Insight

IN-DEPTH DISCUSSION

April 24, 2017

Security Breach Notification Becomes More Complex For Employers

BY PHILIP L. GORDON AND JOON HWANG

With new and sophisticated schemes perpetrated by hackers and scammers, and sensitive personal information becoming increasingly accessible to numerous insiders, it is only a matter of time before most employers will be required to notify employees of a data breach. According to a report released by the Identity Theft Resource Center, the number of U.S. data breaches tracked in 2016 reached an all-time high of 1,093, an increase of 40% over the near-record high of 780 reported data breaches in 2015.

For all employers, and particularly multi-state ones, the state breach notification laws complicate the employer's response to a security breach because an appropriate response requires compliance with the breach notification law of each state where affected individuals reside. This web recently became even more entangling as New Mexico became the 48th state to enact a data breach notification law, Virginia took the lead in expanding its law to address the recent explosion of W-2 phishing scams,[1] and Tennessee once again amended its breach notification statute. This Insight explains New Mexico's new law as well as the amendments to Virginia's and Tennessee's data breach notification laws.

New Mexico Becomes the 48th State to Enact a Data Breach Notification Law

On April 6, 2017, New Mexico joined 47 other states when Governor Susana Martinez signed the Data Breach Notification Act into law.[2] The new law is similar, in many respects, to other data breach notification laws. However, New Mexico's law has some unique aspects that cannot be overlooked.

---

1 *See* Philip L. Gordon, *It's W-2 Phishing Season: How to Stop, and Respond to, Tax-Related Identity Fraud Aimed at Your Organization's Employees*, Littler Insight (Mar. 7, 2017).

2 The only states remaining without a data breach notification law are Alabama and South Dakota.

Like most states, New Mexico defines a security breach to be the unauthorized acquisition of unencrypted, computerized, personal identifying information. "Personal identifying information"—the compromise of which triggers breach notification obligations—is defined to include, as in all other states, the individual's first name or initial and last name in combination with any of the following data elements: (a) social security number; (b) driver's license number or other government-issued identification number; or (c) account number or credit or debit card number with any required security code. New Mexico's definition of personal information also includes "biometric data," such as fingerprints, voice prints, and iris or retina scans.

Even when a security incident satisfies the new law's definition of a "security breach," notification is required only if, after an appropriate investigation, the employer determines that that there is "a significant risk of identity theft or fraud." A substantial majority of states have a similar materiality standard. New Mexico is one of a handful of states that imposes a set, maximum time period for notification to affected individuals, namely, 45 days from the date of discovery. Notification may be delayed at the request of law enforcement.

The notification to affected individuals must address at least seven elements enumerated in the statue. These elements include: (1) the name and contact information of the notifying person; (2) a list of the types of personal identifying information subject to a security breach, if known; (3) the date or estimated date of the breach, if known; (4) a general description of the incident; (5) the toll-free telephone numbers and addresses for Equifax, Experian, and TransUnion (collectively, "the nationwide credit bureaus"); (6) advice that directs the recipient to review personal account statements and credit reports to detect errors resulting from the security breach; and (7) advice that informs recipients of their right to place a fraud alert on their credit account.

In addition to notifying individuals, a compromised employer must notify New Mexico's attorney general and the nationwide credit reporting agencies when more than 1,000 state residents are affected. This notice also must be delivered within 45 days of the date of discovery. The notice to the attorney general must include the number of affected state residents and a copy of the notice sent to affected individuals.

New Mexico's new law—like the notice law in California, Texas, and Massachusetts—also contains data protection provisions. Specifically, the new law requires data owners to "implement and maintain reasonable security procedures and practices [for personal identifying information] appropriate to the nature of the information to protect the personal identifying information from unauthorized access, destruction, use, modification or disclosure." When personal identifying information of New Mexico residents is disclosed to a service provider pursuant to a contract, the service agreement must impose similar data protection provision requirements. Finally, the new law requires secure destruction of personal identifying information.

Although the law does not create a private cause of action, the state's attorney general may request an injunction and damages, up to $150,000. Consistent with the data breach notification laws of many other states, financial institutions subject to the Gramm-Leach-Bliley Act (GLBA) and entities covered by the Health Insurance Portability and Accountability Act (HIPAA) are not required to comply with New Mexico's Data Breach Notification Act because they are already subject to breach notification requirements promulgated pursuant to those laws. New Mexico's law will go into effect on June 16, 2017.

Virginia Amends its Data Breach Notification Law to Address Heightened Risk of W-2 Phishing Scams

Virginia has expanded its data breach notification statute in response to the significant increase in W-2 phishing scams.[3] This expansion – the first of its kind – specifically requires that employers and payroll service providers notify the Commonwealth's attorney general if they discover, "unauthorized access and acquisition of unencrypted and unredacted computerized data containing a taxpayer identification number

3 *See* note 1, *supra.*

in combination with the income tax withheld for that taxpayer" and the "the employer or payroll provider reasonably believes [this breach] has caused or will cause, identity theft or other fraud."[4] The notice must include the employer's name and federal employer identification name.

Scammers typically will use this information to file false tax returns in order to receive a false tax refund. In an effort to thwart the scammers, the attorney general's office will inform the Department of Taxation of the compromised employer. The Department of Taxation can then use this information to flag taxpayers whose W-2 information might be misused to obtain a false tax return.

Tennessee Clarifies that "Encrypted Data" Does Not Trigger Breach Notification Requirements

Tennessee's lawmakers have amended the state's data breach notification law for the second time in less than a year. Tennessee's original data breach notification law, enacted in 2005, included an encryption safe harbor by omitting encrypted data from the definition of "personal information," in line with the data breach notification laws of all other states. This exemption meant that a breach of encrypted data would not trigger any notification requirements.

In March 2016, Tennessee amended its data breach notification law in a way that seemingly jettisoned this encryption safe harbor,[5] or at the very least, created considerable confusion as to whether a compromise of encrypted data was, or was not, exempt from notification requirements. Specifically, the 2016 amendment removed "unencrypted" from the definition of a "breach of security of the system," but retained the reference to encryption in the definition of "personal information."[6] The latest amendment, effective April 1, 2017, clarifies that Tennessee's data breach notification law does not apply to "information that has been encrypted in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2 if the encryption key has not been acquired by an unauthorized person."[7]

Recommendations for Employers

Data breach notification laws continue to evolve and expand in their attempt to adapt to heightened risks associated with increasingly sophisticated hacks and scams to gather personal information. Consequently, employers should monitor the laws in the states where their employees reside for new developments. In addition, employers should consider (a) designating a security incident response team; (b) implementing a security incident response plan that is periodically updated to address legislative changes; (c) reviewing and enhancing their administrative, physical and technical safeguards for personal information to reduce the risk of a security breach; (d) negotiating agreements with identity protection services and other vendors that support security incident response, such as printing, mailing and call center providers, in advance of a breach; (e) developing template notification letters; and (f) conducting drills and/or simulations to test the effectiveness of the incident response plan.

4 Va. Code Ann. § 18.2-186.6 (M).

5 *See* Philip L. Gordon, Jennifer L. Mora, and Kwabena A. Appenteng, *Four States Expanded Employer Data Breach Notification Obligations in 2016*, Littler Insight (Sept. 23, 2016).

6 *See* S.B. 2005/H.B. 1631, available at http://www.capitol.tn.gov/Bills/109/Bill/SB2005.pdf.

7 *See* S.B. 547, available at http://www.capitol.tn.gov/Bills/110/Bill/SB0547.pdf.