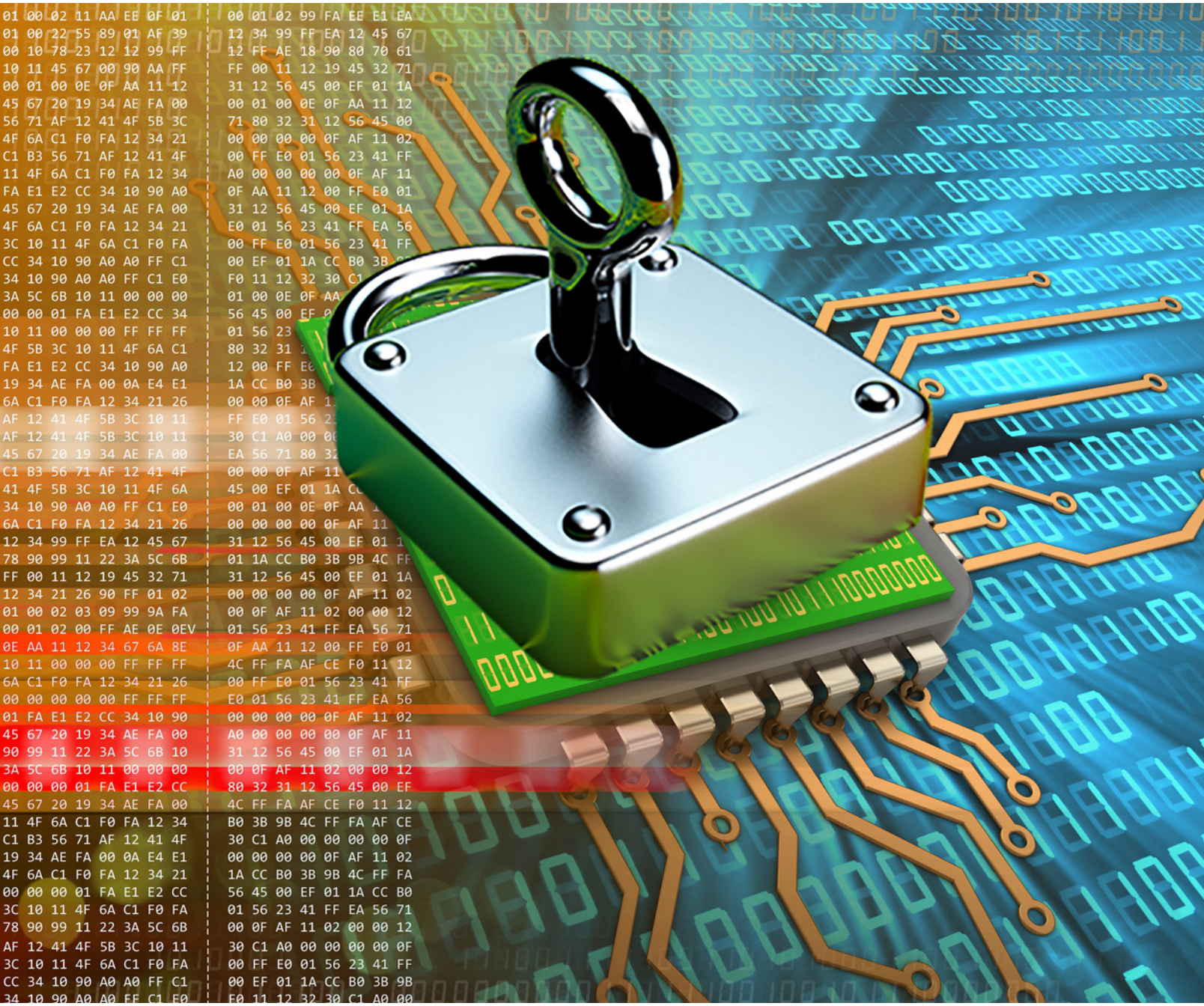
Data Breach Litigation:
Defenses Against the Rising Tide

Joseph M. Brunner, Vorys Sater Seymour & Pease LLP



Data breaches are increasingly a fact of life. Personal information is valuable to all manner of cyber criminals who increasingly have the means and opportunity to access and use it. The litigation associated with such breaches is also increasingly a fact of life. Even for companies that take steps to protect their data, once a breach happens, litigation follows closely behind. This litigation is fueled by government attorneys who are empowered by state laws creating new causes of action, as well as private litigants who seek to punish breaches—all ostensibly to promote better data security, but ultimately raising the costs of a breach even higher. But what if there were incentives for business entities to raise their data protection standards and reduce the costs of litigation? This article explores a recent attempt to offer just that.

The Threat Is Growing

Theft is a crime of opportunity. More and more data is placed on computer systems and used for basic everyday transactions, and advances in technology and the growing sophistication of cybercrime tools make that data more accessible. The technologies for securing that data, however, lag behind and are underutilized. The threats from hackers, cyber criminal organizations, and nation-state actors have become more diverse and distributed, but while the sophistication of available tools is growing, the sophistication required to use them is declining.[1]

The frequency and impact of attacks is thus growing. While 2013 saw 2,615 incidents worldwide, by 2017 the number of incidents doubled to 5,207.[2] The number of records exposed in that timeframe ballooned even more—from 1.1 billion in 2013 to a staggering 7.89 billion in 2017,[3] of which 2,330 of those breaches occurred in the United States, exposing 2.3 billion records.[4] Virtually every sector of the economy is targeted, but health care had the dubious distinction of leading the field in 2017 (along with Information Technology) by accounting for 8.5% of all breaches.[5] Of those health care breaches, 34.4% involved hospitals, 32.4% involved practitioners' offices, and 27.2% came from non-hospital facilities. The frequency of attacks within the health care industry is growing as well. The Department of Health and Human Service's Office for Civil Rights (HHS-OCR) maintains a breach portal logging all the data breach incidents reported to HHS-OCR. Hacking and IT incidents are the leading cause of health care data breaches. In 2018, 153 of the reported breaches were classified as "Hacking/IT Incidents," an increase over the 147 hacking incidents reported in 2017. Unauthorized access and disclosure incidents are a close second, with 139 reported in 2018 and 128 in 2017.[6]

Why is the health care sector such a target? Money and opportunity.

Why is the health care sector such a target? Money and opportunity. Whereas the black market value of social security and credit card numbers is just pennies, a full medical record can fetch between $500 to $1,000.[7] A person who has been impacted by a data breach can change her stolen credit card numbers, put credit freezes in place, and even change her social security number if it is stolen, but a person's medical record is the most comprehensive and immutable collection of information that exists regarding that individual. It can be used for more than just buying a few things online, such as submitting fraudulent insurance claims, obtaining prescription drugs, and blackmail. In addition, health care organizations often do not have the proper controls and systems in place to detect and deter breaches.[8]

Litigation Risks and Defenses

All of these breaches inevitably present a risk of litigation. With no comprehensive national rules or legislation in place, both government and private actors resort to trying to fit these new

To address the growing data breach trend, both federal and state governments have turned to litigation.

factual situations into existing frameworks, and when states have acted, they have almost overwhelmingly elected to try and curb data breaches by creating new causes of action and new "sticks." The state of Ohio, however, is now attempting a different approach.

Compliance Through Litigation

To address the growing data breach trend, both federal and state governments have turned to litigation. For example, the Federal Trade Commission—in lieu of formally promulgating regulations addressing data breach issues—has brought claims under Section 5(a) of the Federal Trade Commission Act[9] against businesses for engaging in "unfair" or "deceptive" trade practices for not securing customer data that was subsequently breached.[10] State attorneys general (or other state entities), likewise, have authority to bring suit for violations of state-specific data breach laws (which are often extensions of state unfair consumer practices or unfair trade practices statutes).[11] The state may typically recover a per-breach civil penalty, as well as its costs for investigating and bringing the lawsuit. Note that some states characterize the penalty as per incident of breach,[12] not per individual affected by the breach, while others do tie the penalty to the number of individuals involved.[13] It is also worth noting that some states, such as Iowa, exempt Health Insurance Portability and Accountability Act (HIPAA)-compliant entities from their statutory scheme.[14]

Some state laws create a private right of action empowering individual citizens to bring suit for violation of the state data security regime.[15] Such laws typically permit individuals who have been injured by a data breach to recover their actual damages stemming from the breach. New Hampshire even permits treble damages for willful or knowing violations.[16] Some, such as Hawai'i, the District of Columbia, and South Carolina, also permit recovery of attorneys' fees.

Even in states that do not create a specific private right of action, private litigants have myriad common law and statutory legal theories to rely on. For businesses that have contracts with their customers governing use and maintenance of personal information—such as a payroll processor or an insurance company—breach of contract is an obvious theory.[17] Even when there is no formal contract, plaintiffs allege the existence (and breach) of an implied contract.[18] In addition, statutory remedies such as the Fair Credit Reporting Act and various state law unfair competition and consumer protection statutes form bases for litigation.[19] Tort law claims such as negligence, invasion of privacy, and bailment and conversion are also common.[20]

A New Defense

Whereas all previous state responses have focused on expanding liability, creating sticks, and punishing data breaches, Ohio has now decided to offer a "carrot." On August 3, 2018 Ohio Governor John Kasich signed Senate Bill 220, also known as the Ohio Data Protection Act.[21] The act, effective November 2, 2018, established a safe harbor for businesses that create and maintain a cybersecurity program against certain types of litigation that stem from a data breach. Unlike previous state approaches that aimed to punish businesses for data breaches, the Data Protection Act is "intended to be an incentive and to encourage businesses to achieve a higher level of cybersecurity through voluntary action."[22] It did not purport to create a minimum cybersecurity standard,[23] and expressly states that it "shall not be construed to provide a private right of action, including a class action, with respect to any act or practice regulated under" the act.[24]

The Data Protection Act creates "an affirmative defense to any cause of action sounding in tort that is brought under the laws of [Ohio] 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 or restricted information."[25] The Act is specifically directed at tort claims, such as negligence and invasion of privacy, and does not cut off contract or statutory claims. An affirmative defense is any defensive matter that, while admitting the existence of a claim, provides a basis why the plaintiff cannot have any recovery on that claim.[26] This is in contrast with the more traditional "negative defense," which denies the plaintiff's allegations and attempts to discredit the facts and law supporting the plaintiff's claim.[27] The burden of proving the affirmative defense is on the party asserting it.[28]

The Data Protection Act applies to a "covered entity," which is expressly defined as "a business that accesses, maintains, communicates, or processes personal information or restricted information in or through one or more systems, networks, or services located in or outside" Ohio.[29] To avail itself of the safe harbor, a covered entity must satisfy four criteria. First, it must

"create, maintain, and comply with a written cybersecurity program" that safeguards personal and restricted information.[30] Note that simply having a "cybersecurity program" is not enough—it must be in writing, and the organization must actually implement and comply with it. And because the Data Protection Act creates an affirmative defense only and not a complete immunity to litigation, the covered entity will have the burden of proving its compliance.[31]

Second, the cybersecurity program must also be designed to accomplish three objectives. It must protect the security and confidentiality of the personal/restricted information, protect against threats and hazards to that security and confidentiality, and "[p]rotect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates."[32] While Ohio has a specific criminal statute addressing identity theft,[33] the Data Protection Act should not be read as only requiring covered entities to protect against the risk of criminal identity fraud. Because the Act provides an affirmative defense against common law tort claims, logically it would require covered entities to protect against material risks of those types of tort claims.

Third, the Data Protection Act also requires the cybersecurity program to be "appropriate" in scale and scope.[34] The Act recognizes that not all businesses seeking its protection are the same, nor are their cybersecurity needs and the data that should be protected.[35] Five factors govern whether the covered entity's cybersecurity program is appropriate: "(1) the size and complexity of the covered entity; (2) the nature and scope of the activities of the covered entity; (3) the sensitivity of the information to be protected; (4) the cost and availability of tools to improve information security and reduce vulnerabilities; [and] (5) the resources available to the covered entity."[36] This is a very fact-specific inquiry that must be evaluated by the trier of fact on a case-by-case basis.[37]

Fourth and finally, the cybersecurity program must "reasonably conform to an industry recognized cybersecurity framework[.]"[38] The Data Protection Act identifies a number of different industry cybersecurity frameworks, including NIST (National Institute of Standards and Technology), FedRAMP (the Federal Risk and Authorization Management Program), the Center for Internet Security's Critical Security Controls for Effective Cyber Defense, and ISO's Information Security Management Systems Standards,[39] as well as federal laws like Title V of the Gramm-Leach-Bliley Act and the Federal Information Security Modernization Act.[40] Most relevant for health care entities, however, is the fact that the Data Protection Act also identifies HIPAA's security requirements and the Health Information Technology for Economic and Clinical Health (HITECH) Act as industry-recognized cybersecurity frameworks.[41] Therefore, as long as a health care entity can show "reasonable compliance" with HIPAA and HITECH, it can satisfy this element of the Data Protection Act's affirmative defense.

Whereas all previous state responses have focused on expanding liability, creating sticks, and punishing data breaches, Ohio has now decided to offer a "carrot."

Future Responses

The Ohio Data Protection Act is certainly no silver bullet. It is limited to tort claims and does nothing to protect covered entities from breach of contract or statutory claims. Some might argue that by only creating an affirmative defense, it does not go far enough to reduce litigation costs (although a complete immunity from litigation is an unrealistic option), and given the national scope of data breach litigation, litigants will most likely file in other states.

Despite these apparent limitations, the main potential impact or contribution of Ohio's Data Protection Act is that it provides a template for other state or federal laws. It offers a different approach to enhance private-sector cybersecurity by offering an incentive to companies that take steps to enhance their cybersecurity programs, while still preserving the possibility of liability for those that do not. Ohio's Data Protection Act strikes a good balance between reward and punishment and the competing interests of all the different actors involved. State and federal lawmakers should review and consider Ohio's Data Protection Act as a model for future, comprehensive legislation addressing this growing national litigation trend.

Joseph Brunner is a litigation partner in the Cincinnati office of Vorys Sater Seymour and Pease LLP. His practice focuses on complex civil litigation, with an emphasis on representing hospitals and health systems.

Thanks go out to the leaders of the Health Care Liability and Litigation Practice Group (HCLL PG) for contributing this feature article: **Kristen Pollock McDonald,** Jones Day, Atlanta, GA (Chair); **Scott R. Grubman**, Chilivis Cochran Larkin Bever LLP, Atlanta, GA (Vice Chair—Strategic Planning and Special Projects); **Steven D. Hamilton**, McGuireWoods LLP, Chicago, IL (Vice Chair—Publications); **Jonay Holkins,** Feldesman Tucker Leifer Fidell LLP, Washington, DC (Vice Chair—Research & Website); **Kirstin Ives,** Falkenberg Ives LLP, Chicago, IL (Vice Chair—Membership); **Lindsey Lonergan,** Navicent Health Inc, Macon, GA (Vice Chair—Educational Programs); and **Courtney G. Tito,** McDonald Hopkins LLC (Social Media Coordinator).

Endnotes

1 U.S. Dep't of Justice, Report of the Attorney General's Cyber Digital Task Force (2018), https://www.justice.gov/ag/page/file/1076696/download.

2 Risk Based Security, Inc., *Data Breach QuickView Report: Data Breach Trends—Year End 2017*, at 3 (Jan. 2018), https://pages.riskbasedsecurity.com/2017-ye-breach-quickview-report.

3 *Id.*

4 *Id.* at 10.

5 *Id.* at 8.

6 U.S. Dep't of Health & Human Services-Office for Civil Rights, *Breach Portal*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

7 James T. Mulder, *Syracuse Hospital Data Breach Part of Massive National Problem*, Syracuse.com (Nov. 13, 2018), https://www.syracuse.com/news/index.ssf/2018/11/syracuse_hospital_patient_data_breach_part_of_massive_national_problem.html; Mariya Yao, *Your Electronic Medical Records Could Be Worth $1,000 To Hackers*, Forbes (Apr. 14, 2017), https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#7bf08e4a50cf.

8 *See Mulder supra* note 7.

9 15 U.S.C. § 45(a).

10 *E.g., FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014); *Fed. Trade Comm'n v. D-Link Sys.*, No. 3:17-cv-00039-JD (N.D. Cal. Sept. 19, 2017).

11 *See, e.g.*, Ala. Code § 8-38-9(b)(2); Ariz. Rev. Stat. § 18-552(L); Ark. Code Ann. § 4-110-108; Colo. Rev. Stat. § 6-1-716(4); Conn. Gen. Stat. § 36a-701b(g); 6 Del. C. § 12B-104; Fla. Stat. § 501.171(9); Idaho Code § 28-51107; Ind. Code Ann. § 24-4.9-4-2; Kan. Stat. Ann. § 50-7a,02(g); Me. Rev. Stat. tit. 10 § 1349; Mass. Ann. Laws ch. 93H § 6; Mich. Comp. Laws Serv. § 445.63; Minn. Stat. Ann. § 325E.61; Miss. Code Ann. § 75-24-29; Mo. Rev. Stat. § 407.1500; Mont. Code. Ann. § 30-14-1705; Neb. Rev. Stat. Ann. § 87-806; Nev. Rev. Stat. Ann. 603A.360; N.M. Stat. Ann. § 57-12C-11; N.Y. Gen. Bus. Law §899-aa(6)(a); N.D. Cent. Code § 51-30-07; Ohio Rev. Code Ann. § 1349.192; Okla. Stat. tit. 24, § 165; Or. Rev. Stat. Ann. § 646A.624; 73 Pa. Stat. § 2308; SD Codified Laws § 22-40-25; Tenn. Code Ann. § 47-18-2105; Tex. Bus. & Com. Code § 521.151; Utah Code Ann. § 13-44-301; Vt. Stat. Ann tit. 9, § 2435(g); Wash. Rev. Code Ann. § 19.255.010(17). W.Va. Code § 46A-2A-104; Wyo. Stat. Ann. § 40-12-502(f).

12 *E.g.,* Fla. Stat. Ann. § 501.171(9)(b).

13 *See, e.g.,* D.C. Code § 28-3853.

14 Iowa Code § 715C.2(7)(d).

15 *See, e.g.*, Alaska Stat. § 45.48.080; Cal. Civ. Code § 1798.84(b); D.C. Code § 28-3853(a); Haw. Rev. Stat. Ann. § 487N-3; 815 Ill. Comp. Stat. Ann. 530/20; La. Rev. Stat. Ann. § 51:3075; Md. Code Ann., Com. Law § 14-3508; N.H. Rev. Stat. Ann. § 359-C:21; N.C. Gen. Stat. § 75-65(i); 11 R.I. Gen. Laws § 49.3-5; S.C. Code Ann. § 39-1-90(G); Tenn. Code Ann. § 47-18-2104; Wash. Rev. Code Ann. § 19.255.010(13); Wis. Stat. § 134.98.

16 N.H. Rev. Stat. Ann. § 359-C:21.

17 *See, e.g., Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011); Am. Compl., *Beckett v. Aetna, Inc.*, No. 2:17-cv-03864 (E.D. Pa. Dec. 5, 2017).

18 *See, e.g., Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 690-91 (7th Cir. 2015); Am. Compl., *Giancola v. Lincare Holdings Inc.*, No. 8:17-cv-02427 (M.D. Fla. Dec. 29, 2017).

19 *See Remijas*, 794 F.3d 688.

20 *See id.*; *see also Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 386 (6th Cir. 2016); Am. Compl., *Delkener v. Cottage Health Sys.*, No. 30-2016-00847934 (Cal. Sup. Ct. Feb. 9, 2017); Am. Compl., *Beckett v. Aetna, Inc.*, No. 2:17-cv-03864 (E.D. Pa. Dec. 5, 2017).

21 Office of the Governor of Ohio, Press Release, *Kasich Announces Actions on Eleven Bills* (Aug. 3, 2018), https://governor.ohio.gov/Media-Room/Press-Releases/ArticleId/966/kasich-announces-actions-on-eleven-bills-8-3-18.

22 The Ohio Data Protection Act, Sub. S.B. 220, 132nd Gen. Assemb. § 3(B) (2018).

23 *Id.*

24 Ohio Rev. Code Ann. § 1354.04.

25 Ohio Rev. Code Ann. § 1354.02(D)(2).

26 *State ex rel. Plain Dealer Publ. Co. v. City of Cleveland*, 75 Ohio St. 3d 31, 33 (1996).

27 *E.g.*, *Ex parte Gadsden Country Club*, 14 So. 3d 830, 834 (Ala. 2009).

28 *E.g., Meacham v. Knolls Atomic Power Lab.*, 554 U.S. 84, 91-92 (2008).

29 Ohio Rev. Code Ann. § 1354.01(B).

30 Ohio Rev. Code Ann. § 1354.02(A). "Personal information" is defined as an individual's name when linked to either that individual's social security number, driver's license number, or credit or debit card account number and account passcode. Ohio Rev. Code Ann. § 1354.01(D); Ohio Rev. Code Ann. § 1349.19(7)(a). "Restricted information" is information about an individual, other than personal information, that could be used to identify that individual. Ohio Rev. Code Ann. § 1354.01(E).

31 *See, e.g.*, *5th Hearing on S.B. 220 Before the S. Comm. on Gov't Oversight and Reform*, 132nd Gen. Assemb. (2018) (statement of Mike DeWine, Att'y Gen. of Ohio) ("Businesses have to show action . . . to be reasonably compliant, a business must remain vigilant.").

32 Ohio Rev. Code Ann. § 1354.02(B)(3).

33 Ohio Rev. Code Ann. § 2913.49.

34 Ohio Rev. Code Ann. § 1354.02(C).

35 *1st Hearing on S.B. No. 220 Before the S. Comm. on Gov't Oversight and Reform*, 132nd Gen. Assemb. (2017) (statement of Sens. Kevin Bacon and Bob Hackett, bill sponsors) ("Understandably, the cybersecurity needs for a business varies with the size of the business and the type of industry that the business engages in. As a result, S.B. 220 is 'scalable' to the needs of a particular business.").

36 Ohio Rev. Code Ann. § 1354.02(C).

37 *5th Hearing on S.B. No. 220 Before the S. Comm. on Gov't Oversight and Reform*, 132nd Gen. Assemb. (2018) (statement of Mike DeWine, Att'y Gen. of Ohio) (stating that the affirmative defense "is not a motion to dismiss issue, rather, it will be decided by the trier of fact at trial.").

38 Ohio Rev. Code Ann. §1354.02(A)(1).

39 Ohio Rev. Code Ann. §1354.03(A).

40 Ohio Rev. Code Ann. § 1354.03(B).

41 Ohio Rev. Code Ann. § 1354.03(B)(1)(a), (d).