Vol. 4, No. 30 September 19, 2018 PRINT E-MAIL

STATE LAWS

Ohio Adopts Pioneering Cybersecurity Safe Harbor for Companies

By Vincent Pitaro

The Cybersecurity Law Report

On August 3, 2018, Ohio Governor John R. Kasich announced that he had signed Substitute Senate Bill 220, also known as the Ohio Data Protection Act (Act). The most significant purpose of the Act, which will take effect on November 2, is to create a safe harbor for covered entities that implement a cybersecurity program in accordance with the Act "to be pled as an affirmative defense to a cause of action sounding in tort that alleges or relates to the failure to implement reasonable information security controls, resulting in a data breach." This article details the provisions of the Act that establish the cybersecurity safe harbor and those that deem blockchain transactions to be electronic transactions, with insights from Jason Wool, a counsel at ZwillGen.

The Act is likely to benefit businesses that qualify for the safe harbor, but its greatest significance, in Wool's view, is that it may be "indicative of a future trend in which states – and maybe even the federal government – will provide meaningful incentives to companies for the implementation of cybersecurity frameworks and standards on a voluntary basis."

Several states now require covered entities to adopt reasonable cybersecurity measures. See "Colorado's Revised Cybersecurity Law Clarifies and Strengthens Existing Requirements," (Sep. 12, 2018); and "Analyzing New and Amended State Breach Notification Laws" (Jun. 6, 2018). See also "Synthesizing New York and Colorado's Trailblazing Data Security Regulations for Financial Firms" (Jul. 12, 2017).

Cybersecurity Program Safe Harbor

Key Definitions

A "covered entity" is one that maintains, transmits or processes "personal information" or "restricted information" through services located within or outside of Ohio.

"Personal information" includes a person's first name or first initial and last name in combination with at least one of the following identification numbers, if the number is readable, unencrypted or unredacted: Social Security number, state-issued identification number or financial account number with any associated security code or password. It does not include "publicly available information that is lawfully made available to the general public from federal, state, or local government records" or from news or other widely distributed media.

"Restricted information" is information about an individual that "alone or in combination with other information, including personal information, can be used to distinguish or trace the individual's identity or that is linked or linkable to an individual, if the information is not encrypted, redacted, or [rendered unreadable] and the breach of which is likely to result in a material risk of identity theft or other fraud to person or property."

"'Restricted information' really serves as a kind of catch-all to ensure that sensitive personal data is protected, whereas 'personal information' is very specific," Wool told The Cybersecurity Law Report. "For instance, 'personal information' requires that the data elements be combined with an individual's name, and only covers a person's SSN, driver's license number and certain financial account data. On its own, 'personal information' would not, for instance, cover biometrics or online account credentials, whereas 'restricted information' could," he explained.

See "Biometric Data Protection Laws and Litigation Strategies (Part One of Two)" (Jan. 3, 2018), Part Two (Feb. 14, 2018).

A "data breach" is the unauthorized acquisition of computerized information that compromises the security or confidentiality of personal information or restricted information held by a covered entity that causes or that can reasonably be expected to cause "a material risk of identity theft or other fraud to person or

Recent Issues
Vol. 4, No. 29 (Sep. 12, 2018)
Vol. 4, No. 28 (Sep. 5, 2018)
Vol. 4, No. 27 (Aug. 29, 2018)
Vol. 4, No. 26 (Aug. 22, 2018)
Vol. 4, No. 25 (Aug. 15, 2018)
View full archive ...

property." It does not include information acquired and used by a covered entity for its lawful business purposes or the acquisition of information pursuant to a search warrant, subpoena or other legal process.

Three Requirements to Establish Affirmative Defense

A covered entity that satisfies the following three requirements is entitled to "an affirmative defense to any cause of action sounding in tort that is brought under the laws of this state or in the courts of this state and that alleges that the failure to implement reasonable information security controls resulted in a data breach" concerning personal information and/or restricted information.

1. The covered entity must adopt and comply with a written cybersecurity program (Program) that "contains administrative, technical, and physical safeguards" for the protection of personal information or both personal information and restricted information, as the case may be, and that "reasonably conforms to an industry recognized cybersecurity framework," as defined below.
2. The Program must be designed to accomplish all of the following:
    a. protect the security and confidentiality of the relevant information;
    b. protect against threats to the security or integrity of the information; and
    c. protect against unauthorized acquisition of information that is "likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates."
3. The scope of the Program must be based on:
    a. the entity's size and complexity;
    b. the nature and scope of its activities;
    c. the sensitivity of the relevant information;
    d. the cost and availability of tools to protect the information; and
    e. the entity's available resources.

See "How to Build a Cybersecurity Culture Using People, Processes and Technology" (Aug. 15, 2018).

A covered entity's Program may be designed to protect personal information or both personal information and restricted information. The safe harbor is not available to an entity that suffers a breach involving restricted information if its Program was designed only to protect personal information.

The safe harbor is not limited to Ohio data and should be available regardless of a plaintiff's residence: "[T]he affirmative defense is meant to be available in response to tort claims alleging failure to implement reasonable cybersecurity measures brought under the laws of Ohio or in Ohio courts. . . . This could be important in the event of class action litigation, and could provide a strong incentive for defendants to try to get Ohio law to apply," Wool explained.

See "Minimizing Class Action Risk in Breach Response" (Jun. 8, 2016).

Eligible Cybersecurity Frameworks

A Program "reasonably conforms to an industry recognized cybersecurity framework" if it satisfies at least one of the following:

1. The Program "reasonably conforms" to the current version of one or more of the following :
    a. NIST cybersecurity framework [see "NIST Program Manager Explains Pending Changes to Its Cybersecurity Framework" (Jan. 17, 2018)];
    b. NIST special publication 800-171 or 800-53 and 800-53a [see "Deadline Passes for DOD Contractors and Subcontractors to Provide "Adequate Security": Are They Ready?" (Jan. 17, 2018)];
    c. Federal Risk and Authorization Management Program (FedRAMP) security assessment framework;
    d. Center for Internet Security critical security controls for effective cyber defense; or
    e. ISO/IEC 27000 family - Information security management systems [see "Guide to Getting Your Security Program Certified Under ISO 27001" (Nov. 2, 2016)].
2. The relevant covered entity "is regulated by the state, by the federal government, or both, or is otherwise subject to the requirements of any of the laws or regulations listed below, and the cybersecurity program reasonably conforms to the entirety of the current version of any of the following. . .":
    a. the security requirements specified in the Health Insurance Portability and Accountability Act (HIPAA) [see "Lessons From the Continued Uptick in HIPAA Enforcements" (Feb. 8, 2017)];
    b. Title V of the Gramm-Leach-Bliley Act of 1999;
    c. Federal Information Security Modernization Act of 2014; or

d. Health Information Technology for Economic and Clinical Health (HITECH) Act [see "Steps to Take Following a Healthcare Data Breach" (Apr. 22, 2015)].

3. The Program reasonably complies with both the current version of the Payment Card Industry Data Security Standard (PCI DSS) and the current version of one of the standards or frameworks listed in paragraph 1 above [see "Essential Cyber, Tech and Privacy M&A Due Diligence Considerations" (Aug. 8, 2018)].

The Act is notable for offering flexibility to businesses: "Some of the framework options are much more feasible to implement for companies than others – for instance, NIST SP800-171, which is essentially a 'light' version of SP800-53 that was designed for government contractors that handle controlled unclassified information," Wool said. In addition, there is no certification or third-party auditing requirement, and a Program must only "reasonably conform" to the selected framework.

In each case, a covered entity must comply with any revisions to any of the relevant standards and frameworks to which its Program conforms within one year after an amendment, in the case of a government statute or regulation, or a final revision, in the case of a non-governmental standard or framework.

The second requirement is confusing, Wool pointed out, because it is not clear why only state or federally regulated businesses should be able to qualify for the safe harbor by complying with the listed statutes and regulations. "As written, any state-regulated business – such as a bail bondsperson – that complies with HIPAA's security rule – even if it is not subject to HIPAA – could apparently take advantage of this section," Wool noted. At the same time, an unregulated business would not be able to qualify for the safe harbor in the same way.

The third requirement is confusing because it suggests that compliance with PCI DSS alone is not sufficient. If that is the case, and an entity also complies with one of the standards listed in paragraph 1, then paragraph 3 would be superfluous, he said.

"The statute raises a lot of unresolved questions, many of which are the result of sloppy drafting. The true utility of the law will probably only be revealed once it is tested in actual litigation," Wool noted. Nevertheless, "Ohio deserves kudos for taking the lead on this," he said.

No Private Right of Action

The Act's stated purpose is to encourage businesses to improve their cybersecurity voluntarily. It does not "create a minimum cybersecurity standard that must be achieved, nor shall it be read to impose liability upon businesses that do not obtain or maintain practices in compliance with the act." It also states that it does not create a private right of action, including class actions, with respect to the described cybersecurity practices.

Wool sees Ohio's offer of a carrot to businesses to improve their cybersecurity programs as "a much more business-friendly approach to using policy and legislation to improve corporate cybersecurity, as opposed to the approach recently taken by California to offer a private right of action against businesses that fail to implement reasonable cybersecurity measures." In fact, during the development of the business-friendly NIST cybersecurity framework, there were calls for legislation "to reward companies that implement the framework but not punish those companies that choose not to," he added.

See "What to Expect From California's Expansive Privacy Legislation" (Jul. 18, 2018).

Taking Advantage of the Act

"Businesses that reasonably anticipate that they could become involved in data security tort litigation in an Ohio court or subject to Ohio law should definitely consider implementing one of the frameworks, especially as some of the options are more attainable for companies that aren't highly mature in the cybersecurity context," Wool recommended. "Companies headquartered in Ohio or that have a lot of customers in Ohio are prime candidates," he added.

See "Proactive Steps to Protect Your Company in Anticipation of Future Data Security Litigation (Part One of Two)" (Nov. 25, 2015), Part Two (Dec. 9, 2015).

In order to qualify for the safe harbor, a company that has implemented a risk-based written cybersecurity program for the protection of PI could adopt one of the listed frameworks or, if eligible, comply with one of the listed laws, according to Wool. "To adopt a framework, one option would be to review each of the controls listed in the framework and assess whether the business's cybersecurity program currently meets the requirement. To the extent it doesn't, the business would need to implement measures to meet the requirement," he explained.

Because the Act does not explain what it means to "reasonably conform" to a framework, "it is possible that the cybersecurity program does not have to 100-percent satisfy the requirements of the framework. In fact, at least with respect to the NIST Cybersecurity Framework, it is entirely unclear what it means to 'reasonably conform,' as the framework is not prescriptive and is actually designed to be flexible," he added.

See also "NIST Program Manager Explains Pending Changes to Its Cybersecurity Framework" (Jan. 18, 2018).

Recognition of Blockchain Transactions as "Electronic"

The Act also makes clear that transactions recorded by blockchain technology are covered by Ohio's Uniform Electronic Transactions Act: The definition of "electronic record" has been amended to include a "record or contract that is secured through blockchain technology." Similarly, "electronic signature" now includes a "signature that is secured through blockchain technology. . . ."

This is a significant change, according to Wool, because "it will expand the ability of blockchain-based technologies to be used in contracting and will provide users of these technologies with greater confidence in the legal enforceability of contracts executed in this manner."

See our three-part series on blockchain technology: "Basics of the Blockchain Technology and How the Financial Sector Is Currently Employing It" (Jun. 14, 2017); "How Financial Service Providers Can Use Blockchain to Improve Operations and Compliance" (Jun. 28, 2017); and "Blockchain and the Financial Services Industry: Potential Impediments to Its Eventual Adoption" (Jul. 12, 2017).