Insight

IN-DEPTH DISCUSSION

SEPTEMBER 23, 2016

Four States Expanded Employer Data Breach Notification Obligations in 2016

BY PHILIP GORDON, JENNIFER MORA AND KWABENA APPENTENG

With over 680 security breaches reported so far in 2016,[1] more employers are being forced to confront the issue of how to respond to a breach. All states except Alabama, South Dakota and New Mexico now require notification when information commonly maintained by employers, such as Social Security numbers and driver's license numbers, is compromised. While many of these breach notification laws were initially modeled after California's pioneering 2002 breach notification statute, more and more states are amending their notice laws in different ways, increasing the complexity of security incident response for multi-state employers.

Following on amendments by eight states in 2015,[2] four states—Illinois, Tennessee, California, and Nebraska—reinforced their data breach notification statutes in 2016. For employers, the net impact of these amendments is an increased number of circumstances in which they must inform employees, customers, or other state residents whose personal information has been compromised (and, in some cases, the state's attorney general) of a data breach. The following Insight highlights the key amendments to these laws in Illinois, Tennessee, California and Nebraska, of which employers should be aware.

1 Identity Theft Resource Center Data Breach Report, September 20, 2016..

2 These states were California, Montana, South Dakota, Oregon, Rhode Island, Washington, Connecticut, and Nevada. See Philip Gordon and Jennifer Mora, *Recent Amendments to Security Breach Notification Laws Further Complicate Breach Notification for Employers*, Littler Insight (Nov. 4, 2015).

A Breach of Encrypted Information Can Now Trigger a Notification Obligation

Tennessee Now Requires Notification of a Breach Within 45 Days, Even if the Compromised Personal Information is Encrypted

In March, Tennessee made its data breach notification law the strictest in the country by requiring Tennessee residents to be informed of a data breach, regardless of whether the compromised information is encrypted. Effective July 1, 2016, the Tennessee Code now defines a breach as any "unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder."[3] Personal information is defined as an individual's first name or first initial and last name, in combination with the individual's: : (1) Social Security number (SSN); (2) driver's license number; or (3) information that would permit access to a financial account.

Prior to this amendment, Tennessee, like all other states with data breach laws, required notification of a data breach only if the compromised personal information was unencrypted. Tennessee is now the only state in the country that requires notification of a breach of encrypted personal information.

Tennessee coupled this expansion of the notification obligation with a reduction in the period of time in which a Tennessee resident must be informed of a breach. Tennessee now requires notification within 45 days from the discovery of the breach, or notification by a service provider that it has discovered a breach. This 45-day period can be tolled to enable law enforcement to complete a criminal investigation.

Lastly, the amendments to the Tennessee Code clarified that its notification requirement encompasses situations where an employee who may have authority to receive or obtain personal information, intentionally uses the personal information for an unlawful purpose.

Illinois, California and Nebraska Require Notification of a Breach if the Encryption Key is Disclosed in the Breach

Without going as far as Tennessee, Illinois, California and Nebraska also enacted amendments to their data breach notification laws that limit the ability to avoid notification because the compromised personal information was encrypted or redacted. Under these states' amended laws, if encrypted or redacted personal information is breached, notification is still required if information needed to unencrypt or unredact the personal information is acquired with the encrypted personal information. All of these states define "personal information" to include, among other things, an individual's SSN, driver's license number, and information that would permit access to the individual's financial account. This situation could arise, for example, if a hacker obtains a decryption key along with an encrypted file containing personal information.

Illinois and Nebraska Expand Categories of Trigger Data

Illinois and Nebraska join California, Florida, Nevada, and Wyoming in deeming log-in credentials to be personal information, the compromise of which triggers breach notification obligations ("trigger data").

3 Tenn. Code § 47-18-2107(a)(1).

In June, Illinois enacted several amendments to its data breach notification law, titled the Personal Information Protection Act (PIPA). Set to take effect on January 1, 2017, the amended version of PIPA expands the categories of trigger data to include:

- Health insurance information;
- Medical information;
- Unique biometric data; and
- An individual's user name or email address, in combination with a password or security question and answer that would permit access to an online account, i.e., log-in credentials.

The amendments to PIPA provide that an entity that suffers a breach involving an Illinois resident's log-in credentials can notify the Illinois resident of the breach in electronic form. The notice must direct the individual to "promptly change his or her user name or password and security question or answer."[4]

The amendments to Nebraska's data notification statute, titled the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, which took effect in July 2016, similarly expands the list of trigger data to include "a user name or email address, in combination with a password or security question and answer, that would permit access to an online account."

Nebraska and Illinois Add Obligations to Notify the State's Attorney General of a Breach

Under the amendments to the Nebraska law, where notification of a breach is required to be given to a Nebraska resident, the entity suffering the breach must also notify Nebraska's Attorney General. However, Nebraska does not require that its residents receive notice of a breach merely because trigger data is disclosed; Nebraska requires notification only when, following an investigation, the organization determines that trigger data "has been or will be used for an unauthorized purpose." This likelihood of harm standard ensures that employers will not have to notify the Nebraska Attorney General of every data security incident that occurs.

Illinois also amended PIPA to require notice to the Illinois Attorney General of any data breach that impacts more than 250 Illinois residents. This notice must be provided within the sooner of 45 days of the discovery of the breach, or when notification of the breach is sent to Illinois residents. The notification must detail:

- The types of personal information compromised in the breach;
- The number of Illinois residents affected by the breach at the time of notification;
- Any steps the company has taken or plans to take relating to notification of the breach to affected individuals; and
- The date and timeframe of the breach, if known at the time notification.

4 815 ILCS 530/10(a)(2).

Recommendations for Employers

For multi-state employers in particular, the continual amendments to data breach notification laws create a complex web of obligations, several of which may need to be followed at the same time in the event of a breach. Accordingly, employers should periodically review and, if necessary, update their security incident response plan to keep track of breach response requirements in each relevant state. Employers also should consider doing the following:

- Establish a security incident response team that is trained on how to comply with the data breach notification laws of various states;
- Review, and if necessary enhance, their administrative, physical and technical safeguards for personal information to reduce the risk of a security breach;
- Negotiate agreements with identity protection services and other vendors that support security incident response, such as printing and mailing and call center providers, in advance of a breach;
- Develop template notification letters; and
- Conduct simulations to test the effectiveness of the incident response plan.