Washington State Amends Data Breach Notification Statute

April 28, 2015

Last week, the Washington Governor signed into law amendments to the state's data breach notification statute. Importantly, the amendments, which take effect July 24, 2015, (1) expand the statute to cover breaches of non-computerized data; (2) mandate that businesses notify the Washington Attorney General of a breach affecting more than 500 Washington residents; and (3) require that notification to consumers and to the Attorney General occur no later than 45 days after the date of discovery of the breach. The amendments were requested by Washington Attorney General Bob Ferguson.

Washington now joins only a handful of states whose breach notification statutes require notice of a breach of non-computerized data containing consumer personal information. The amendments clarify, however, that notice is only required – both for computerized and non-computerized data – if the breach is reasonably likely to subject consumers to a risk of harm. Risk of harm is assumed, though, if the data is not secured, or if the means to decipher the secured information (*e.g.*, the encryption key) is also compromised. "Secured" is defined as "encrypted in a manner that meets or exceeds the National Institute of Standards and Technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable."

In addition to mandating that notification occur within 45 days of discovery of a breach, the amendments prescribe the content of the notice to both consumers and the Attorney General (if more than 500 Washington residents are affected). Specifically, the consumer notice must be written in plain language and include (1) the business's name and contact information, (2) a list of the types of personal information reasonably believed to have been the subject of the breach, and (3) the toll-free telephone numbers and addresses of the major credit reporting agencies. The notice to the Attorney General must include the number of Washington residents affected and a sample copy of the consumer notice, provided electronically.

Despite pending federal legislation, which contains broad federal preemption provisions, state legislatures, often at the request of the Attorney General, are strengthening existing notification requirements, likely in response to the several high-profile breaches that have occurred over the last few years, to attempt to safeguard consumer personal information and prevent identity theft. We continue to track such legislation in several states, including Indiana and New Jersey, as well as the goals of state attorneys general, such as those in New York and Oregon requesting such legislation.