Updates

A flurry of legislative activity over the past year has brought meaningful changes to a variety of privacy and security provisions in state and federal law.

At the state level, as in 2022, we have seen a handful of changes to generally applicable breach notification statutes, along with action on both narrower security provisions and broader omnibus privacy laws. On the federal level, the most significant development is the U.S. Security and Exchange Commission's (SEC) recent changes to reporting requirements for public companies, but rulemaking is underway in multiple other sectors as well.

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

State Breach Laws Updates

Pennsylvania

The first major update to Pennsylvania's Breach of Personal Information Notification Act was passed earlier this year. The updates include a range of changes consistent with those adopted in other states in the last several years, so these updates are unlikely to substantially change nationwide compliance for most private sector companies (Pennsylvania government entities, on the other hand, will face substantial new requirements and tight deadlines). The amendments took effect on May 2, 2023.

- **Expanded definition of personal information.** Personal information now includes "medical information" and "health insurance information," as well as online account credentials.
- **Additions of "discovery" and "determination" of a breach.** The amendments add the concept that there is a gap between "discovery" of a breach (the "suspicion" that a breach has occurred) and the "determination" ("verification or reasonable certainty") that a breach has occurred. In a nod to the practicalities of breach response, notice is not required until such a determination is made. (The statute did not previously include, and the amendments do not add, a deadline for notice. The standard remains "without unreasonable delay" following the determination.)
- **Deadlines for governments, agencies, and schools.** The amendments added specific provisions requiring state agencies, counties, municipalities, and schools to provide notice to both individuals and the state attorney general within seven business days. State agencies must also notify the governor's Office of Administration within three business days.

Included with the breach notification amendments were two new provisions requiring state agencies and their contractors to implement policies and procedures regarding the proper encryption and storage of personal information held "on behalf of the commonwealth." These policies must be reviewed at least annually and updated as necessary.

Utah

New attorney general notice requirement. Utah passed Cybersecurity Amendments creating a new "Utah Cyber Center" with a variety of cyber policy-related responsibilities. Most relevant to the private sector, the bill added a requirement to report breaches affecting more than 500 Utah residents to both the state attorney general and the new Cyber Center, and to report breaches affecting 1000 or more residents to the credit reporting agencies. The Cybersecurity Amendments took effect on May 3, 2023.

Texas

New attorney general notice deadline. As of September 1, 2023, Texas shortened the deadline for organizations to notify the state attorney general from 60 days to "as soon as practicable and not later than 30 days," while leaving in place the 60-day deadline to notify individuals. The amendments also require covered entities to submit breach reports to the state attorney general via an electronic form that is accessible on the state attorney general's website. The attorney general's office has 30 days to publish these reports, but in practice publishes the information almost immediately.

Florida

New types of personal information. Florida's Digital Bill of Rights includes, among its many changes to various consumer privacy protections, a change to the definition of "personal information" in the breach notification statute. The bill adds an individual's biometric data and "any information regarding an individual's geolocation" to the statute, without any corresponding definitions. This amendment takes effect July 1, 2024.

California

Expanded private right of action. Although not strictly a change to the state breach notifications statute, the California Privacy Rights Act (CPRA) made two changes affecting the breach notification landscape. Under the California Consumer Privacy Act (CCPA), statutory damages applied to private lawsuits regarding breaches of data listed in Cal. Civ. Code 1798.81.5. This list was different from the data covered by California's breach notification law in one key respect: it did not include online account credentials. The CPRA remedied this omission and made breaches of account credentials subject to the private right of action, effective January 1, 2023. In addition, the CPRA includes a provision stating that "implementation and maintenance of reasonable security procedures and practices" *after* a breach do not constitute a "cure" under the statute (which requires plaintiffs to provide companies notice an opportunity to cure 30 days before following suit).

State Updates to Security Requirements

In addition to revisions to breach notification statutes, states are making a variety of changes to substantive data security obligations. Changes applicable to private companies include:

- **Security obligations in comprehensive privacy laws.** To date, 12 states have passed comprehensive privacy laws regulating "personal information," very broadly defined (as opposed to the narrower definitions traditionally used by state breach notification and data security statutes). Some, although not all, include general security provisions requiring companies to appropriately secure all personal data (such as Iowa and Tennessee). California also requires, uniquely thus far, comprehensive cybersecurity audits of some companies; proposed regulations defining the scope of the required audits have just been released. Although enforceable by state attorneys generally, these provisions are generally not enforceable with private rights of action.
- **Affirmative defenses.** Iowa became the fourth state (after Connecticut and Utah, described in our 2021 update, as well as Ohio) to add a law establishing an affirmative defense to data breach cases brought in tort law, if the company maintains a written cybersecurity program designed to address reasonably foreseeable risks, estimate the company's probable loss, and communicate to affected parties following a data breach. The Iowa law cites six general frameworks, the Payment Card Industry Data Security Standard (PCI-DSS), and requirements under multiple federal regulations and agencies that are deemed to comply with the statute's requirements, but does not restrict the availability of the defense to companies using any particular standards.
- **Insurance data security requirements.** In June 2023, Illinois became the 23rd state to pass a law focused on the state's insurance licensees. Illinois licensees must develop and implement a written information security program, investigate cybersecurity events, and notify the Illinois Department of Insurance as promptly as possible, but no later than three business days after determining a cybersecurity event has occurred. Like most other states, the law is based on the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law (MDL-668). The law goes into effect January 1, 2024. (Note also that laws in Kentucky, Maryland, and Vermont passed last year have just come into effect over the last several months.)
- **New York Department of Financial Services updates.** In June 2023, the New York Department of Financial Services (NYDFS) proposed revised amendments to its cybersecurity regulations. Among other changes, the proposed regulations would expand the cybersecurity event notification requirement to

expressly cover new types of cybersecurity events and introduce a new notification requirement for ransom payments. Now aligning with the Federal Trade Commission (FTC) Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA), the proposed regulations require multifactor authentication (MFA) for any access to an entity's systems, or, in the alternative, a chief information security officer (CISO) may approve in writing the use of reasonably equivalent or more secure compensating controls. The NYDFS kicked off a 45-day public comment period that ended on August 14, 2023. If no additional updates are proposed, the bulk of the proposed regulations will take effect in February 2024.

Federal Action

Following last year's passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) (rulemaking for which should formally commence in 2024), the major action on the federal front this year came from the SEC, which formalized disclosure requirements for public companies. We are also following proposed new or expanded rules from the FTC related to health data breaches, the FCC covering customer proprietary network information (CPNI), and the SEC for broker-dealers.

SEC

Public Companies

In July 2023, the SEC adopted a final rule establishing cybersecurity risk management, governance, and incident reporting requirements. These new requirements will apply to foreign private issuers and U.S. public companies.

The final rule went into effect on September 5, 2023, with compliance deadlines as early as December 2023. In short, the new rule requires:

- Form 8-K disclosure of material cybersecurity incidents within four business days of a company's determination that the incident is material or will result in material changes for investors, and updates without unreasonable delay.
- Annual disclosure in Form 10-K regarding the company's cybersecurity risk management and strategy which should include the company's process for assessing, identifying, and managing material risks from cyber security threats.
- Separate annual disclosures of the company's cybersecurity governance, describing the roles of the board and oversight processes for cybersecurity risks.

Because of the complexity of the SEC's rules—as well as the impending December effective date—we encourage all organizations to thoroughly review the requirements. To that end, our team outlined the SEC's new requirements here and provided in-depth commentary on grappling with the new "materiality" standard and how to incorporate the new standard into incident response.

Broker-Dealers and Market Entities

The SEC is also in the process of proposing new cyber rules for broker-dealers, clearing agencies, major security-based swap participants, the Municipal Securities Rulemaking Board, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers, and transfer agents (collectively known as market entities) to address their cybersecurity risks. The proposed rule includes both internal requirements for improved cyber policies and procedures, and notification requirements to the SEC and the public following a "significant" cybersecurity incident (defined as an incident that significantly degrades operations or causes significant harm).

The SEC also simultaneously proposed revisions to Regulation S-P that would require individual notice within 30 days following a breach involving "sensitive personal information," the definition of which is information "the compromise of which could create a reasonably likely risk of substantial harm or inconvenience." The commentary and examples indicate this standard is intended to apply to broader types of information than state laws and current federal guidance applicable to banks, but limited by strong concepts of harm. The proposal would also broaden the regulation's existing information safeguards requirements.

Comments on both proposals closed June 5, 2023. Alongside these two proposals, the SEC also re-opened comments on its proposed Cybersecurity Risk Management proposals for investment advisors, which includes similar requirements.

FCC

In 2023, the FCC proposed new rules regarding data breach reporting requirements for CPNI. The proposed rules include the following changes:

- Expanding the definition of "breach" to include inadvertent disclosures of customer information.
- Requiring carriers to notify the commission and Federal Bureau of Investigation (FBI) of any incident where access, use, or disclosure occurs.
- Eliminating the seven-day waiting period for notifying customers of breaches.
- Providing specific requirements for customer notification.

The comment period under the rule-making process ended in March 2023.

FTC

The FTC has proposed changes to the Health Breach Notification Rule (HBNR) that applies to "vendors of personal health data" and others not covered under Health Insurance Portability and Accountability Act (HIPAA). The proposed changes, like the FTC's first enforcement actions on this rule earlier this year, take an expansive approach to the rule, which would apply to a variety of technologies and circumstances. The comment period ended on August 8, 2023.

Takeaways

All companies holding data on U.S. residents—including employees—should understand the scope of the laws described above and how they may affect 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

Amelia M. Gerlicher

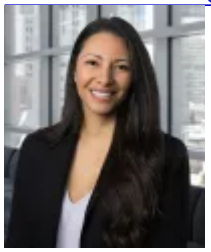
Partner
AGerlicher@perkinscoie.com 206.359.3445

Peter Hegel

Counsel
PHegel@perkinscoie.com 312.324.8683

Akua N. Asare-Konadu

Associate
AAsareKonadu@perkinscoie.com 206.359.3252



Oviett Worthington Wargula

Associate
OWorthingtonWargula@perkinscoie.com 206.359.3130

Explore more in

Privacy & Security Retail & Consumer Products

Related insights

Update

It’s Official: Cybersecurity Disclosure Is Coming This Year

Update

FTC Claims Sharing User Health Data With Advertising Platforms Is a “Security Breach”