Updates
June 27, 2019
States Continue to Expand Breach Notification Requirements in 2019

As more and larger data breaches come to light, states continue to update and expand their breach notification statutes, adding to the patchwork of notification obligations that now exists in every state. Generally speaking, none of this year's modifications require substantial changes to preparations for a nationwide breach response because they are similar to changes made by other states in the past or reflect existing best practices. However, organizations that operate primarily in a particular state or that maintain state-specific response procedures should review their plans in light of these changes.

Over the past six months, Arkansas, Connecticut, Maryland, Massachusetts, New Jersey, Oregon, Texas, Utah, Virginia, and Washington have amended their breach notification statutes, and bills in Illinois and New York have passed their state legislatures and await signature from their respective governors. Notable changes are described below.

Expanded Data Elements

States continued a long-running trend of expanding the types of data elements that trigger notification, primarily to add online account credentials and biometric information.

- **New Jersey** (effective September 1, 2019), **Oregon** (effective January 1, 2020), and **Washington** (effective March 1, 2020) added **account credentials** to their definitions of "personal information."
- **Arkansas** (effective July 23, 2019) and **Washington** amended their laws to include **biometric data**.
- **Virginia** (effective July 1, 2019) and **Washington** added **military ID and passport numbers** to their statutes.
- **Washington** also added several other data types to its definition of "personal information," including **private key (unique to an individual to authenticate or sign an electronic record)**, **student ID number**, **health insurance policy or identification number**, and **medical history or physical/mental condition**.
- In addition, **New York's** amended law (awaiting the governor's signature) would also expand the definition of "private information" to include **biometric data** and **account credentials**.

Regulatory Agency Notifications

While some states added requirements that companies notify state regulators following a breach—a consistent trend for many years—states with existing notice requirements added requirements for the content of that notice.

- **Washington's** amended law (effective March 1, 2020) will require the notification to the attorney general to include a list of the types of personal information affected, how long the data was exposed, and a sample copy of the consumer breach notification. The notice must also be updated if any of the information to be provided is unknown at the time notification is required. This notice is currently made public.
- **Arkansas** updated its law (effective July 23, 2019) to require notice to the attorney general when **1,000** state residents are affected, either at the same time at which consumer notice is provided, or 45 days after the entity determines there is a likelihood of harm to individuals, whichever is sooner.

- **Texas** added a requirement (effective January 1, 2020) that the attorney general be notified if **250** Texas residents are affected, no later than 60 days after the determination that the breach occurred. Consistent with a number of other states, the notification must include basic facts about the breach including what happened, the number of Texas residents affected, and what additional measures the company took to address the issue.
- **Massachusetts** (effective April 11, 2019), which has long required notification to the attorney general and the Office of Consumer Affairs and Business Regulation for *all* breaches affecting Massachusetts residents, now specifies a dozen required elements for the regulatory notification. While most of these were already requested in the forms published by those agencies, the additions most notably require the company to affirmatively disclose whether it has a written information security plan as required under Massachusetts' data security law. Moreover, the attorney general's office must publish on its website both the individual notice and a "report" of the regulatory notice, as well as inform the public of the ability to obtain the full report through a public records request.
- In addition, **Illinois** (also pending the governor's signature) will require notice to the attorney general when more than **500** state residents are affected, no later than when consumers are notified.

Timing of Notification

- **Washington** shortened the time (effective March 1, 2020) by which consumers and the attorney general should be notified from 45 days to **30**. Washington thus joins Colorado and Florida as the states with the shortest notification periods in the United States.
- **Texas** added a deadline of **60** days to its notification statute (effective January 1, 2020).

Other Changes of Note

- **Arkansas** will require companies to retain a copy of their determination of whether a breach occurred and any supporting documentation for five years.
- **Oregon** made certain changes to the language of its statute to confirm its application to entities that process, on their own behalf, data they do not own. In addition, it requires vendors (i.e., those who process data on behalf of another) to notify the entity that owns the data within 10 days, and, if that entity does not notify the attorney general, the vendor must do so.
- For breaches involving social security numbers, **Massachusetts** and **Connecticut** now require victim companies to offer credit monitoring for 18 months and 24 months, respectively. (Connecticut previously required victim companies to offer monitoring for 12 months, although the attorney general's office routinely requested 24 months.)
- **New York's** pending law, in addition to enhancing the breach notification statute, adds specific data security requirements for all businesses collecting personal information from New York residents.

It's critical for all companies holding data on U.S. residents—including employees—to 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 notification. For further questions on state or international breach notification requirements or data breach prevention and remediation planning, please contact experienced counsel.

Authors

Explore more in

Privacy & Security Retail & Consumer Products

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law