Ohio's Data Protection Act: An Opportunity for Financial Institutions That Operate in Ohio

Dec 05, 2018

Categories:

Blockchain and Digital Assets
Blogs

Good news! The Ohio legislature has offered financial institutions some legal protections in the form of the Ohio Data Protection Act (the "Act"). However, you must be proactive. It will be good for your business and may help in future litigation.

The Act was signed by Governor Kasich in the summer of 2018 and is now effective. The Act is codified as Ohio Revised Code sections 1354.01 *et seq*. When proposed, the Act was believed to be a first-of-its-kind state law. The purpose of this blog post is to suggest to financial institutions that they can get the benefit of the Act's protections without excessive effort because many financial institutions are probably already meeting most of the Act's requirements.

Financial institutions necessarily obtain and use both of the types of information described in the Act: (A) "restricted information," which is information about an individual that, alone or in combination with other information, can be used to distinguish or trace the individual's identity; and (B) "personal information" which is an individual's name combined with one of that individual's (i) social security number, (ii) driver's license number, (iii) state identification number, (iv) account number, (v) credit card number, or (vi) debit card number.[1]

Fortunately, the Act creates an affirmative defense for a financial institution to use in litigation, if that financial institution suffers a data breach and is subsequently the target of civil tort litigation due to the improper release of restricted information or personal information.[2] To create and benefit from the litigation defense, the financial institution must "create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of both personal information and restricted information" in reasonable conformance with the standards of certain set by the legislature in

FBT Gibbons

Ohio Revised Code Section 1354.02.

In my experience, financial institutions are concerned about data security involving their customers, employees and others.[3] Before they worry about data breach litigation, they care about data security because they know that a breach is bad for business and protecting their customer's data is the proper thing to do. Given these circumstances, there is no reason for a financial institution not to assess its current data security plan and see if it meets the Act's requirements or can be reasonably modified to meet the Act.

The Act's initial requirements in Section 1354.02 may be already met by the financial institution's existing data security plan because those sections require that the data security plan (i) be designed to protect the security and confidentiality of information against anticipated threats including unauthorized access by outsiders and insiders, (ii) be scaled and designed to cover the institution and varied depending on the threat [the threat of outside hackers is not the same as the threat that a teller will commit identity theft and so the plan needs to be tailored as appropriate], and (iii) meet certain other requirements. If the Act's tests in Section 1354.02 are met, the above-described affirmative defense is available.

If a financial institution wants to assert the affirmative defense without having its data security plan tested against the general standards of Section 1354.02, that institution can opt to meet the requirements of Section 1354.03. This is commonly referred to as a "safe harbor." The legislature has determined that the data security requirements promulgated by the experts listed in Section 1354.03 automatically meet the requirements of Section 1354.02 and so the affirmative defense is then available.

If it chooses to try for a safe harbor, a financial institution should assess all the security plan creating experts listed in Section 1354.03 to determine which set of expert's standards it wants want to meet because those particular standards best meet the institution's needs. I suggest that financial institutions focus on Subsection 1354.03(B) because the experts listed in that section are aimed at regulated entities like financial institutions. Of particular interest to financial institutions is the fact that one of the data protection promulgations they may choose to follow were

created by the Graham-Leach-Bliley Act of 1999 also known as the Financial Services Modernization Act of 1999.[4] I know that many financial institutions are already familiar with the data protections arising from that law because it is aimed at financial institutions and is nearly 20 years old. The data security requirements flowing from the Graham-Leach-Bliley Act are primarily a security rule and a privacy rule, both promulgated by the Federal Trade Commission.

Another option in the Act that might fit some financial institutions is found in Section 1354.03(C)(1) which permits financial institutions and other businesses, such as merchants, into the safe harbor and access to the affirmative defense discussed above if the financial institution's data security plan meets the "payment card industry (PCI) data security standard" and certain other requirements. Financial institutions should consider shaping their data security plan to meet the payment card industry data security standard[5] because there is an excellent chance that the financial institution is already familiar with, and perhaps complying with, the payment card industry data security standard which are technical and operational requirements for organizations accepting or processing payment transactions.

Before the rise of internet hackers, entities with sensitive data faced disgruntled employees who stole information and dumpster divers who sought information that was handled sloppily. Those risks still exist and new ones (malware, spoofing and phishing) arise regularly. Current events prove that data breaches will happen, and litigation will follow – both seem sadly inevitable. Knowing these facts, it is logical and appropriate for financial institutions to:

- assess the institution's current data protection plans and improve them as needed;
- compare the institution's data security plans with the general requirements of Ohio Revised Code Section 1354.02 to determine if you can use the offered affirmative defense in the event of data breach litigation;
- consider avoiding the generalized tests of your institution's data security plan found in Section 1354.02 by reviewing the data security standards promulgated by the experts listed in

Section 1354.03; and

- financial institutions might pay particular attention to the data security standards already tailored to their industry arising from (a) the Graham-Leach-Bliley Act of 1999 also known as the Financial Services Modernization Act of 1999 and (b) payment card industry data security standard. Both of those sources of data security standards are designed specifically for some of the business activities conducted by financial institutions.

Again, be proactive and assess whether you are able to afford your institutions with the protections offered under the Ohio Data Protection Act. Remember that Frost Brown Todd can assist you as needed!

Using his law degree, MBA and the experience of having passed the CPA examination, Vincent Mauer has spent 30+ years representing financial institutions. He can be reached at vmauer@fbtlaw.com.

---

[1] The Act's definition of "personal information" is from Ohio's Consumer Protection Act, O.R.C. section 1349.19.

[2] Specifically, the Act offers "an affirmative defense to any cause of action sounding in tort that is brought under the laws of" Ohio or in Ohio courts that "alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information or restricted information." This affirmative defense can apply to negligence claims, breach of privacy claims and breach of duty claims.

[3] This includes noncustomers whose personal information is in the institution's possession such as declined loan applicants and the former owners of closed accounts.

[4] Ohio Revised Code Section 1354.03(B)(1)(b).

[5] The Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit and debit cards. Those standards were created by major card entities to increase controls around cardholder data. The standards are potentially useful and beneficial for entities that

obtain, use and transmit cardholder data.

FBT Gibbons