EPSTEIN BECKER GREEN

Employment, Labor & Workforce Management

ACT NOW ADVISORY

# New York Joins the Wave of States Requiring Businesses to Adopt Reasonable Cybersecurity Safeguards to Protect Private Information

**August 12, 2019**

**By Brian G. Cesaratto**

---

New York has joined California, Massachusetts, and Colorado in adopting a law that requires businesses that collect private information on residents to implement reasonable cybersecurity safeguards to protect that information. New York's law mandates the implementation of a data security program, including measures such as risk assessments, workforce training, incident response planning and testing, and secure data destruction protocols. Businesses should immediately begin the process to comply with the law's requirements effective March 21, 2020. Notably, New York's law covers all businesses, employers, or individuals, regardless of size or location, who collect private information on New York State residents.

The Stop Hacks and Improve Electronic Data Security Act (or "SHIELD Act"), signed into law on July 25, 2019, requires implementation of an information security program to protect "private information," defined as:

(i) any individually identifiable information, such as a name, personal mark, number, or other identifier that can be used to identify a natural person, **coupled with the following:** (a) a Social Security number; (b) a driver's or non-driver identification card number; (c) an account number, or a credit or debit card number in combination with any security code, access code, password, or any other information that would permit access to the individual's financial account; or (d) biometric information (such as a fingerprint, voice print, retina or iris image, or other electronic measurements of unique physical characteristics);

(ii) any individually identifiable information **coupled with** an account number, or a credit or debit card number if any "circumstances exist" wherein such number could be used to access an individual's financial account **even without** additional identifying information, or a security code, access code, or password; **or**

(iii) a username or email address **in combination with** a password or security question and answer that would permit access to an online account.

The SHIELD Act broadly requires that "any person or business" that owns or licenses computerized data that includes private information of a New York State resident "shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information."

In order to achieve compliance, an organization must implement a data security program to protect private information that incorporates:

(i) reasonable **administrative safeguards** that may include designation of one or more employees to coordinate the security program, identification of reasonably foreseeable external and insider risks, assessment of existing safeguards, workforce cybersecurity training, and selection of service providers capable of maintaining appropriate safeguards and requiring those safeguards by contract;

(ii) reasonable **technical safeguards** that may include risk assessments of network, software design, and information processing, transmission, and storage; implementation of measures to detect, prevent, and respond to system failures; and regular testing and monitoring of the effectiveness of key controls; and

(iii) reasonable **physical safeguards** that may include detection, prevention and response to intrusions, and protections against unauthorized access to or use of private information during or after collection, transportation, and destruction or disposal of the information.

Small businesses of fewer than 50 employees, less than $3 million in gross revenues in each of last three fiscal years, **or** less than $5 million in year-end total assets are covered but may scale their data security programs according to their size and complexity, the nature and scope of their business activities, and the nature and sensitivity of the information collected.

Organizations that are covered by and in compliance with the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act ("HIPAA"), and/or the New York State Department of Financial Services ("NYSDFS") cybersecurity regulations (23 NYCRR 500) will be deemed in compliance with the SHIELD Act. The SHIELD Act's reach includes health care and financial institutions subject to other data protection requirements, but it does not require the implementation of additional cybersecurity safeguards as long as the organizations are in compliance with those data protection requirements. Absent clarifying guidance, health care and financial services institutions will need to implement the SHIELD Act requirements as to information systems holding private information that is not also subject to HIPAA, Gramm-Leach-Bliley, or NYSDFS

regulations (e.g., a financial institution's personnel systems holding biometric or other private information on its employees—which are not subject to mandated protections for systems holding financial customers' information—will need to independently meet the SHIELD Act's requirements).

Failure to implement a compliant information security program may result in an action by the New York State Attorney General. Injunctive relief and civil penalties of up to $5,000 may be imposed against an organization and individual employees for "each violation." Depending on how the Attorney General seeks to apply this provision, this could potentially lead to significant monetary penalties for entities and their employees who fail to take required protective measures, including when those failures lead to a data breach. We can expect vigorous enforcement because the Attorney General submitted the SHIELD Act as an agency-sponsored bill to keep pace with the use and dissemination of private information. Indeed, absent future clarification, the Attorney General may seek civil penalties to enforce reasonable cybersecurity safeguards even in the absence of a data breach. Of course, any enforcement activity by the Attorney General's office will also have other damaging consequences, such as reputational harm, and raise supply chain issues with the organization's business partners.

The SHIELD Act also amends New York State's existing data breach notification provisions, broadening the existing definition of data "breach" to reach not only unauthorized acquisition but also any unauthorized "access" to the private information.

**What Businesses and Employers Should Do Now**

- Identify information systems containing private information on New York State consumers and employees.

- Conduct a formalized risk assessment, considering anticipated threats to those systems and likely impacts from unauthorized access or acquisition.

- Consider the effectiveness of existing cybersecurity safeguards in light of the risk.

- Adopt a formalized information security program based on the results of the risk assessment that includes workforce cybersecurity training, external and insider threat prevention (including from employees and other trusted insiders), network and application security, encryption and cryptographic key management, evaluation of business partners' cybersecurity measures and imposition of protective contractual requirements, and robust incident response planning and testing (tailored to the statute's new broader definition of data "breach").

- For those businesses and employers that are subject to ***both*** the California Consumer Privacy Act ("CCPA"), including recent proposed amendments, and SHIELD Act requirements, develop a strategy for complying with applicable

provisions of both laws. The CCPA becomes effective on January 1, 2020, with the SHIELD Act effective shortly thereafter, on March 21, 2020.

****

For more information about this Advisory, please contact:

**Brian G. Cesaratto**
New York
212.351.4921
bcesaratto@ebglaw.com

*This document has been provided for informational purposes only and is not intended and should not be construed to constitute legal advice. Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.*

**About Epstein Becker Green**
Epstein Becker & Green, P.C., is a national law firm with a primary focus on health care and life sciences; employment, labor, and workforce management; and litigation and business disputes. Founded in 1973 as an industry-focused firm, Epstein Becker Green has decades of experience serving clients in health care, financial services, retail, hospitality, and technology, among other industries, representing entities from startups to Fortune 100 companies. Operating in locations throughout the United States and supporting domestic and multinational clients, the firm's attorneys are committed to uncompromising client service and legal excellence. For more information, visit www.ebglaw.com.