THOMPSON HINE

Privacy & Cybersecurity Update

May 2024

Tennessee Enacts Data Breach Class Action Safe Harbor

On May 21, Tennessee Governor Bill Lee signed into law House Bill (HB) 2434, which provides a legal safe harbor for businesses that are victims of data breaches. Given the sophistication of today's criminal cyber actors, a data breach can impact even the best-prepared business. Unfortunately, a business that falls victim to a cybersecurity event may itself become the target of litigation or government enforcement actions. Accordingly, with HB 2434, Tennessee joins the growing number of states seeking to provide legal protections to businesses that suffer data breaches and to deter frivolous litigation. The law goes into effect immediately.

Tennessee Data Breach Safe Harbor

HB 2434 provides that a "private entity is not liable in a class action lawsuit resulting from a cybersecurity event," provided the event was not "caused by willful and wanton misconduct or gross negligence on the part of the private entity."

Interestingly, the law does not limit the type of class action claims affected by the safe harbor. Given that most data breach-related class actions allege negligence, breach of contract, and invasion of privacy-type claims, the reach of the safe harbor likely is very broad. In addition, unlike other data breach safe harbor laws, HB 2434 does *not* prescribe any specific information security standard or program the private entity must satisfy or establish to be afforded the legal safe harbor. However, Tennessee has enacted other laws related to the safe disposal of sensitive personal information and security control requirements for the protection of consumers' personal information.

Key Terms

The law defines a "cybersecurity event" broadly as an "event resulting in unauthorized access to, or disruption or misuse of, an information system or nonpublic information stored on an information system." Accordingly, it could apply to ransomware attacks, business email compromises, or stolen devices containing accessible protected information.

The term "nonpublic information" means "information that is not publicly available and concerns a person that, because of a name, number, personal mark, or other identifier, can be used to identify that person, in combination with":

- A Social Security number
- A driver's license number or non-driver identification card number
- A financial account number or credit or debit card number
- A security code, access code, or password that would permit access to the person's financial accounts
- Biometric records

Interestingly, this definition includes types of personal data that are not included in Tennessee's data breach notification statute, but does not cover all the various types of data that may trigger notification obligations under various federal and state personal data breach notification laws, such as passport numbers, military identification numbers, dates of birth, health data, and online accounts and passwords.

Further, the law defines an "information system" as either a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic nonpublic information; or a specialized system, including an industrial or process control system, a telephone switching and private branch exchange system, or an environmental control system.

The term "private entity" means "a corporation, religious or charitable organization, association, partnership, limited liability company, limited liability partnership, or other private business entity, whether organized for-profit or not-for-profit," and therefore HB 2434 will cover several different types of private-sector organizations.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Thora Knight, Ph.D.
212.908.3971
Thora.Knight@ThompsonHine.com

Marla M. Izbicky
312.998.4253
Marla.Izbicky@ThompsonHine.com
Certified Information Privacy Professional/United States (CIPP/US)