New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 263—NO. 87
WEDNESDAY, MAY 6, 2020

CYBERSECURITY

Expert Analysis

Navigating the Ambiguous Requirement Of 'Reasonable Security' Measures While Protecting Personal Information

BY STEPHEN E. BREIDENBACH AND TERESE L. ARENTH

Over the last couple of years, cybersecurity laws have commonly required that sensitive information be protected through the use of "reasonable security." Business owners have likely heard that they are required to protect sensitive information, but may not understand how to specifically go about this. The term "reasonable security" often has been left ambiguous and guidance as to what is required for your specific business might be hard to find.

As a starting point, it is important to understand that what constitutes appropriate security safeguards may depend upon the type of information that you collect and the type of business that you operate. For example, if you are a medical professional, or holding information for a medical professional, you may be subject to the HIPAA Security Rule (HIPAA) (which lists specific safeguards for the protection of electronic health information), and if you are a financial institution, or holding information for a financial institution, you may need to comply with the Gramm-Leach-Bliley Act (GLBA) (which identifies specific requirements and safeguards for the protection of customer information). See 45 CFR Part 160 and Part 164, Subparts A and C (HIPPA); 15 U.S.C §6801(b) (GLBA). Administrative guidance elaborates on each of these laws by laying out certain cybersecurity safeguards that should be put in place, including but not limited to: access controls, monitoring solutions and disaster recovery procedures. See Security Rule Guidance Material, U.S. Department of Health & Human Services; 12 C.F.R. Pt. 364, App. A. Further, under both HIPAA and GLBA, if any of the regulated entity's vendors receive protected information from that regulated entity, then the regulated entity is required to contractually bind that vendor in writing to treat the protected information in the same manner as the regulated entity. See 12 C.F.R. Pt. 364, App. A III.D.; 45 C.F.R. 164.502(e).

In addition to laws and regulations that require entities to implement appropriate safeguards, attorneys' ethical requirements provide guidance on determining what constitutes reasonable security and read in the requirements to implement specific cybersecurity safeguards. See Formal Opinion 483, American Bar Association (Oct. 17, 2018); Formal Opinion 477R, American Bar Association (revised May 22, 2017).

Even if, however, you are not subject to the laws and regulations referenced above, if you collect private information from a New York state resident, you are still required to implement reasonable security. As

of March 21, 2020, the New York "Stop Hacks and Improve Electronic Data Security Act" (SHIELD Act) specifically requires that any person or business that collects private information of a New York resident must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information, including but not limited to, disposal of the data. N.Y. Gen. Bus. Law §899-bb. Private information includes: (1) Social Security numbers; (2) driver's license numbers or non-driver identification card numbers; (3) account numbers, credit or debit card numbers, if those numbers would permit access to an individual's financial account; (4) biometric information; or (5) a user name or email address in combination with information that would permit access to an online account. N.Y. Gen. Bus. Law §899-aa(1)(b). The SHIELD Act enumerates several administrative, technical and physical safeguards that larger businesses must develop, implement and maintain. These safeguards include, but are not limited, to: identifying reasonably foreseeable internal and external risks; assessing risks in network and software design, information processing, transmission, storage and disposal; and detecting, preventing and responding to attacks, system failures and intrusions. N.Y. Gen. Bus. Law §899-bb(2). For small businesses, the Act simply provides that "the small business's security program [should contain] reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers." N.Y. Gen. Bus. Law §899-bb(2)(c). A small business is any person or business with fewer than 50 employees, less than $3 million in gross annual revenue in each of the last three fiscal years, or less than five million dollars in year-end total assets.

> The term "reasonable security" often has been left ambiguous and guidance as to what is required for your specific business might be hard to find.

Despite all of these legal requirements and safeguards, what constitutes "reasonable security" remains ambiguous to this day. As previously noted, most laws currently provide that the safeguards implemented by a business should be reasonable and appropriate given the size of the business and the information they collect. Agencies such as the Federal Trade Commission (FTC) have recognized that there is no such thing as perfect security, but that security is a continuing process that requires the business to detect risks and adjust their safeguards accordingly. See Andria Aria, The NIST Cybersecurity Framework and the FTC, Federal Trade Commission (Aug. 31, 2016).

While these sources do not provide a ceiling for the safeguards that a business should have in place, they appear to have at least begun the creation of a floor. For years, the FTC has been the primary enforcer of cybersecurity regulations. The FTC has brought numerous actions for deceptive or unfair business practices under the FTC Act for businesses that claimed—but failed—to have reasonable security in place. In the case of *F.T.C. v. Wyndham Worldwide*, the FTC provided some guidance on where the threshold for reasonable security can be drawn from. Therein, the FTC provided that "the Court can evaluate the reasonableness of Hotels and Resorts' data-security program in view of the following: (1) industry guidance sources that Hotels and Resorts itself seems to measure its own data-security practices against; and (2) the FTC's business guidance brochure and consent orders from previous FTC enforcement actions." *F.T.C. v. Wyndham Worldwide*, 10 F. Supp. 3d 602, 616-17 (D.N.J. 2014), aff'd, 799 F.3d 236 (3d Cir. 2015); see also Wyndham Settles

FTC Charges It Unfairly Placed Consumers' Payment Card Information at Risk, Federal Trade Commission Dec. 9, 2015.

Consequently, as best practices, businesses seeking to come into compliance are well-advised to draw knowledge from the publications of their regulators and to also consult the FTC's published guidance on what their type of business is required to implement. Many of these FTC guidelines go into greater detail of the types of safeguards businesses should implement, including: FTC's guidelines for small businesses and the FTC's explanatory material on the Cybersecurity Framework published by the National Institute of Standards and Technology (NIST) (a voluntary framework that includes standards, guidelines and best practices to manage cybersecurity risk). See also Financial Institutions and Customer Information: Complying With the Safeguards Rule, Federal Trade Commission; Start With Security: A Guide for Business, Federal Trade Commission.

Bear in mind that if you collect information from individuals located in other states, you will also have to evaluate the laws of those states, which may be stricter than the laws of the state in which your company has its principal place of business. For example, unlike the SHIELD Act, the California Consumer Privacy Act of 2018 (CCPA) provides a private right of action to California residents whose personal information was subject to "an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices." Cal. Civ. Code §1798.150(a)(1). This private right allows a successful plaintiff to recover damages in the amount of "not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater." Cal. Civ. Code §1798.150(a)(1)(A). To put this in context by way of example, if a compromised database has information on a mere 10,000 people, a business could be subject to damages of $1,000,000 to $7,500,000. In contrast, New York's SHIELD Act imposes civil penalties of not more than $5,000 for failing to implement reasonable security and, under New York's Breach Notification law, potential penalties are the greater of $5,000 or up to $20 per instance for failing to notify affected consumers of a data breach, not to exceed $250,000. N.Y. Gen. Bus. Law §899-aa(6)(a) and §350-d.

Further, states may differ in their interpretation of "reasonable security". In California, for example, in the California Data Breach Report 2012-2015, California's Attorney General Kamala D. Harris provided that "the 20 controls in the Center for Internet Security's Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the controls that apply to an organization's environment constitutes a lack of reasonable security." See Kamala Harris, California Data Breach Report 2012-2015 (February 2016), at pg. v.

Although the CCPA just became effective on Jan. 1, 2020, the CCPA's private right of action has already generated a number of cases. While a New York company that is not conducting business in California may not be subject to California jurisdiction, the cases spawned from the CCPA could likely influence the interpretation of what constitutes reasonable security by other jurisdictions.

As most businesses collect and maintain sensitive personal information about their customers, the key takeaway is to first assess the type of business that you operate and the types of personal information that you collect. From that starting point, develop, implement and maintain a sound security plan to collect only the information that you need, to keep that information safe, and to dispose of it securely. This will form the foundation to help your business meet its legal obligations and protect that sensitive data.

STEPHEN E. BREIDENBACH *is an associate and* TERESE L. ARENTH *is a partner at Moritt Hock & Hamroff.*