harm. The combined effect of these changes is a significant departure from previously applicable law that should be carefully reviewed by covered institutions.

For more information, please see our previous publication, FTC Announces Data Breach Reporting Obligation Under GLBA Safeguards Rule.

Regulation S-P (SEC)

In May 2024, the SEC finalized amendments to Regulation S-P (Reg S-P), which defines privacy and security requirements for broker dealers, investment companies, registered investment advisers, and transfer agents. Up until 2024, the data security requirements applicable to these companies were quite short, much like the FTC's Safeguards Rule before its 2021 updates. The amendments require covered institutions to implement and maintain written policies and procedures for an incident response program. The program must be reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including specific documentation requirements related to security incidents.

In addition, Reg S-P includes new obligations around customer notification following a data breach. Under the new rule, covered institutions must provide notice to individuals as soon as reasonably practicable but not later than 30 days after becoming aware of the unauthorized access to or use of customer information. Notification must be given to each individual whose sensitive customer information was, or was reasonably likely to have been, accessed or used without authorization—and if the institution cannot determine which specific individuals' information was accessed, it must provide notice to everyone whose information was stored on the affected system.

The notice obligation applies to any information elements that "alone or together" create a reasonably likely risk of substantial harm or inconvenience, including an increased risk of becoming a victim of fraud or identity theft. The statute provides examples of different types of information that could satisfy these standards, including so-called "authenticating information," such as a partial Social Security number or mother's maiden name, *if* it can be used to access an account. As with the FTC rule described above, covered institutions should carefully consider how this rule would apply to their business in practice.

FCC Breach Notification Rule

In December 2023, the Federal Communications Commission (FCC) issued its order finalizing changes to its breach notification requirements, which we discussed last year. The changes were effective March 13, 2024.

The rules apply to telecommunications services providers and Voice over Internet Protocol (VoIP) providers (carriers), as well as telecommunications relay services (TRS) providers that allow customers with hearing or speech disabilities to place and receive calls. Similar to the other changes discussed above, the new rules cover a substantially broader set of incidents. The rules (1) expand the scope of breach notifications to all types of information that might identify a customer; and (2) expand the definition of "breach" to include inadvertent PII disclosures by carriers and TRS providers. Affected entities must also notify the FCC. For more information, see

our prior Update summarizing the changes.

CIRCIA

On April 4, 2024, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) published a Notice of Proposed Rulemaking containing proposed rules to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Under CIRCIA, "covered entities" will be required to quickly report to CISA any covered cyber incidents, ransom payments, and substantial new or different information discovered related to a previously submitted report. Specifically, "covered cyber incidents" must be reported to CISA within 72 hours, and ransom payments must be reported to CISA within 24 hours. Failure to comply with these reporting obligations will result in a Request for Information (RFI) from CISA, and further failure to respond to an RFI may result in a subpoena to compel information.

Reportable covered cyber incidents are any "substantial cyber incidents." In the proposed rules, CISA defined the term "substantial cyber incident" to mean a cyber incident that leads to any of the following:

- Substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network.
- Serious impact on the safety and resiliency of a covered entity's operational systems and processes.
- Disruption of a covered entity's ability to engage in business or industrial operations or deliver goods or services.
- Unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by either a compromise of a cloud service provider, managed service provider, other third-party data hosting provider, or a supply chain compromise.

The proposed rules suggest that covered entities should include all entities within the "critical infrastructure sectors" under Presidential Policy Directive (PPD) 21 (as well as certain additional sector-based criteria). The PPD sectors include such broad categories as food and agriculture, commercial real estate, and information technology. Although entities that qualify as a "small business" under U.S. Small Business Administration rules are exempt, the comments make clear that CISA intends for the rule to have broad application.

The notice and comment period for the CIRCIA proposed rules closed on June 4, 2024, although the final rules are not anticipated until late 2025. While CISA is expected to harmonize reporting requirements that exist with other government agencies, for entities looking to get ahead of CIRCIA implementation, it may be useful to review areas where the proposed rules expand on existing incident reporting obligations and assess internal compliance with potential new obligations.

All companies holding data on U.S. residents—including employees—should understand the scope of the laws described above 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 provisions described above, please contact experienced counsel.

Authors

Explore more in

Privacy & Security Technology Transactions & Privacy Law Retail & Consumer Products Communications

Related insights

Publication

Security Breach Notification Chart