Tucker Ellis LLP

CLIENT ALERT

OHIO JOINS GROWING TREND REQUIRING CYBERSECURITY STANDARDS AND REPORTING OBLIGATIONS FOR INSURANCE INDUSTRY

FEBRUARY 2019

Insurers, brokers, and agents doing business in Ohio must be aware of a new law going into effect on March 20, 2019. Ohio Sub S.B. 273, signed by former Governor John Kasich on December 19, 2018, will require insurance industry-specific minimum cybersecurity standards and reporting obligations for breaches, ransomware attacks, and similar events. The new law makes Ohio one of a small but growing group of states (South Carolina and Michigan being the others) to adopt similar insurance-focused legislation based on the National Association of Insurance Commissioners' Model Data Security Law. Under the law, a covered business will be required to implement and maintain an appropriate written cybersecurity program, have a written incident response plan, and ensure its Board of Directors' participation and oversight. The law also grants authority to the Ohio Department of Insurance to investigate and enforce compliance.

WHO IS COVERED?

The new law applies to "licensees," which includes any business that is required to be licensed, authorized to operate, or registered with the Ohio Department of Insurance. Sub. S.B. 273, R.C. 3965.01(M). This generally includes insurers, brokers, and agencies, and covers both Ohio-based businesses and foreign businesses operating within the state. The law does not apply to a purchasing group or a risk retention group chartered and licensed in another state or a licensee that is acting as an assuming insurer that is domiciled outside of Ohio. *Id.*

Licensees are exempt from the written cybersecurity program requirements only if:

- They have fewer than 20 employees;
- They have less than $5 million in gross annual revenue;
- They have less than $10 million in assets, as measured at the end of the business's fiscal year; or
- They are covered by the HIPAA Privacy and Security Rules and certify their HIPAA compliance with the Ohio Department of Insurance.

R.C. 3965.07(A) – (B). Licensees who are affiliated with another licensee in certain ways, such as an employee or independent contractor, are also exempt if they are covered by the other licensee's cybersecurity program. *Id.* (C). Exempted licensees will still be required to comply with the reporting obligations discussed below. *Id.*

COVERED BUSINESSES MUST HAVE A CYBERSECURITY PROGRAM MEETING MINIMUM STANDARDS

Sub. S.B. 273 is designed to ensure that a covered business takes steps to protect the "nonpublic" business and consumer information in its possession. The law defines this provision broadly and includes biometric data and health information, in addition to personal identifiers, social security numbers, financial account information, and driver's license numbers. R.C. 3965.01(O).

The new law's required cybersecurity standards found in R.C. 3965.02 incorporate fundamental principles of information security. The key requirements include:

- A **comprehensive written cybersecurity program**;
- Ongoing **risk assessment and management programs**;
- The incorporation of **administrative, physical, and technical safeguards**, including **encryption**, **access controls** to limit access to only authorized personnel, **multi-factor authentication**, **data retention and disposal policies**, and **staff security awareness training**;

- **Testing and monitoring** security controls and procedures to evaluate performance and to detect attacks and intrusions;
- A **written incident response plan**;
- A **third-party vendor risk management program**;
- **Active Board of Directors' involvement and oversight** and incorporating cybersecurity into the business's enterprise risk management process; and
- **Annual compliance reporting to the Ohio Department of Insurance** for insurers domiciled in Ohio.

BREACHES AND OTHER CYBER EVENT REPORTING

Sub. S.B. 273 also introduces new obligations that require prompt investigation of potential "cybersecurity events" to ensure timely notification to the Department of Insurance. Notably, "cybersecurity events" include more than just breach-type events where confidential information is improperly accessed and stolen or disclosed. They also include ransomware attacks and other incidents that disrupt access to a business's own computer network and its business operations overall. *See* R.C. 3965.01(E) & .03.

The new law provides a very short initial notification deadline for reportable events: no later than three (3) business days from determining that a cybersecurity event occurred. These reporting obligations generally apply to (a) covered businesses based in Ohio and (b) any covered business located outside of Ohio where the event involves 250 or more Ohio residents. *See* R.C. 3965.04. The law also specifies the investigation and reporting obligations in the event of breaches and security incidents involving third-party vendors, as well as assuming and ceding insurers.

Sub. S.B. 273 does not change the reporting requirements to individuals under Ohio's data breach notification law, R.C. 1349.19. See our August 2018 Client Alert here for more information. Covered businesses, however, will be required to provide copies of the individual notices to the Department of Insurance. *See* R.C. 3965.04(C).

AFFIRMATIVE DEFENSES TO DATA BREACH LAWSUITS

Compliance with Ohio's new law will assist businesses in seeking to defend against tort claims in data breach lawsuits. Compliance provides a specific affirmative defense to such claims (*see* R.C. 3965.08) and assists businesses seeking to qualify for the Ohio Data Protection Act's (ODPA) "safe harbor" defense through the maintenance of a cybersecurity program that reasonably conforms to an industry-recognized cybersecurity framework. Our August 2018 Client Alert here provides more information on the ODPA. Sub. S.B. 273 is intended to create a similar framework under the ODPA, and a business that meets the requirements of the new law is deemed to have a cybersecurity program that qualifies for the ODPA defense. *See* R.C. 3965.02(J).

WHEN MUST A COVERED BUSINESS COMPLY WITH THE NEW LAW?

The new breach and cybersecurity event reporting requirements go into effect on March 20, 2019. Covered businesses will be required to implement most of the written cybersecurity program requirements under R.C. 3965.02 by March 20, 2020 (one year from the effective date of the law). The remaining third-party vendor due diligence and oversight requirements must be implemented by March 20, 2021 (two years from the effective date of the law).

WHAT INITIAL STEPS SHOULD BUSINESSES TAKE TO COMPLY?

With Sub. S.B. 273, Ohio joins a growing trend of states enacting minimum cybersecurity requirements for the insurance industry. Ohio, South Carolina, and Michigan have adopted versions of the NAIC's Model Data Security Law, which has many similarities to New York's Financial Services Cybersecurity Regulations, 23 NYCRR 500, that became effective in 2017. Similar legislation is currently pending in Rhode Island, and it is anticipated that this trend will continue through 2019 and into 2020. All insurance businesses operating in

Ohio and elsewhere will need to monitor developments to ensure that they are in compliance with any requirement that applies to them.

All companies doing insurance-related business in Ohio need to evaluate whether the new law applies to them. Covered businesses then need to assess their ability to comply with the new breach and cyber event reporting obligations going into effect in March. Covered businesses should also begin to assess their cybersecurity program's compliance with the minimum standards requirements as implementation of a compliant program can be a lengthy process. Outside experts to counsel on the new law's legal and technical requirements and the implementation of those requirements can assist in this process. Beyond the compliance benefits, taking these steps now will enhance a business's ability to protect the confidential and proprietary information it holds while also improving its ability to timely and effectively respond in the unfortunate event of a data breach or ransomware attack.

ADDITIONAL INFORMATION

For additional information, please contact:

- **Bill Berglund** | 216.696.2698 | william.berglund@tuckerellis.com
- **Rob Hanna** | 216.696.3463 | robert.hanna@tuckerellis.com
- **Paul Janowicz** | 216.696.5787 | paul.janowicz@tuckerellis.com