Data Breach Notification Requirements – 2018’s Bumper Crop of Changes

By: Laura L. Ferguson

We have rounded up the latest changes to data breach notification laws. During 2018, there have been several significant revisions to U.S. state data breach notification laws. Also, with the recent enactment of the Alabama data breach law, all 50 states now have data breach notification laws. Below is a brief summary of the developments:

**Alabama:** Effective **June 1, 2018**, Alabama’s data breach notification law will apply to any person or entity that acquires and uses sensitive personally identifiable information of Alabama residents. Sensitive PII is defined as an individual’s first name or initial and last name in combination with (i) non-truncated SSN, (ii) non-truncated drivers’ license number/passport number/military ID number/other unique ID number issued on a government document used to verify identity, (iii) financial account number (bank account, credit card, debit card) with security code/access code/PIN/expiration date, (iv) any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional, (v) an individual’s health insurance policy number/subscriber ID and any unique ID used by the health insurer to identify an individual, and (vi) a user name or email address with password or security question (and answer) permitting access to an online account affiliated with the person/entity that acquires and uses the sensitive PII. Subject to a harm threshold, notification to an affected individual is required as a result of the unauthorized acquisition of electronic sensitive PII. In the event more than 1,000 consumers are being notified, the Alabama Attorney General and consumer reporting agencies must be notified. For the text of this law, click here.

**Delaware:** On **April 14, 2018**, Delaware’s amendment to its data breach notification law took effect, which, among other changes, expands the definition of personal information to include biometric and other health information, imposes a 60-day notice deadline, and requires 1 year of free credit monitoring if an individual’s Social Security number is breached. For the text of the amendment, click here.

**Massachusetts:** On **February 1, 2018**, the Massachusetts Attorney General’s Office rolled out a new online form for submitting data breach notifications, as an efficient alternative to notifying the AG’s office by paper letter or email.

**Oregon:** Effective **June 2, 2018**, Oregon amended its data breach notification law to expand the scope of individuals or entities that are required to report breaches to include individuals or entities that “otherwise possess” personal information, require notice is provided no later than 45 days after discovery (except for HIPAA covered entities), and include biometric and certain other health information in the definition of personal information. For the text of this amendment, click here.

**South Dakota:** Effective **July 1, 2018**, South Dakota’s data breach notification law applies to any person or entity conducting business in South Dakota that owns or licenses computerized personal or protected information of South Dakota residents. “Personal information” includes (i) Social Security number; (ii) driver’s license number or other unique identification number created or collected by a government body; (iii) account, credit card, or debit card number, in combination with any required security code, access code, password, routing number, PIN, or any additional information that would permit access to a person’s financial account; (iv) health information as defined in 45 CFR 160.103; or (v) identification number assigned to a person by the person’s employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication purposes. “Protected information” includes (x) user name or email address, in combination with a password, security question answer, or other information that permits
access to an online account; and (y) account number or credit or debit card number, in combination with any required security code, access code, or password that permits access to a person’s financial account. Subject to a harm threshold, notification to an affected individual and consumer reporting agencies is required as a result of the unauthorized acquisition of unencrypted or encrypted (with the encryption key) computerized personal or protected information. If relying on the harm threshold to avoid notification, notification must be provided to the Attorney General. In the event more than 250 South Dakota residents must be notified, notification to the Attorney General is required. For the text of this law, click here.

Looking outside the U.S., the following key developments are coming into effect:

**Canada**: Recently, an Order in Counsel declared that the federal data breach notification requirements of the Digital Privacy Act of 2015, which amended Canada’s Personal Information Protection and Electronic Documents Act, will go into effect November 1, 2018. The act only applies to companies that are subject to federal regulation, such as banking, broadcasting, telecommunications, interprovincial trucking. In the event of a loss of, unauthorized access to or unauthorized disclosure of personal information that creates a real risk of significant harm to an individual, a company must, as soon as feasible, notify the affected individual(s) and the Privacy Commissioner of Canada regarding the breach. “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 a credit record and damage to or loss of property.” Notifications must also be made to any other organization or government institution if it would help mitigate the potential harm to an individual. Companies must maintain records regarding investigation, notification, and other compliance with the law for a period of 24 months after the date of a breach. Substantial fines of up to $100,000 per day per affected individual can apply for failure to report or maintain records as required by this law. For the text of this amendment, click here.

**GDPR**: U.S. entities trying to determine whether they need to comply with GDPR, with its rapidly approaching effective date of May 25, 2018, can review our prior article for more information.

For more information on the above data breach notification laws, data breach response preparedness, and/or GDPR compliance, please contact any member of Locke Lord’s Privacy & Cybersecurity practice group.

**CYBERSECURITY**

**AUSTIN**
Patrick J. Hatfield | 512-305-4787 | phatfield@lockelord.com

**CHICAGO**
Thomas J. Smedinghoff | 312-201-2021 | tom.smedinghoff@lockelord.com
Molly McGinnis Stine | 312-443-0327 | mmstine@lockelord.com

**HARTFORD**
Theodore P. Augustinos | 860-541-7710 | ted.augustinos@lockelord.com

**HOUSTON**
Laura L. Ferguson | 713-226-1590 | lferguson@lockelord.com

**LONDON**
Andrew Shindler | +44 (0) 20 7861 9077 | andrew.shindler@lockelord.com

For more information, visit www.lockelord.com.