Ohio Takes the Lead in Blockchain with Signing of Cybersecurity Bill

The state of Ohio took a big step to position itself as a leader in cybersecurity and a haven for blockchain technology. On August 3, Ohio Governor John Kasich signed the Data Protection Act (Senate Bill 220) into law.[1] The Data Protection Act creates an affirmative defense to a tort action stemming from a data breach for businesses that proactively develop cybersecurity programs that meet specific requirements outlined within the legislation.[2] However, the Data Protection Act is particularly noteworthy because of an amendment that creates a stronger legal basis for blockchain-based business transactions in Ohio.[3]

This legislation is an important first step for Ohio to attract cutting-edge technology companies and startups to the Buckeye State.[4] Ohio is just the fourth state to pass blockchain-focused legislation, behind Colorado, Delaware, and Illinois.[5]

What is Blockchain?

Blockchain is a technology that allows for records to be recorded securely in a constantly growing digital list.[6] Essentially, blockchain is a digital, decentralized public ledger that helps verify transactions.[7] Blockchain is an important emerging technology, because it creates a permanent record and can be verified by an entire community instead of a singular, centralized authority.[8] Blockchain is best known for being the technology underlying emerging cryptocurrencies such as Bitcoin, Ethereum, and Ripple.

Blockchain is an exciting technology for businesses, because backers believe blockchain has potential applications in other industries and sectors such as real estate transactions, supply chain management, and medical records storage.[9]

What is the Ohio Blockchain Amendment?

The blockchain amendment in the Data Protection Act specifically outlines that transactions recorded by blockchain technology will be permitted under the Uniform Electronic Transactions Act.[10] The amendment modifies the definition of “electronic record” to allow for records or contracts secured through blockchain technology to fall under the definition of “electronic record.”[11] The amendment further modifies the definition of “electronic signature” to allow for signatures secured through blockchain technology to fall under the definition of “electronic signature.”[12]
With these minor amendments, contracts and electronic signatures processed through blockchain technology will have a more solid legal foundation in Ohio.

**What is the Ohio Cybersecurity Safe Harbor?**

The principle portion of the Data Protection Act creates a cybersecurity “safe harbor” for Ohio businesses in the event of a data breach.

**How does a safe harbor work for Ohio businesses?**

A safe harbor is a legal standard established in statute that, if satisfied, will protect a business from certain liability. The Data Protection Act establishes such a safe harbor for businesses that develop and implement a cybersecurity program that meets the Data Protection Act’s requirements. If a business meets the Data Protection Act’s requirements, it will be able to claim an affirmative defense against a tort action, making the business immune from liability stemming from a data breach. This means if a person brings a tort action claiming a business’ negligence was to blame for a data breach, so long as the business can prove it implemented a cybersecurity program that meets the Data Protection Act’s requirements, then the business will not be liable for any damages to the person stemming from the data breach.

To further incentivize businesses to pursue the safe harbor, the Data Protection Act explicitly does not create a private right of action that would allow a person to sue a business for failing to follow the Data Protection Act’s safe harbor requirements.

**Who qualifies for the safe harbor? What information is protected?**

The safe harbor is available to all “covered entities” as defined under the Data Protection Act. A covered entity is defined broadly in the Data Protection Act and includes LLCs, LLPs, corporations, and other corporate entities, whether operating for profit or not for profit. Financial institutions are also captured in this definition.

Regarding the type of information the Data Protection Act protects, there are two types: personal information and restricted information. Personal information has the same meaning as in Ohio’s data breach notification statute, while restricted information is newly defined in the Data Protection Act.

**How does my business qualify for the safe harbor?**

In order to qualify for the safe harbor, a covered entity must “create, maintain, and comply with a written cybersecurity program” that protects personal information and restricted information. The cybersecurity program must conform with the below three requirements to qualify for the safe harbor:

1. Protect the security and confidentiality of the information;
2. Protect against any anticipated threats or hazards to the security or integrity of the information; and
3. Protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud.

The Data Protection Act is mindful that there is no “one size fits all” cybersecurity program for covered entities. Therefore, the size and scope of a cybersecurity program will be based on several factors including the size and complexity of the business, the sensitivity of the information to be protected, and the scope of the
Are there any other specific requirements?

The Data Protection Act outlines that on top of the above requirements, a covered entity’s cybersecurity program must also reasonably conform to one of the below three categories of frameworks:

- Industry recognized cybersecurity frameworks, including:
  - NIST Special Publication 800-171;
  - NIST Special Publications 00-53 and 800-53a; and

- Statutory cybersecurity frameworks, including:
  - The federal Health Insurance Portability and Accountability Act (“HIPAA”);
  - The federal Gramm-Leach-Bliley Act (“GLBA”); and
  - The federal Health Information Technology for Economic Clinical Health Act (“HITECH”).

- The Payment Card Industry (“PCI”) data security standard.

Conclusion

The signing of Data Protection Act into law creates an excellent opportunity for businesses to evaluate their own cybersecurity practices. Businesses should consider aligning their cybersecurity programs with one of the industry recognized frameworks or statutory frameworks enumerated in the Data Protection Act. Such efforts could limit liability in the event of a data breach.

Ice Miller has the cybersecurity professionals and experience to help clients take that initial step in identifying which cybersecurity framework is the best fit for your business considering your business’ size, industry, and corporate structure. To speak to an attorney, please contact Nicholas Merker at nicholas.merker@icemiller.com, Stephen Reynolds at stephen.reynolds@icemiller.com, or Matthew Diaz at matthew.diaz@icemiller.com.

This publication is intended for general information purposes only and does not and is not intended to constitute legal advice. The reader should consult with legal counsel to determine how laws or decisions discussed herein apply to the reader’s specific circumstances.

[6] Id.
[12] Id.
[14] Id.
[15] Id.
[16] Id.
[17] Id.
[18] Id.
[20] Id.
[21] Id.
[22] Id.
[23] Id.