

Data Breach Disclosure Laws: A State-by-State Perspective

The state of California enacted its data breach disclosure law back in July 2003. Today 38 other states have enacted their own data breach laws. While similar in many respects, security professionals need to be aware of the subtle differences and how to react in the event that a disclosure affects customer spanning multiple states.

**By Philip Alexander
December 17, 2007**

Is your company aware of all the different data-breach-notification laws in the US? Sure, there's California Senate Bill 1386, but what about the other 38 states that have similar laws? Do you think you're familiar with the subtle differences between the various state laws?

Okay, let's test your knowledge. True or false: A breach of data that includes a person's first name, last name and their credit card account number without the PIN doesn't require disclosure? If you think that's always true, look up Kansas Senate Bill 196 and think again. Are you legally required to securely destroy sensitive data on paper? In some states are you. Check out Virginia House Bill 872, for example. Of course, the issue then becomes what to do if certain state laws require disclosure of a specific data breach while other's do not? Do you only disclose to those customers who you're legally obligated to notify? That could be a public relations nightmare if the other customers found out -- and they will find out.

If your company has a multi-state brick-and-mortar footprint or it sells products on the Internet, you must be aware of and must comply with the requirements of the various state data-breach-notification laws.

Caveat Emptor

One constant in the various laws is that companies that have third-party firms maintain customer data for them are still liable if the data is breached. I call that outsourcing the work while 'in-sourcing' the liability! Third-party firms are only responsible for notifying the companies they service that they have suffered, or may have suffered, a data breach. The data owner is still liable to disclose the breach to its customers.

Among the various states, encryption of customer data generally provides an exemption to disclosure requirements. Security professionals and computer engineers certainly know that encryption is not the end-all to protecting data as it's designed to protect the confidentiality of data from unauthorized persons. If a hacker can fool the system into recognizing him or her as an authorized user, they will gain access to the data. Security of the encryption keys themselves is also very

important; if the keys are stolen along with the data, then the hacker can gain access to the information. These gaps were apparently being considered in Pennsylvania when they passed Senate Bill 712. That bill states that, "An entity must PROVIDE NOTICE OF the breach if encrypted information is access and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption keys."

Kansas, Colorado and Delaware are among 18 states that have provisions exempting companies from disclosure if, upon investigation, it is believed that the stolen data will likely not be misused. I would caution companies from relying too heavily on such a provision. For one thing, there is a clear conflict of interest for a company to conduct its own investigation to determine if the data stolen as a result of a security breach is likely to be misused or not. In addition, how can anybody know the hacker's intent? The risk, then, is the negative public perception if it gets out that your company had a data breach and unilaterally decided that the data wasn't likely to be misused.

Half of the states with data breach laws specifically mention data redaction as offering an exemption to disclosure requirements (as is the case in Arizona's Senate Bill 1338). An example would be to edit (redact) a credit card account number so that it would no longer be a true account number. The lesson here is to only use nonpublic personal information (NPI) when it is critical to do so. For example, many companies are using internally developed customer identification numbers rather than social security numbers to track customers. This meets business needs while at the same time reducing data security risks.

As noted earlier, information breach notification laws are not just limited to electronic data. A handful of states, including California, New York, Utah, Vermont and Virginia, have laws specific to the secure disposal of NPI on paper. There are many companies nationwide that provide secure document disposal services.

Do as I Say

All 39 states that have information-breach-notification laws hold businesses liable for the security of NPI, yet only 22 apply the same requirements to their own government agencies. That means eleven states -- Alabama, Colorado, Georgia, Maine, Minnesota, Montana, North Carolina, Oklahoma Texas, Utah or Vermont -- gave themselves a pass on their own laws. This leads me to wonder about the robustness of the data-privacy policies within those states. A caution for the would-be hacker: Several states have made it a criminal offense, some even a felony, to steal somebody's identity. Arizona House Bill 2484, for example, makes identity theft a felony.

It's important to know your customer base and in which states they reside. If you sell online, assume that you have customers in all 50 states. Know the subtle difference of the various data breach notifications laws to better ensure compliance. Be carefully when considering selective breach disclosures based solely on a lack of legal requirements to notify customers in certain states. The public relations fall-out could be more damaging to your company than the actual disclosure itself.

Future State

It's my belief that of the 11 states that currently don't have data breach disclosure laws, most will within the next 3 years. I also expect the federal government to step in within the next couple of years to pass their own law. It will set a baseline making compliance somewhat easier. However, it won't totally negate the effects of the subtle variances amongst the state level laws, but rather provide a minimum for businesses to follow.

Philip Alexander is the author of the book [Data Breach Disclosure Laws: A State-by-State Perspective](#), published by Thomson West.