Pennsylvania on Data Breach – Shoot First, Ask Questions Later

May 6, 2013

Almost every data breach is complex. If you're a lucky lawyer, your client will contact you immediately upon discovering that something is amiss, allowing you to envelope the episode in attorney-client privilege and to investigate the matter without witness fear of every unfortunate fact seeing the light of day.

Once you're called, you breathe a sigh of relief regarding your involvement, you roll up your sleeves, and you get down to business, and this is no small business - you must serve as general contractor of a multi-faceted, extremely time-sensitive project, coordinating among internal IT; the general counsel's office (if there are any in-house lawyers); insurers; state and federal law enforcement; computer forensics and security experts; PR professionals; counsel for third parties whose data or business practices may be in question; notice, call center, and credit-monitoring service providers; consumers; state regulators; federal regulators; and the list goes on and on. You pray that your work in investigating and mitigating the data breach will foreclose regulatory penalties or private litigation, which present a whole host of other time-consuming and expensive challenges.

The various elements of data breach response can be mind-boggling, but what should not be lost in the storm are the fundamental questions of whether PII and/or PHI is really involved, if so, whether it was actually breached, and, if so, whose data was breached. Those three questions alone can in some cases take months of painstaking investigation to determine. That is why short statutory or regulatory consumer notification periods make absolutely no sense.

The latest example of unduly short notification periods is in Pennsylvania. After a series of embarrassing governmental data breaches, the Pennsylvania Senate has overreacted, imposing a seven-day notice requirement on governmental entities faced with data breaches. While governmental entities certainly should be held to the same data breach standards as private industry, this seven-day requirement simply goes too far and ensures that in responding to data breaches, Pennsylvania agencies will fail. Mistakes will be made, erroneous conclusions will be drawn, and rather than be helped by this short notification period, many consumers could actually be hurt.

Those deserving notice will not get it; those who should not get notice will. The mess resulting from the unnecessarily swift response will draw regulatory and private action scrutiny. And rather than assisting the

Pennsylvania government in responding to data breaches with reasonable alacrity, the seven-day requirement will ensure that compliance with the law will be impossible.

It is clear that the legislators passing this law did not fully comprehend the complexity of data breach response. Rather than shooting first and asking questions later, responders need time to fully investigate before selecting their targets.

For more cutting edge insights, news, and commentary, visit our Media, Privacy & Beyond blog at www.media-privacy.com.