The Banking Law Journal

Established 1889

An A.S. Pratt™ PUBLICATION **JANUARY 2022**

LexisNexis

THE BANKING LAW JOURNAL

VOLUME 139 **NUMBER 1** **January 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Matthew T. Burke at ..... (800) 252-9257
Email: ..... matthew.t.burke@lexisnexis.com
Outside the United States and Canada, please call . . . . . (973) 820-2000

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
Customer Service Website . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

ISBN: 978-0-7698-7878-2 (print)
ISSN: 0005-5506 (Print)

Cite this publication as:

The Banking Law Journal (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub.4815)

Editor-in-Chief, Editor & Board of Editors

THE BANKING LAW JOURNAL (ISBN 978-0-76987-878-2) (USPS 003-160) is published ten times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to bankers, officers of financial institutions, and their attorneys. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, LexisNexis Matthew Bender, 230 Park Ave, 7th Floor, New York, NY 10169.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, A.S. Pratt & Sons, 805 Fifteenth Street, NW, Third Floor, Washington, DC 20005-2207.

"Safe Harbor" Ports in a Cybersecurity Litigation Storm

Molly McGinnis Stine and Hannah Oswald*

There has been a recent trend of legislatures considering or passing laws that incentivize companies to voluntarily take cybersecurity measures to prevent cyberattacks. Specifically, a number of states have proposed safe harbors or affirmative defenses that shield companies from some types of liability when they maintain a cybersecurity program that meets certain prescribed standards. The authors of this article discuss safe harbors adopted in Ohio, Utah, and Connecticut and similar bills that have been proposed in other states.

Every organization with an online presence needs to continuously think about its cybersecurity. The number of cyberattacks spiked significantly during the COVID-19 pandemic with an estimated global loss of nearly $1 trillion.[1] These assaults are expected to keep increasing and some reports estimate that cybercrime will cost the world $10.5 trillion annually by 2025.[2]

Cyberattacks are very costly for companies not only in terms of monetary losses, but also in terms of reputational damage, lost time, and exposure to potential lawsuits. Indeed, legislatures across the country have enacted a variety of laws to respond to the growing threat from cyberattacks. For example, over a number of years, all states have adopted notification laws that require companies to notify individuals of certain data breaches.[3] Other legislatures

---

* Molly McGinnis Stine is a partner at Locke Lord LLP and a member of the firm's Insurance: Litigation and Counseling Practice Group, the Steering Committee of the firm's Privacy & Cybersecurity Practice Group, its Incident Response Team, and its New York Department of Financial Services and California Consumer Privacy Act initiatives. Hannah Oswald is an associate at the firm focusing her practice on litigation and arbitration, including matters involving breach of contract, trade secret misappropriation, loss-sensitive insurance programs and insurance insolvency litigation. Resident in the firm's office in Chicago, the authors may be reached at mmstine@lockelord.com and hannah.oswald@lockelord.com, respectively.

[1] Tonya Riley, *The Cyber Security 202: Global losses from cybercrime skyrocketed to nearly $1 trillion in 2020, new report finds,* Washington Post (Dec. 7, 2020), https://www.washingtonpost.com/politics/2020/12/07/cybersecurity-202-global-losses-cybercrime-skyrocketed-nearly-1-trillion-2020/.

[2] Chuck Brooks, *Alarming Cybersecurity Stats: What You Need to Know for 2021*, Forbes (Mar. 3, 2021), https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-what-you-need-to-know-for-2021/?sh=1a6d408e58d3.

[3] *Security Breach Notification Laws*, NCSL (April 15, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

have enacted regulations that require companies to meet certain cybersecurity standards.[4]

Notably, there has also been a recent trend of legislatures considering or passing laws that incentivize companies to voluntarily take cybersecurity measures to prevent cyberattacks.

Specifically, a number of states have proposed safe harbors or affirmative defenses that shield companies from some types of liability when they maintain a cybersecurity program that meet certain prescribed standards. Ohio, Utah, and Connecticut are the first three states to adopt these safe harbors and similar bills have been proposed in other states.

ENACTED SAFE HARBORS: OHIO, CONNECTICUT, AND UTAH

Ohio was the first state to pass a cybersecurity affirmative defense in 2018.[5] Connecticut[6] and Utah[7] recently adopted their acts in 2021. The laws enacted in Connecticut and Utah are generally modeled after Ohio's statute. The Ohio statute provides an "affirmative defense" to companies with a prescribed written cybersecurity program that face tort claims arising out of a data breach. If proven by the company, the safe harbor would bar tort claims asserted against it. The defense applies only to tort claims related to allegations that the company failed to implement reasonable security controls. To invoke the affirmative defense, the company must "create, maintain and comply with a written cyber security program"[8] that meets the following requirements:

- The program must have administrative, technical, and physical components that protect personal or restricted information.
- The program must meet one or more of three approaches, to the extent that the available approaches apply to a given entity and its information. It must reasonably conform to the current version of one or more of the enumerated frameworks for cybersecurity, including NIST, FedRAMP Security Assessment Framework, or ISO/IEC. Alternatively, if the personal information covered by the program is regulated by the federal or state government, then the company must comply with the security

---

[4] *See, e.g.*, "Stop Hacks and Improve Electronic Data Security Act" (SHIELD ACT), N.Y. Gen. Bus. Law § 899-bb (effective March 21, 2020).

[5] Ohio Rev. Code Ann. § 1354.02 (effective date November 2, 2018).

[6] 2021 CT H 6607, Public Act No. 21-119 (effective date October 1, 2021).

[7] Utah Code Ann. § 78B-4-703 (effective date May 5, 2021).

[8] Ohio Rev. Code Ann. § 1354.02(A)(1); Connecticut Public Act No. 21-119 § 5(b).

requirements of HIPAA, the Gramm-Leach-Bliley Act, or other applicable federal or state regulations. Further, if the personal information is protected by the PCI data security standard, then the program must reasonably comply with the current version of the PCI data security standard.

- Where a company models its program after one of the enumerated frameworks and that framework is amended, the company must reasonably conform to the amended guidelines within one year. This requirement provides a grace period while also ensuring that companies stay up to date on industry standards for their cybersecurity programs.

The Utah affirmative defense differs in four respects.

First, the Utah affirmative defense does not apply where the entity had actual notice of a security threat and failed to take remedial efforts to redress it.

Second, the Utah statute is not expressly limited to tort claims. Instead, the law apparently applies to any claims alleging failure to implement reasonable security measures that results in a data breach. As such, the Utah affirmative defense may have broader applicability than the Ohio and Connecticut statutes, although this has not yet been tested.

Third, the Utah affirmative defense allows companies to comply with one or more of four approaches, rather than three. Specifically, a company can either comply with one of the three approaches covered by the Ohio statute or it can implement a "reasonable security program" that meets certain statutory requirements that are similar to the industry-recognized frameworks.

Finally, while Ohio and Connecticut require that a company "create, maintain and comply" with their cybersecurity program, the Utah statute requires that companies "creates, maintains and *reasonably* complies"[9] with their cybersecurity program. The presence of the word "reasonably" could give a company an opportunity to assert their "reasonable compliance" under the Utah statute if their practices "reasonably" deviate from their written cybersecurity protocols.

The Connecticut statute also has three variations.

First, unlike the Ohio or Utah law, the Connecticut statute offers a more limited protection by providing a safe harbor defense only against punitive damages for tort claims.

Second, the Connecticut statute stipulates that the affirmative defense will not apply where the company's failure to implement cybersecurity controls was the result of gross negligence or willful or wanton conduct.

---

[9] Utah Code Ann. § 78B-4-702(1).

Finally, the Connecticut statute only provides a grace period of six months, rather than a full year as in the other two states, for companies to update their programs after a framework is amended.

Overall, all three statutes generally encourage companies to develop and maintain a cybersecurity program that conforms to industry standards.

PROPOSED SAFE HARBORS: IOWA, NEW JERSEY, GEORGIA, AND ILLINOIS

Several states have proposed similar safe harbor laws. Specifically, Iowa[10] and New Jersey[11] both proposed similar bills in 2020, and Georgia[12] and Illinois[13] introduced legislation in 2021. While these proposals all provide an affirmative defense to companies with cybersecurity programs, the requirements vary between states. For example, the Georgia bill does not specifically list the industry standard frameworks that are referenced in the Ohio, Utah, and Connecticut acts.

Instead, the Georgia bill requires a "reasonable" framework that takes into consideration the size and complexity of the company and sensitivity of the information protected. While this approach is integral to the industry standard frameworks in the other states' laws, the Georgia bill apparently chose not to limit the choices to those particular frameworks.

INCENTIVIZING CYBERSECURITY PRACTICES

Overall, it is likely that states will continue to emphasize the importance of cybersecurity programs. Some laws could encourage stronger cybersecurity by providing an affirmative defense. Others could mandate certain cybersecurity practices without affording an explicit affirmative defense. No matter the specifics of a statute or even in the absence of a statute, companies will be well-served to implement an industry-recognized cybersecurity framework. Not only will the frameworks likely reduce the frequency or severity of data breaches, but they may also improve a company's defense against alleged liability in the event a data breach does occur.

---

[10] Iowa S.F. 2073, https://www.legis.iowa.gov/legislation/BillBook?ba=SF%202073&ga=88.

[11] 2020 New Jersey S.B. 3062, https://www.njleg.state.nj.us/2020/Bills/S3500/3062_I1.HTM.

[12] GA S.B. 52, https://www.legis.ga.gov/legislation/59139.

[13] Illinois H.B. 3030, https://www.ilga.gov/legislation/BillStatus.asp?DocNum=3030&GAID=16&DocTypeID=HB&SessionID=110&GA=102/a.