Washington DC expanding data breach notification law

Dominic A. Paluzzi | Wednesday, June 17, 2020

Washington, D.C. is joining dozens of states that are expanding the applicability of, and the requirements under, their data breach statutes. Importantly, the amendment makes the following changes:

- **Additional data elements triggering a notification.** Additional data elements were added to the definition of "personal information," including: an individual taxpayer number, passport number, military identification number, or other unique identification number issues by a government entity; medication information; genetic and biometric information; health insurance information.
- **Notification letters must include the contact information for the Washington, D.C. Attorney General.**
- **Notification to Washington, D.C. Attorney General required for a breach impacting 50 or more Washington, D.C. residents.**
- **Requires 18 months of identity theft protection for individuals with Social Security number or taxpayer identification numbers impacted.**
- **Establishes data security requirements for any business that owns, licenses, maintains, handles, or possesses the personal information of Washington D.C. residents.** Such businesses are required to have reasonable security safeguards "appropriate for the nature of the personal information and the nature and size of the entity or operation," and to require the same of nonaffiliated third party service providers.

The amendments to the Washington, D.C. statute also partially exempt entities that are giving notice pursuant to the Gramm-Leach-Bliley Act (GLBA) or the Health Insurance Portability and Accountability Act (HIPAA) from the application of the statute.

Importantly, under the revisions of the statute, a business is allowed to perform a risk of harm analysis and not provide notice to Washington, D.C. residents if, "after a reasonable investigation and consultation with the Office of the Attorney General for the District of Columbia and federal law enforcement agencies [that the acquisition of personal information] will not result in harm to the affected individuals."

The amendments to the Washington, D.C. data breach statute, along with the changes in an increasing number of states, are indicators of the increased importance of data privacy law in the U.S. Businesses should ensure that they have adequate data security safeguards and respond appropriately to data security incidents, rather than risk running afoul of the increased state requirements.

If you need assistance analyzing the Washington, D.C. statue, or any other state statute relating to data breach, contact any of the members of McDonald Hopkins' national data privacy and cybersecurity practice.

Dominic A. Paluzzi