Insight

IN-DEPTH DISCUSSION

NOVEMBER 4, 2015

Recent Amendments to Security Breach Notification Laws Further Complicate Breach Notification for Employers

BY PHILIP GORDON AND JENNIFER MORA

It is not a matter of "if" but "when" an employer will be required to notify employees of a security breach. Forty-seven states require employers to notify employees when defined categories of personal information, including Social Security numbers, are acquired by unauthorized parties, and every employer maintains SSNs. At the same time, security breaches are rampant. According to the Privacy Rights Clearinghouse's Chronology of Data Breaches, more than 1,000 breaches, implicating more than 280 million records, have been publicly reported since January 2013.

For multi-state employers, the multitude of breach notification laws complicates the employer's response to a security breach because common practice calls for compliance with the breach notification law of each state where affected individuals reside. In 2015, that undertaking has become even more complicated as eight states enacted amendments to their breach notification laws, adding new and unique requirements. It is critical for employers to be aware of these recent changes, which we discuss in detail below, to ensure their response to a security breach fully complies with applicable law.

California Now Requires a Specific "Form" of Notice

In October 2015, California became the first state to mandate a specific form to notify individuals of a security breach. The amendment requires the breach notification to be titled, "Notice of Data Breach," and requires the entity to provide information about the breach under each of the following headings:

- What Happened
- What Information Was Involved
- What We Are Doing
- What You Can Do
- Other Important Information
- For More Information

This standard form creates practical problems for employers addressing a multi-state breach. Other states require that the breach notification include information in addition to, or different from, California's mandate. For example, employers in Massachusetts and Rhode Island must inform individuals of their right to obtain a police report, and Wyoming employers must state whether law enforcement requested the employer to delay the notification. As a result, multi-state employers will find it difficult to draft a single notification that satisfies California's new notification law as well as all other notification laws.

Reporting a Security Breach to the State's Attorney General

As of the end of 2014, 18 states required a report to the state's attorney general when an entity experiences a security breach—in addition to the notice to affected individuals. This requirement creates significant risk for employers because the report potentially exposes the employer to an administrative investigation and penalties. While most of the 18 states require reporting any breach, regardless of the number of affected individuals, a handful require reporting only if the number of affected individuals exceeds a certain threshold, such as 1,000 affected individuals in Hawaii and 500 affected individuals in Florida.

In 2015, five additional states—Montana, North Dakota, Oregon, Rhode Island and Washington—amended their breach notification law to require entities to report a breach to state regulators. Falling in with the majority of states, Montana's reporting requirement applies regardless of the number of affected Montana residents. In North Dakota and Oregon, the reporting requirement applies only if the breach involves more than 250 state residents, and Rhode Island and Washington set a reporting threshold of 500 affected state residents. These reporting requirements already have gone into effect in Montana, North Dakota, and Washington, and will go into effect on January 1, 2016, in Oregon and on July 2, 2016, in Rhode Island. Like the other breach notification laws that require a report to state authorities, these new laws require employers to notify the state and affected individuals contemporaneously.

State Amendments Expand the Categories of "Trigger Information" Requiring Notice

When an employer discovers a security incident, one critical question is whether the compromised information triggers breach notification requirements. All breach notification laws define the categories of "trigger information" to include, at a minimum, first name or initial and last name in combination with Social Security number, driver's license or state identification number, or credit or debit card number or financial account number coupled with any required security code. In the last few years, many states have expanded this definition to include other categories of information, most commonly health information and health insurance information.

In 2015, four states expanded the categories of information that constitute trigger information, thereby increasing the risk that a security incident will result in breach notification obligations. Effective October 1, 2015, Montana law now includes medical record information, taxpayer identification number, or identity protection personal identification number issued by the Internal Revenue Service as trigger information. Effective July 1, 2015, Nevada added the following to its list of trigger information: medical identification number; health insurance identification number; or a user name, unique identifier or email address in combination with a password, access code or security question and answer that would permit access to an online account. Effective January 1, 2016, Oregon's security breach law will add the following categories of trigger information:

- Health insurance policy number or identification number;
- An individual's medical history, condition, diagnosis, or treatment; or
- Data from automatic measurements of an individual's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the individual's identity in the course of a financial transaction or other transaction.

Effective July 2, 2016, Rhode Island law expands its list of "trigger information" to include (1) medical or health insurance information, and (2) an email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance or financial account.

Connecticut Entities Are Now Required to Offer Identity Protection Services to Affected Individuals

Entities that experience a security breach routinely offer identity protection services to affected individuals even in the absence of a legal requirement. Motivations vary, but chief among them are a sense of obligation to affected individuals, concern about public and/or employee relations, and the desire to reduce the likelihood that affected individuals will sue.

Until late 2014, no jurisdiction required companies to offer this benefit to affected individuals. On September 30, 2014, California became the first state requiring businesses to provide free identity protection services to affected individuals, but only for one year and only for breaches involving an individual's Social Security number – information that almost all employers maintain on their employees.

In 2015, Connecticut followed California's lead. Under the amendment to Connecticut's notification law, entities must provide identity protection services to residents affected by a security breach involving their Social Security number or driver's license number. Such services must be provided at no cost to affected residents for a period of not less than 12 months. The covered entity must provide in the breach notification all information necessary for affected residents to enroll in the services and how to place a credit freeze on his or her credit file.

Some States Impose Strict Deadlines for Notifying Affected Individuals of a Breach

Most security breach notification laws provide a flexible deadline for notifying affected individuals, typically "as soon as reasonably practicable" or "without unreasonable delay." A few states, however, impose strict deadlines. Ohio, Vermont, Washington, and Wisconsin require notice within 45 days of discovery, and Florida requires notice within 30 days.

In 2015, three states set hard deadlines. Washington requires notice within 45 days after discovery, and the same deadline will apply in Rhode Island, effective July 2, 2016. In addition, Connecticut now requires notice within 90 days of discovery of the breach.

Recommendations for Employers

The amendments to breach notification laws in 2015 have increased the risks, and potential costs, associated with a security breach for employers with employees in California, Connecticut, Montana, Nevada, North Dakota, Oregon, Rhode Island, and Washington. Employers in other jurisdictions should expect similar amendments in coming years as other legislatures follow the trend towards requiring reports to the state's attorneys general, expanding the categories of "trigger information," mandating offers of free identity protection services, and setting hard deadlines for breach notification. The time to grapple with these security breach notification requirements is not under the extreme pressure of a security breach response. Instead, employers should prepare for a security breach well before it occurs by, among other things, (a) reviewing, and if necessary enhancing, their administrative, physical and technical safeguards for personal information; (b) establishing a security incident response team; (c) developing a security incident response plan; (d) negotiating agreements with identity protection services and other vendors that support security incident response, such as printing and mailing and call center providers; (e) developing template notification letters; and (f) conducting simulations to test the effectiveness of the incident response plan.