Updates
September 14, 2021

2021 Breach Notification Law Update: Connecticut and Texas Expand Requirements, Ransomware and Supply Chain Attacks Take Spotlight

Cyberattacks continue to make the news and affect our lives in increasingly more significant ways. However, after several years in which states have actively updated breach notification laws in reaction to significant data breaches, 2021, like 2020, has been relatively quiet. Just two states—Connecticut and Texas—have updated their general data breach notification laws, and only Connecticut's changes will have significant impacts on compliance. Connecticut and Utah also enacted novel "safe harbor" laws that provide reprieve from liability in certain data breach tort actions, but only if a company adopts specific recognized data security practices. (States have been actively debating privacy legislation this year—with Colorado and Virginia joining California in enacting omnibus privacy laws—but those laws generally do not impose any security requirements.)

Though state law updates have been relatively quiet, the recent spate of cyberattacks has ushered in a new era of federal attention to cybersecurity. In addition to updated breach reporting requirements, companies should take note of federal agency guidance on cybersecurity measures that should be implemented to prevent ransomware and other cyberattacks.

We discuss relevant state and federal updates below.

State Breach Law Updates

Connecticut

Connecticut recently signed into law a significant expansion of its breach notification law that becomes effective on October 1, 2021. The changes in Public Act 21-59, while substantial, are generally in line with trends seen across the country over the last few years (see, e.g., developments in 2019 and 2018).

- **Broadened Application.** Connecticut's law previously applied only to entities that "conduct business" in the state and collect personal information in the ordinary course of their business. The amended law discards these qualifiers and applies to any entity that "owns, licenses or maintains computerized data that includes personal information" of Connecticut residents.
- **Expanded Definition of Personal Information.** The amended law significantly expands the definition of covered "personal information," aligning Connecticut with trends in other states. New categories of personal information include:
    - Individual taxpayer identification number;
    - Identity protection personal identification number issued by the Internal Revenue Service;
    - Passport number, military identification number, or other identification number issued by the government that is used to verify identity;
    - Medical information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional;
    - Health insurance policy number or subscriber identification number, or any unique identifier used by a health insurer to identify the individual;

    - Biometric information consisting of data generated by electronic measurements of an individual's unique physical characteristics and used to authenticate or ascertain the individual's identity, such as a fingerprint, voice print, retina, or iris image; and
    - Username or email address, in combination with a password or security question and answer that would permit access to an online account.
- **Expedited Notice Deadline.** PA 21-59 shortens the deadline for providing notice to Connecticut residents and the attorney general's office, from 90 days to 60 days from the date of discovery.
- **Breaches of Login Credentials.** Notice for breaches of login credentials may be provided in electronic form or other means (so long as it is not sent to a breached email account) that directs affected individuals to change their credentials or take other steps to protect their online account(s).
- **Credit Monitoring Obligations.** The amendment expands the existing requirement to offer 24 months of free identity theft prevention and mitigation services if a breach involves Social Security numbers or breaches of taxpayer identification numbers.
- **HIPAA Compliance.** While PA 21-59 adds medical information to the definition of "personal information" triggering notice, it also exempts entities that are covered by and in compliance with HIPAA and HITECH. Such an entity will be deemed in compliance with Connecticut's law as long as the entity notifies the attorney general any time a Connecticut resident is notified pursuant to HITECH and complies with the credit monitoring provisions, when required.
- **Freedom of Information Requests.** PA 21-59 exempts certain materials related to data breaches from public disclosure pursuant to the Connecticut freedom of information law.

Texas

Texas updated its data breach notification statute in June to include new attorney general reporting requirements. The amended law is effective September 1, 2021.

- **Content of the Attorney General Notice.** As of September 1, 2021, notice to the Texas attorney general must include the number of affected residents in the state (in addition to the other information already prescribed by the statute).
- **Attorney General Website.** The amendment requires the attorney general to publicly post a list of data breach notifications it receives on its website. Each notice must be posted no later than 30 days after receipt. A notice can be removed after a year unless the relevant business reports another breach to the attorney general in that time.

State Affirmative Defense Laws

In 2021, both Utah and Connecticut enacted laws providing that certain types of cybersecurity programs may be the basis for an affirmative defense against data breach lawsuits, following on Ohio's similar 2018 law. Utah's Cybersecurity Affirmative Defense Act (Utah Code § 78B-4-701) and Connecticut's Act Incentivizing the Adoption of Cybersecurity Standards for Businesses (Public Act 21-119) each encourage companies to adopt recognized cybersecurity standards by offering a safe harbor from tort liability in certain circumstances. The Utah law became effective in May. Connecticut's law goes into effect on October 1. Overall, the laws are structured similarly, but the Connecticut law applies to a broader set of incidents, has a more restrictive set of qualifying cyber programs, and protects only against punitive damages.

The specific similarities and differences between each are discussed below.

- Both laws apply to entities that possess "personal information" and experience a "breach of system security" or "data breach," as those terms are defined by their respective state data breach laws.

Connecticut's safe harbor law also applies to "restricted information," a new term that encompasses essentially any information about an individual, "the breach of which is likely to result in a material risk of identity theft or other fraud to a person or property."

- **Safe Harbor.** Utah provides an affirmative defense, and Connecticut a liability shield against punitive damages, in certain tort actions alleging that a company's failure to implement reasonable cybersecurity controls resulted in a data breach. To take advantage of the safe harbor in each state, companies must create, maintain, and comply with a cybersecurity program that meets certain requirements (see below).
- **Cybersecurity Program Requirements.** The Utah and Connecticut laws detail similar requirements for what must comprise a company's cybersecurity program in order to make use of the safe harbor. Under each law, the cybersecurity program must contain administrative, technical, and physical safeguards designed to protect personal information (and restricted information in Connecticut).

Both laws list recognized cybersecurity frameworks that satisfy the statute's requirements, with the following frameworks appearing on both lists (as well as in Ohio's statute):

- National Institute for Standards and Technology (NIST) SP 800-171, 800-53 and 800-53a;
- The FedRAMP Security Assessment Framework;
- The Center for Internet Security's "Center for Internet Security Critical Security Controls for Effective Cyber Defense" framework;
- The ISO 2700 series; or
- Statutory requirements of HIPAA and/or HITECH, GLBA, and FISMA.

Connecticut's list is limited to these frameworks plus NIST's "Framework for Improving Critical Infrastructure Security." Utah also includes compliance with PCI-DSS or any applicable state or federal regulation, in addition to providing a separate list of elements that constitute an acceptable program, without needing to specifically conform to one of the listed frameworks.

Federal Action: Ransomware and Supply Chain Attacks

The escalation of ransomware and supply chain attacks during 2021 has prompted a flurry of activity from the federal government related to breach reporting and cybersecurity measures, signaling an increased focus on cybersecurity that may serve as a roadmap for what is expected from business' cybersecurity programs.

- **Biden Administration Executive Order.** In June 2021, the Biden administration issued an open letter urging corporate executive and business leaders to take steps to prevent ransomware attacks. The letter describes the federal government's strategy to curtail attacks and offers recommendations for the private sector. These recommendations include adopting the "five best practices" outline in the president's May 2021 Executive Order on Improving the Nation's Cybersecurity, namely multifactor authentication, endpoint detection, endpoint response, encryption, and security teams. These best practices are mandates for certain government contractors and federal agencies under the executive order, which also imposes breach reporting requirements for certain data breaches that could affect federal networks.
- **SEC.** In June 2021, the U.S. Securities and Exchange Commission (SEC) sent requests for information to hundreds of companies that used SolarWinds' software. The SEC requested information relating to how companies were affected by the cyberattack, including remedial actions taken in response. The request offered amnesty to targeted companies that voluntarily provided the requested information and warned that noncompliance may result in enforcement actions and heightened penalties. (The SEC has also signaled heightened attention to cyber incident disclosures with recent settlements involving Pearson and First American Financial.)

- **Other Agencies.** Since April 2021, the U.S. Federal Trade Commission (FTC), the U.S. Department of Labor (DOL), U.S. Department of Health and Human Services' Office for Civil Rights (OCR), and the New York Department of Financial Services (NYDFS) have each announced guidance addressing ransomware attacks. These notices include recommended cybersecurity measures entities to be implemented in each agency's purview.

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

Explore more in

Privacy & Security Retail & Consumer Products

Related insights

Update

The New Administration’s Impact on Retailers

Update

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