Updates
June 12, 2018
New Data Breach Notification Laws Spring 2018: What You Need to Know

This spring has brought a particularly active round of revisions to state data breach notification laws. Most notably, as of July 1, 2018, **every state** will have a breach notification law. Alabama and South Dakota both passed laws within weeks of each other earlier this year with effective dates of June 1 and July 1, respectively.

These laws, along with revisions to existing laws passed in four additional states, reflect national trends to require notification to both consumers and regulators within a stated time period and to trigger notification requirements based on a broader range of data, including online account credentials, health information, passport numbers and biometric data. As a result, while these changes do add complexity to the national landscape, they should not require substantial changes to existing procedures for handling multistate breaches. Notable features of each of the statutes are described below.

Expanded Data Elements

- In addition to the standard elements of social security number, driver's license number and financial account number, Alabama and South Dakota's laws both cover **usernames and passwords**. South Dakota's law also includes **employee identification numbers** "in combination with any required security code, access code, password, or biometric data." It is also notable that Alabama's law only protects usernames and passwords that are "affiliated with the entity" and where the account itself contains other defined personal information.
- Arizona's amended law (effective August 20, 2018) significantly broadens the definition of personal information to include **usernames and passwords, insurance numbers, health data, passport number, taxpayer identification number, biometric data and any private e-sign or authentication key unique to an individual.**
- Louisiana's amended law (effective August 1, 2018) changes the definition of "personal information" to include **passport numbers, state identification numbers and biometric data**.
- Colorado's amended law (effective September 1, 2018) added **student, military or passport identification number; medical information; health insurance identification number; biometric data; and usernames and passwords** to its definition of personal information. Colorado also now requires notification for exposed financial account information even if no name was exposed.

Shorter Timing Requirements

- Colorado joins Florida in requiring notification within **30 days** of determining that a breach has occurred.
- Oregon's amended law (effective June 2, 2018) as well as Arizona's now require notification no later than **45 days** after discovering a breach—previously both laws required that notification occur "in the most expeditious manner possible, without unreasonable delay." Alabama also joined the 45-day club.
- Louisiana and South Dakota implemented a **60-day** deadline for notification.

Additional Regulator and Consumer Reporting Agency Notifications

- South Dakota requires notification to consumer reporting agencies *regardless of the number of affected state residents* and requires notification to the attorney general when more than **250** residents are affected.
- Arizona and Alabama added requirements that entities must notify consumer reporting agencies and the attorney general if the breach affects more than **1,000** state residents.
- Colorado now requires notice to the attorney general when more than **500** state residents are affected by a breach. (The law already requires that consumer reporting agencies be notified when more than 1,000

Colorado residents are notified.)

Retaining Harm Thresholds

- Both Alabama and South Dakota included harm thresholds in their new laws. Alabama requires notification if the company determines that there has been "unauthorized acquisition" of sensitive personally identifying information and the acquisition is "reasonably likely to cause substantial harm." South Dakota requires notification of an "unauthorized acquisition" unless it "will not likely result in harm;" however, unlike Alabama, entities must notify the attorney general and conduct an appropriate investigation before relying on this determination.
- Louisiana previously had a provision that notification was not required if an incident was not reasonably likely to result in harm. The amendments retained this provision but added a requirement that entities document the determination in writing and, if requested, make this documentation available to the attorney general.

In addition to these changes, Louisiana and Colorado added more general statutory requirements for data security and, in Colorado's case, data disposal.

These updates to the United States' patchwork of breach laws arrive on the heels of the European Union implementing its first ever mandatory data breach notification standard. The EU's comprehensive data privacy law, the General Data Protection Regulation (GDPR), went into effect on May 25, 2018. In addition to mandating notification to regulatory authorities within 72 hours—one of the shortest notice time frames globally—it potentially requires notification for an extremely broad set of data: "any information relating to an identified or identifiable natural person." Notification requirements in turn are entirely based on harm; notification to regulatory authorities is not required if the breach is "unlikely to result in a risk to the rights and freedoms of natural persons," and notification to affected individuals is *only* required when the breach poses a "high" risk to the person's rights and freedoms. Our summary of the GDPR's breach notification requirements provides more information on this regulation.

It should also be noted that Canada's Digital Privacy Act, which amended Canada's existing data privacy law to include mandatory breach notification, comes into effect on November 1, 2018. The law and its accompanying regulations parallel the GDPR in several respects. "Personal information" is defined broadly to include any information about an identifiable individual. The law also contains an expansive harm trigger; "significant harm" includes "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property." Although, unlike in the EU, it only requires notice to regulators "as soon as feasible."

Perkins Coie's Security Breach Notification Chart offers a comprehensive and current summary of state laws regarding security breach 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

General Data Protection Regulation (GDPR) 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