Published on *The National Law Review* https://natlawreview.com

Data Breach 101, Part I: Data Breach Notification Laws

Article By:

Courtney M Bowman

In 2017, there are few words that make companies – and their counsel – shudder more than “data breach.” Recent high-profile breaches and the resulting litigation have shown that breaches can be embarrassing, harmful to a company’s brand, and extremely expensive to handle – both in terms of response costs and, potentially, damages paid to the affected individuals, third parties, and regulators. As headline-grabbing security incidents increasingly become a fact of life, litigators need to develop familiarity with the issues associated with data breaches so they can be prepared to walk their clients through the aftermath. This is the first in a series of blog posts about what commercial litigators need to know about data breaches.

When a client first receives word of a data breach, it may be overwhelmed with important to-dos: it must stop the security breach as soon as possible, repair or otherwise address any vulnerability that led to the incident, quickly ascertain what information was compromised, and notify affected data subjects as soon as possible. Almost all US jurisdictions have their own laws relating to data breach notification, and – in the case of a large-scale, multi-jurisdictional breach where multiple breach notification laws are in play – figuring out what is required of the client may be a daunting and time-consuming task.

Forty-seven of the fifty US states, as well as Washington, D.C., Guam, Puerto Rico, and the Virgin Islands have statutes requiring businesses or governmental entities to notify individuals whose personal information has been compromised in a security incident. (Only Alabama, New Mexico, and South Dakota have not enacted breach notification laws.) The laws vary as to how they define personal information, when affected individuals must be notified, what that notification must contain (or not contain), what form the notification must take, and whether or not they grant a private right of action to individuals when a company does not comply with the notification law. For example:

- Some jurisdictions set out a specific period of time in which affected individuals must be informed of the breach. Florida, for example, requires that disclosure be made to individuals affected by the breach no later than 30 days from the date of “the determination of a breach or reason to believe a breach occurred.” Others aren’t as specific but still emphasize expeditiousness: New York requires companies that have suffered a breach to notify New York residents affected “without unreasonable delay,” subject to certain exceptions.

- Sometimes state agencies and other governmental entities must be notified of a breach, and in some cases within short time frames. For example, Puerto Rico requires companies that

have suffered data breaches to notify the Department of Consumer Affairs within 10 days of learning about the breach (a fairly quick turnaround time given all that must be accomplished in the days immediately following a breach). New Jersey requires companies to notify the state police.

- California law mandates that the notification be named “Notice of Data Breach” and present certain required information (such as the date of the breach, description of the incident, whether the breach exposed social security numbers) under prescribed headings. Massachusetts law, meanwhile, states that notices may not include information about the nature of the breach or the number of Massachusetts residents affected.

While the summary above provides a brief overview of some notable laws, it is important to determine where data breach victims reside in order to identify the relevant requirements in each case.

Lawyers must also consult the data breach laws of other countries if the breach affects individuals living outside the United States. The European Union has a patchwork of data breach notification laws that vary among member states, but this will change with the introduction of the General Data Protection Regulation in May 2018. This new regulation will harmonize data breach notification law across the EU and require that controllers suffering a breach notify the appropriate national supervisory authority within 72 hours of learning of the breach and affected individuals “without undue delay.” Countries outside the EU have laws of their own: Australia, for example, just passed a breach notification law last month.

A client understandably may be daunted by all the work that must be done in the wake of a data breach and may be especially absorbed by figuring out the cause of the breach and whether the incident has stopped or is ongoing. A lawyer who is aware of the differing notification requirements therefore can serve as a valuable asset by helping shepherd the client through the process and preventing the client from further compounding any legal issues that may result from the breach.

National Law Review, Volume VII, Number 75