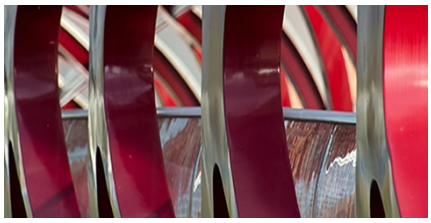
masuda funai



News & Types: Client Advisories

An Overview of U.S. Data Breach Notification Laws

10/8/2020

By: Kenton P. Knop

Practices: Commercial, Competition & Trade, Intellectual Property & Technology

EXECUTIVE SUMMARY

In recent years, news of large-scale breaches of customer data held by retailers such as Target and The Home Depot, followed by class action litigation brought by the affected customers, has become commonplace and has led to intensifying demand for robust data protection laws in the United States. Unlike other jurisdictions with uniform data protection laws such as the European Union's General Data Protection Regulation (GDPR), the United States lacks an overarching federal data protection statute. Instead, a loose patchwork of state and federal legislation forms the current body of U.S. data protection law. So far, data protection laws in the U.S. have taken several different forms, including state website privacy policy laws (such as the California Online Privacy Protection Act (CalOPPA)), state general privacy laws (such as the California Consumer Privacy Act (CCPA)), Washington's new privacy law and the Illinois Biometric Information Privacy Act), state data breach notification laws, and federal statutes providing for protection of specific types of information.[1] Of these different approaches to data protection, data breach notification laws have reached a particularly high level of adoption in the U.S., with all 50 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands having passed data breach notification laws as of 2020.[2] The purpose of data breach notification laws is to place affirmative obligations on entities holding certain personal data of individuals to provide timely notification of breaches to the individuals affected, and in some cases require entities to notify relevant state authorities as well. This article is intended to promote awareness of these data breach notification laws, and to highlight certain aspects of these laws.

WHAT KINDS OF DATA ARE COVERED?

Data breach notification laws concern "personal information" or "personally identifiable information" ("PII") of individuals, which is generally defined as an individual's first name/initial and last name in combination with unencrypted sensitive data such as a social security number, driver's license number, bank account number or credit/debit card number, medical or health insurance information, or a computer user name and password. A common, but narrow, exception to the definition of PII in some states is publicly-available information that is lawfully made available to the general public from federal, state or local government records.

WHAT ENTITIES ARE COVERED?

Generally, data breach notification laws apply to persons or businesses that own or license computerized data that includes PII. In addition, service providers that maintain computerized data on behalf of the data's owner or licensee are also generally covered under data breach notification laws, and would be required to notify the data's owner in the event that the service provider sustains a breach.

WHAT IS A BREACH?

Generally, a "breach" is defined as an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PII maintained by the person or business. A breach may occur either through digital means such as unauthorized access to a business's computer system through hacking, or physical means such as the theft of company property containing PII. Additionally, many states' laws include a "risk of harm" analysis, under which the notification requirement is triggered if the perceived risk of harm from a breach reaches a certain threshold.

WHO MUST RECEIVE NOTICE OF A BREACH?

Each state's data breach notification law functions to protect the residents of their respective states. Under each state's data breach notification laws, a resident of a state must receive notice of the breach according to the law of that particular state. Therefore, a data breach affecting residents located in all 50 states, the District of Columbia and the U.S. territories could potentially require 50 or more different versions of notices that comply with each jurisdiction's particular requirements.

In addition, some states also require that notice be given to the state attorney general or other state authorities in the event that the breach affects a certain number of that state's residents, usually 500 residents or more. However, some states requiring notification to state authorities do not have a minimum threshold amount of affected residents, meaning that a breach affecting a single resident in that state will also require giving notice to the relevant state authorities.

WHEN MUST NOTICE BE GIVEN?

The notice timing requirement varies widely among the states and demands a close review of the applicable individual state laws. The most common provision is that notification must be given "in the most expedient time possible and without unreasonable delay" following discovery or notification that a breach occurred. However, some states impose a strict requirement to provide notice within a certain time period after discovery of the breach, which may be as short as 30 days (Colorado, Florida, Washington), or as long as 90 days (Connecticut), with a 45-day notification period being most common among the remaining states. In addition, many states' laws allow for delay of notice subject to investigations by law enforcement and to restore the reasonable integrity of the data system.

HOW MUST NOTICE BE GIVEN?

The laws in all 50 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands allow for notice to be given by written letter. Individual states differ on whether additional forms of notice, such as by telephone or by electronic means are acceptable. In addition, some states allow for "substitute notice" to be given in certain circumstances if the business can demonstrate that the cost of providing notice would exceed a certain amount (such as $250,000 in the case of Illinois), that the class of affected persons to be notified exceeds a certain number (such as 500,000 in the case of Illinois), or if a data collector (business) does not have sufficient contact information for the persons affected. In Illinois, substitute notice requires an email notice to be sent to affected persons, a conspicuous posting on the business's Internet web site for a minimum of 30 days, and notification to major statewide media.

WHAT MUST THE NOTICE INCLUDE?

Each state's law differs on what specific information the notice must include. Illinois requires for the notice to include, at a minimum, contact information for the three major consumer reporting agencies (Equifax, Experian and TransUnion) and the Federal Trade Commission, and guidance that an individual can obtain information from these agencies about obtaining fraud alerts and security freezes. Other states such as California contain more detailed requirements for the format and contents of the notice. In addition, California requires businesses to offer affected individuals at least 12 months of free credit monitoring services, and Connecticut recently amended its law to require businesses to offer at least 2 years of free credit monitoring services to affected individuals.

WHAT ARE THE PENALTIES FOR NON-COMPLIANCE?

Each state's law provides for an enforcement mechanism, either under the data breach notification law itself or a related consumer protection statute. In several states, a violation of the applicable data breach notification law is considered an unfair or deceptive trade practice that may be enforced by a state attorney general or other government authority and subject a business to civil penalties. Some states such as California allow for affected individuals to have a private right of action to sue a business directly. For example, the California Consumer Privacy Act allows California residents whose PII is disclosed in a data breach to claim statutory damages of up to $750 per resident per incident or actual damages, whichever is greater, and individual residents may combine their claims into a class action. Illinois provides for both enforcement by the Illinois State Attorney General, as well as a private right of action for Illinois residents.

CONCLUSION

As of the writing of this article, there appears to be some indications that Congress may again consider implementing new federal data privacy legislation. In the meantime, businesses and practitioners will need to contend with the current patchwork of federal and state laws in the event of a data breach. Due to the increased complexity and challenge in responding to a data breach arising from the differences between the

various state data breach notification laws, the most important consideration is swift action in compliance with the applicable law(s) once the breach is discovered. By quickly identifying the information disclosed in a breach and the individuals affected so that prompt notice can be sent, a business can help contain and reduce the risks of its customers or employees falling victim to fraudulent transactions and identity theft, as well as mitigate its own risks of litigation from customers or employees affected by the breach. In today's digital world in which a data breach can occur at any time to any business, every business needs to have a plan for how it will respond to a data breach and then train its employees to identify and report a breach when it occurs. With these steps in place, businesses can be confident that they are doing everything possible to safeguard the personal data of their customers and employees in compliance with the law.

[1] Examples of federal data privacy and protection laws are: HIPAA (Health Insurance Portability and Accountability Act), which protects individuals' medical and other health information; GLBA (Gramm-Leach-Bliley Act), which requires financial institutions to protect their individual customers' personal and financial information; and COPPA (Children's Online Privacy Protection Act), which protects the personal information of children under 13 years of age.

[2] For the purposes of this article, the 50 U.S. states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands will be referred to collectively as "states" unless otherwise noted.