CYBERSECURITY AND DATA PRIVACY

TENNESSEE ADDS TECHNICAL REQUIREMENTS TO ITS DATA BREACH NOTIFICATION LAWS

by Justin L. Root and Sara H. Jodka

Are you doing business in Tennessee? Do you have computerized personal information about anyone in Tennessee (including employees, clients, or customers)? Are you encrypting that data in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2? If you answered "yes" to the first two questions, then you need to also know the answer to the third.

On April 4, 2017, Tennessee Governor Bill Haslam signed into law an amendment to the state's data breach notification statute. The amendment does two things: (1) it adds technical requirements to the state's notification safe harbor for encrypted data, and (2) it clarifies the notification deadline to be either 45 days after the breach discovery, or 45 days after a law enforcement agency investigating the incident determines that notification will not compromise a criminal investigation.

The law applies to any person or business conducting business in Tennessee that owns or licenses computerized "personal information," except entities subject to Title V of the Gramm-Leach-Bliley Act of 1999 or the Health Insurance Portability and Accountability Act of 1996 as expanded by the Health Information Technology for Clinical and Economic Health Act. "Personal Information" is defined as a person's first name or initial and last name combined with a social security number, driver license number, or any account, credit card, or debit card number with access code or password that would permit access to an individual's financial account.

Under the law, if an unauthorized person acquires unencrypted computerized data (or encrypted computerized data and the encryption key) in a manner that "materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder," the notification obligation is triggered.

While the encryption safe harbor sounds easy enough, it is not, and to take advantage of it the following conditions must be met.

1. The data compromised must have been encrypted. Although that seems relatively straightforward, the nature of the data breach could result in the extraction of data from a live system in an unencrypted form even if that data is normally kept encrypted. For example, many retail businesses use point-of-sale (POS) devices to process credit card transactions. While those systems process the credit card transaction, the information is held temporarily in the POS's random access memory (RAM) in an unencrypted form. Certain malware, known as RAM-scraping malware, can capture this information in cleartext, which would deprive the affected information holder of the encryption safe harbor in the event of a data breach.

2. Even if the data is encrypted, the statute now requires that the encryption protocol in use be "in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2." This means not only that information holders must encrypt the data in their possession, but they must also have a sufficient understanding of the encryption technology being used to protect the data. Continuing the POS example above, if a company's POS system transmits data wirelessly, and if the wireless signal is secured with an inferior encryption technology (such as the wired equivalent privacy (WEP) encryption technology available on many wireless routers), the statutory safe harbor provision would likely not apply because WEP does not provide FIPS 140-2 compliant encryption.

3. Even if the other two conditions are satisfied, the safe harbor does not apply if the encryption keys are compromised. This means that if the passwords to decrypt the data are stored in unencrypted files that are part of the compromised data set, or if they are written on sticky-notes stuck to a computer that is stolen, the information holder will still be obligated to make notifications. Moreover, because encryption keys can be pulled from RAM on a compromised computer system, the nature of the data breach could again dictate whether the encryption-based notification safe harbor applies.

Takeaways

So how would an information holder even know if the encryption-based safe harbor provision applies? Although it can be challenging, it is important to get the legal and technical analyses right because a violation of Tennessee's data breach notification law could give rise to a private cause of action allowing affected individuals to bring suit for injunctions and damages. It is best to know where you stand before an incident occurs.

After a data security incident, attempting to satisfy all of your statutory or regulatory obligations within the statutorily-proscribed timeframe, including determining what was compromised and how, is an overwhelming task, especially if you have not already positioned yourself to respond to such an incident.

To be properly positioned, information holders should proactively adopt and regularly review tailored data security policies and written information security programs; implement and practice incident response plans; designate and train members of an incident response team; and establish ongoing relationships with law enforcement agencies, incident response forensics companies, and legal counsel experienced in cybersecurity and data breach response. If applicable, cybersecurity liability insurance should also be considered to help mitigate the costs associated with responding to a data breach.

By putting appropriate processes in place ahead of time, information holders can dramatically reduce the likelihood of data security incidents occurring, decrease the time spent investigating and responding to an incident, reduce the costs associated with a breach response, and more quickly identify legal rights and obligations. Proper preparation, although necessitating some up front effort and expenditures, will ultimately result in overall cost, time, and energy savings should a data security incident occur, and allow information holders to return to normal operations as quickly and efficiently as possible. If you are not sure when you last reviewed and updated your applicable policies, Dickinson Wright's cybersecurity and data privacy attorneys encourage you to do so today.

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of Cybersecurity and Data Privacy law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Justin L. Root is Of Counsel in Dickinson Wright's Columbus office. He can be reached at 614.591.5465 or jroot@dickinsonwright.com.

Sara H. Jodka is Of Counsel in Dickinson Wright's Columbus office. She can be reached at 614.744.2943 or sjodka@dickinsonwright.com.