Ohio Enacts Law Acknowledging Blockchain Transactions and Granting Safe Harbor Protections to Eligible Businesses from Data Breach Claims

Aug 09, 2018

Categories:

Blockchain and Digital Assets
Blogs
Publications
Technology Blog

Authors:

Michael E. Nitardy

On Friday, August 3, Governor Kasich signed Ohio Senate Bill 220, which acknowledges for the first time the legitimacy of blockchain transactions as enforceable electronic transactions and creates an affirmative defense to tort actions against eligible businesses for claims relating to data breaches. The law goes into effect in 90 days.

Blockchain

Senate Bill 220 acknowledges the legitimacy of blockchain transactions by affirming that both electronic records and electronic signatures may be created through use of blockchain technology. The law does this by modifying the statutory definitions of "electronic record" and "electronic signature" to include references to blockchain technology.

Safe Harbor – Subject Matter and Scope

In addition to acknowledging the legitimacy of blockchain technology, the law creates an affirmative defense to tort actions brought against eligible businesses that have suffered a data breach.

To be eligible for the affirmative defense, which the law refers to as a "safe harbor," a business must have adopted a cybersecurity program that reasonably conforms to the law's requirements. The safe harbor applies to any tort action—brought either under the law of the State of Ohio or in the courts of the State of Ohio—claiming that a covered entity's[1] failure to implement reasonable information security controls resulted in a data breach involving "personal

information" or "restricted information."

Although the term "personal information" has the same narrow meaning given to it by Ohio's data breach law, the term "restricted information" is more expansive and includes any information that "can be used to distinguish or trace [an] individual's identity or that is linked or linkable to an individual," if such information is not encrypted, redacted or altered in a way to make it unreadable. For example, if an unencrypted database contains only an individual's address, birthdate, and driver's license number, that information would not be considered personal information, nor would it be subject to Ohio's data breach notification requirements because it did not include the person's name. However, this information would be deemed "restricted information." This broad definition of "restricted information" was likely included so that the safe harbor could be applied to claims for damages resulting from identity theft and similar fraudulent activities, even if Ohio's data breach notification law was not implicated.

Requirements for the Safe Harbor

To qualify for the safe harbor, a business must create, maintain, and comply with a written cybersecurity program that contains safeguards for the protection of personal information, restricted information, or both. If a covered entity's program is designed to protect only personal information and not restricted information, the safe harbor protections will not apply to claims relating to a data breach affecting restricted information.

The scale and scope of a covered entity's cybersecurity program is to be determined based upon several factors, including the size of the covered entity, the nature and scope of the activities of the covered entity, the sensitivity of the information to be protected, and the cost and availability of tools to improve information security and reduce vulnerabilities. In addition, the cybersecurity program must "reasonably conform" to the current version of one of several government- or industry-recognized cybersecurity frameworks specified by the law. In the event that a chosen cybersecurity framework is updated, the business has up to a year

to bring its existing cybersecurity program into reasonable compliance.

Practical Considerations

Although blockchain is not new to Ohio, the new law should provide assurances to businesses hesitant to use the technology because of concerns about its legitimacy.

Although implementing a written cybersecurity program that meets the requirements of the law will involve an investment of a business's time, money and other resources, the potential benefits are significant. The safe harbor provides a path businesses may follow to mitigate the risk that a plaintiff can successfully bring a claim that he or she was harmed by lax data security practices. For plaintiffs who are not deterred by the safe harbor, time will be spent litigating whether a covered entity has met the requirements of the safe harbor—i.e., whether the covered entity "reasonably conformed" to its chosen security framework in view of the nature and scope of its activities, the sensitivity of the data, and the cost and availability of tools to improve information security and reduce vulnerabilities. However, for businesses that successfully implement a written cybersecurity program that reasonably conforms to the law's requirements, the safe harbor will be game-changer in lawsuits for damages resulting from a data breach.

---

[1] Covered entities include both for-profit and non-profit businesses, regardless of whether such businesses are located within Ohio.

FBT Gibbons