Updates
June 26, 2020

2020 Breach Notification Law Update: Vermont, District of Columbia, Maine, and California Expand Requirements

States continue to enhance and expand their breach notification requirements, increasing the scope of breaches that require notice as well as the complexity of compliance. Four jurisdictions—Vermont, the District of Columbia, Maine, and California—updated their data breach notification statute in the past year. As of July 1, amended statutes will be in effect in those jurisdictions.

While the number of states modifying their statutes this year was significantly lower than last year, likely due to the COVID-19 pandemic and related issues taking priority, Vermont and D.C. made extensive amendments that are worth noting. In addition to expanding the definition of personal information, the amendments incorporate similar enhanced standards for attorney general notification, content requirements for notification letters, substitute and alternative notice requirements, and HIPAA exemptions found in many other states' breach laws. California's amendment broadened the types of information that trigger notification but largely maintains the state's already robust breach reporting law. Maine passed a limited amendment that only changed the deadline for breach notification in that state.

Notable changes are described below.

Expanded Data Elements

Three of the amendments expanded their state statute's definition of personal information:

- **California** (effective January 1, 2020), **District of Columbia** (effective June 17, 2020), and **Vermont** (effective July 1, 2020) added **biometric information** to their definitions of personal information and expanded the forms of **government identification** that trigger notification to include individual taxpayer number, military ID, and passport number.
- **D.C.** and **Vermont**'s statutes will now require notification for **login credentials** (i.e., email address and/or user name in combination with passwords or other means of account access), although D.C.'s statute is limited to email account credentials.
- **D.C.** and **Vermont** also now cover **genetic information** and certain **health records** (including medical reports and health insurance policy information).

Regulatory Notifications

D.C. and Vermont added new provisions regarding notification to the attorney general's office:

- **D.C.**'s breach law now requires notification to the Office of the Attorney General if **50 or more** D.C. residents are affected by the breach. This notice must be made "in the most expedient manner possible, without unreasonable delay" and must address a number of points, including basic facts on the incident and remediation measures, and whether the regulated entity has any knowledge of foreign country involvement in the incident.

- **Vermont** added a provision specifying that no attorney general notification is required where login credentials were not obtained directly from the company (i.e., when a company is the victim of a credential stuffing attack). Vermont continues to require attorney general notice of all other credential breaches that involve even one Vermont resident.

Other Changes of Note

- **D.C.**'s law now includes a **harm threshold**; an incident is not a breach if the entity determines, after a reasonable investigation and consultation with the attorney general's office and federal law enforcement agencies, that the incident will likely not result in harm to the individual.
- **D.C.** will require companies to **provide free credit monitoring** for 18 months when the breach affects social security numbers or tax identification numbers.
- **D.C.** and **Vermont** now contain a **HIPAA/HITECH exemption**. The laws consider regulated entities compliant if these entities maintain breach notification procedures in accordance with HIPAA/HITECH.
- **Maine** added a notification deadline of 30 days "after becoming aware of the breach and identifying its scope."

In addition to this spring's crop of changes, companies may want to review last year's changes to the law in 12 states, many of which came into effect in 2020.

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

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