Navigating the 50-State Patchwork of Data Breach Laws

PUBLISHED ON
April 23, 2018

After Alabama enacted its data breach law in March, all 50 states now have some kind of regulation governing cybersecurity and the responsibilities of a business should anyone gain unauthorized access to the personal information it maintains regarding its customers, employees or other individuals.

But that doesn't mean all of those laws are the same, which could cause legal havoc for businesses that operate and have customers in more than one state. A singular definition of "data breach notification law" is somewhat difficult to pin down, because each state's law is slightly different.

The common thread running throughout the patchwork is that individuals, business entities and governments in possession of particular personal information must provide prescribed notices following any unauthorized access to certain personal information. Generally, the notice must be provided to the affected person, though vendors that maintain data on behalf of other business entities must generally notify the other company. The timing of the notice will vary by state.

The information that triggers a notification requirement normally includes:

- First and last name of the individual
- Social Security numbers
- Driver's license numbers
- Financial account numbers
- Health insurance policy information
- Login credentials to an email account
- Credit or debit card numbers in combination with any required security code or other access code

This is not an exhaustive list, making it critically important to understand what constitutes "personal information" as to each affected person. The data breach law that will apply to a specific situation will be that of the state of residence of the affected individual and not the state in which the company has its office. A business that has customers in all 50 states will have to be familiar with the law in each state to know when it must supply notification to the affected customers.

Some statutes, such as the new Alabama law, also require reasonable measures to safeguard personal information. Though not all state statutes specifically require reasonable security measures, certain federal agencies have taken on a very active role in the protection of personal information. Therefore, security measures are a must for every business possessing this kind of information.

While the federal government has left it up to each state to enact its own cybersecurity laws, federal legislators have proposed a number of bills over the years that would end the now-complete patchwork of the state laws and establish a national standard for data security breach notification. None have been passed yet. Most recently, in November, a sponsoring group of senators introduced a bill - called Data Security and Breach Notification Act - which if enacted would require companies to notify customers of data breaches within 30 days of their discovery and impose a five-year prison sentence on organizations caught concealing data breaches.

Cybersecurity begins before the breach ever takes place, but companies would be well-advised to consider security a legal issue, as technological soundness might not always equate to regulatory compliance. Failure to comply with data breach laws can trigger serious consequences, as states begin to enforce them more aggressively. Recently, the attorney general of Pennsylvania filed a lawsuit against Uber after it failed to provide notice of a breach for over a year. The lawsuit could seek as much as $13.5 million in civil fines.

Skilled legal guidance is critical in an environment in which so many legal issues may arise, both before and after a breach. If you have any questions please contact any of the attorneys in the Barley Snyder Business Practice Group.