Data Breach Notification Law Roundup

Dana B. Rosenfeld, Alysa Z. Hutnik

April 6, 2018

Just when you think you have it all under control, the data breach notification law landscape changes – again. Over the past few weeks, several data breach notification statutes were updated, including an effective date for Canada's mandatory breach notification obligations, as well as the adoption of legislation in the two holdout states (Alabama and South Dakota). Here is the latest:

- ***Canada:*** On March 26, the Governor General in Council, on recommendation of the Minister of Industry, set November 1, 2018, as the effective date for the mandatory data breach notification obligations in the Digital Privacy Act 2015, which amended the Personal Information Protection and Electronic Documents Act (PIPEDA). Beginning November 1, any organization must report to the Privacy Commissioner if it has a reasonable belief that a breach of information under its control creates a real risk of "significant harm" to Canadian residents, as well as notify affected individuals. The term "significant harm" includes bodily harm; humiliation; damage to reputation or relationships; loss of employment, business, or professional opportunities; financial loss; identity theft; negative effects on the credit record; and damage to or loss of property. The notice to affected individuals must contain sufficient information to allow the individual to understand the significance of the breach and to take any steps to mitigate or reduce the risk of any resulting harm.

- ***Alabama:*** On May 1, 2018, the Alabama Data Breach Notification Act will take effect, requiring that companies provide notice of the unauthorized acquisition of electronic data containing sensitive personally identifiable information that is reasonably likely to cause substantial harm. The term "sensitive personally identifiable information" includes an Alabama resident's first name or first initial and last name in combination with Social Security or tax identification number; driver's license or other unique government-issued identification number; financial account number in combination with the required security code, access code, password, expiration date, or PIN; medical and health insurance information; or online account credentials. The Act sets a 45-day time limit for consumer and Attorney General (if more than 1,000 Alabama residents are affected) notice. The consumer notice must contain (1) the estimated date(s) of the breach; (2) a description of the affected information; (3) a general description of the remedial actions taken; (4) a general description of the steps consumers can take to protect themselves from identity theft; and (5) the company's contact information. The Attorney General notice must contain (1) a synopsis of the event surrounding the breach at the time notice is provided; (2) the approximate number of affected Alabama residents; (3) any free services offered to affected individuals, and instructions on how to use those services; and (4) the name, address, telephone number, and email address of the company's point person for the breach. A violation of the Act will constitute an unlawful trade practice under the Alabama Deceptive Trade Practices Act, subject to a civil penalty of up to $5,000 per day.

- ***South Dakota***: On March 21, South Dakota enacted S.B. 62. Effective July 1, 2018, the statute will require that companies provide notice of the unauthorized acquisition of unencrypted computerized data (or encrypted computerized data and the encryption key) that materially compromises the security, confidentiality, or integrity of personal or protected information. The statute (1) contains expanded definitions of personal and protected information, which include health information, an employer-assigned ID number in combination with the required security code, access code, password, or biometric data, and online account credentials; and (2) sets a 60-day time limit for consumer notice, unless legitimate law enforcement needs require a longer timer period. Attorney General notice is required if the number of affected South Dakota residents exceeds 250. Violators are liable for a civil penalty of up to $10,000 per day per violation.

- ***Oregon:*** On March 16, Oregon enacted amendments to its data breach notification law, which take effect June 2, 2018. The amendments clarify that personal information includes an Oregon resident's first name or first initial and last name in combination with any information or combination of information that would permit access to her financial account, and require consumer and Attorney General (if the number of affected residents exceeds 250) notice within 45 days of discovery of a breach. Additionally, if a company provides free credit monitoring or identity theft prevention and mitigation services, it may not require that consumers provide a credit or debit card number (or any fee) to take advantage of those free services. Likely prompted by the Experian data breach, the amendments also prohibit consumer reporting agencies from charging a fee for a consumer to place or lift a security freeze. Previously, the statute capped such fees at $10.

- ***Arizona*****:** On April 5, the Arizona Governor received H.B. 2154, which if enacted, would (1) expand the definition of personal information to include a private key unique to an individual and used to authenticate or sign an electronic record, medical and health insurance information, passport and taxpayer identification number, unique biometric data, and online account credentials; and (2) require notification to affected consumers, as well as the Attorney General and the three largest credit reporting agencies if more than 1,000 Arizona residents are affected, within 45 days. Such notices would need to include the approximate date of the breach; a brief description of the affected personal information; the toll-free numbers for the three largest CRAs; and the toll-free number, address, and website address for the FTC. Importantly, these amendments would also create notice provisions specific to online account credentials and clarify that notice should not be made to the affected account, and should prompt the individual to (1) immediately change her password or security question and answer, and (2) take appropriate steps to protect the affected account and all other online accounts with the affected account credentials. If Arizona adopts these amendments, it will become the twelfth state to require notice in the event of a breach of online account credentials – joining California, Delaware, Florida, Illinois, Maryland, Nebraska, Nevada, Rhode Island, and Wyoming, and most recently, Alabama and South Dakota.

These developments demonstrate that data breach notification statutes are evolving, often in response to high-profile data breaches and/or concerns about a specific industry or a specific type of data – such as online account credentials. We expect U.S. states to continue to update these laws, and in particular, to (1) expand the definition of personal information to include medical and health insurance information, biometric data, and online account credentials; (2) require notice to consumers and/or regulators within a specific time period; (3) impose data security requirements; and (4) address concerns with specific industries, such as credit reporting agencies. Stay tuned for

more updates!