Breach Notification Statutes: "Um...We Lost Your Social Security Number"

Insights
2.14.11

Employees take and misuse company information for a variety of reasons. Some do it because they want to document what they believe to be unlawful conduct. Others do it because they intend to use it in competition with their soon to be former employers. Regardless of their motivation, when employees misuse customer information, employers must recognize that such misconduct presents more than simply a competitive or employment concern. It also may trigger significant obligations under state breach notification laws.

Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring companies to notify individuals when there is a security breach involving their personal information. These laws are the result of an increasing number of breaches involving personally identifiable information.

California's law is widely recognized as the pioneer, after which a majority of states model their legislation. Although the common attributes of breach notification laws are discussed in detail below, employers must recognize that the laws vary by state, sometimes in significant ways. If your company experiences a data breach involving individuals in more than one state, it is imperative that you examine your obligations in each state as they may, and often will, be different and will require cumulative and concurrent action.

Breach notification laws commonly include: (1) A section defining the scope and nature of information covered by the law; (2) A section specifying events and conditions triggering obligations

under the law; and (3) A section defining obligations under the law in the event action is required.

Scope and Nature of Information Typically Covered by Breach Notification Laws

Breach notification laws typically require any person or business conducting business within a state to notify individuals if their "personal information" was, or reasonably is, believed to have been acquired by an unauthorized person. "Personal information" is commonly defined to include an individual's name combined with a certain "data element" such as a Social Security number, driver's license number, or account number in combination with any password that would permit access to a person's account. In the vast majority of states, the application of breach notification laws is limited to computerized data that contains personal information, and even then, only if the computerized data is unencrypted. In a small handful of states, breach notification obligations may be implicated if personal information in paper records is the subject of a breach.

Events and Conditions Triggering Breach Notification Obligations

Breach notification laws typically apply if "personal information" is acquired by an unauthorized person or in the event that there is a breach of the security of the system. A "breach" is considered to have occurred when someone acquires computerized data that compromises the security, confidentiality or integrity of personal information. Many states require action only if the breach creates a heightened risk of harm to an individual such as identity theft, potential fraud or some other type of economic harm.

When and What Type of Notice is Required?

If a company determines that a breach requiring notice has occurred, the questions that arise include when and how must notice be given? Generally speaking, notice must be given as expeditiously as possible without unreasonable delay, although, notice may be delayed if providing notice would interfere with a law enforcement investigation. A few states have bright line rules setting forth a specific number of days within which notice must be provided.

Most statutes provide some flexibility concerning the type of notice that must be provided. Written notice is the standard approach, with many states allowing electronic notice if such notice is provided in a manner consistent with the Electronic Signatures in Global and National Commerce Act (commonly known as the E-SIGN Act). A few state permit telephone notice.

Under certain circumstances, such as breaches involving an unusually large numbers of individuals, or where costs of notification may be beyond the resources of a small business, substitute notice is permitted. Substitute notice generally requires email notice if possible, conspicuous posting of notice on a company's website, and notification to a major statewide media outlet.

A handful of states require that notice must also be given to state authorities in addition to those individuals whose information was the subject of a breach.

Surprisingly, most state statutes do not specify exactly what must be stated in notice, however, the states that do so serve as useful guidance. Generally, they provide that notice must describe the breach incident, the type of personal information that was placed at risk, and the steps that the company has taken to minimize or prevent further risk. It is also commonly required that notice should include a telephone number that the individual can call with questions or to seek further guidance, as well as a reminder that individuals should exercise diligence in monitoring their accounts and finances such as credit reports to determine whether the breach has resulted in any specific harm.

Practical Steps

In the face of an information security breach, prompt action is required. Because the scope and nature of a breach cannot likely be determined in advance, companies would be well served to develop response plans. Response teams should be assembled and consulted, including IT and human resources personnel, and legal counsel. Teams should be prepared to investigate and ascertain the scope of breaches when they occur. Investigations should be comprehensive, documented, and expeditious. And as noted above, the state-specific requirements must be identified and observed.

*Michael R. Greco is a partner in the Employee Defection & Trade Secret*s Practice Group at Fisher Phillips. To receive notice of future blog posts either follow *Michael R. Greco on Twitter or on LinkedIn or subscribe to this blog's RSS feed.*

Related People

Michael R. Greco
Regional Managing Partner
303.218.3655
Email

Email