LOEB & LOEB LLP

Privacy

MARCH 2020

NY SHIELD Act's Data Security Requirements Are Effective March 21 – Is Your Organization Ready?

The New York "Stop Hacks and Improve Electronic Data Security Act" or "SHIELD Act" expands data breach reporting requirements and requires organizations to implement an information security program to protect the "private information" of New York State residents, including employee and consumer data. The law's data security requirements will take effect on March 21, 2020. With many New Yorkers working remotely, the risk for cybersecurity incidents is even higher than usual. The requirements of New York's law may serve as a guide to all companies looking to tighten their controls amid an increase in vulnerability.

Key Takeaways:

- Expands the definition of private information to include biometric information and online account information.
- Businesses will need to implement a data security program that includes reasonable administrative, technical and physical safeguards. The law provides examples of the safeguards required in each category. Companies should consider performing an analysis to identify whether there are gaps in their program.
- Failure to implement a compliant information security program is enforced by the New York State Attorney General and may result in injunctive relief and civil penalties.

What Data Is Covered?

The SHIELD Act's requirements cover "private information," which is:

- any individually identifiable information, such as name, number or other identifier, coupled with:
  - Social Security number; driver's or nondriver's identification card number or account number; credit or debit card number in combination with any security code, access code, password or other information that would permit access to the individual's financial account; or biometric information (such as fingerprint, voice print, retina or iris image) or
  - an account, credit or debit card number, if 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
- a username or email address in combination with a password or security question and answer that would permit access to an online account.

What Security Controls Are Required?

While many states' laws call for non-specified "reasonable" data security requirements, the SHIELD Act provides a range of measures illustrated by examples. To achieve compliance, an organization must implement a data security program that includes:

- reasonable **administrative safeguards**, such as:
  - designating an employee to coordinate the security program;
  - identifying reasonably foreseeable internal and external risks;
  - assessing the sufficiency of safeguards in place to control identified risks;
  - training and managing employees in the security program practices and procedures;
  - selecting service providers capable of maintaining appropriate safeguards and requiring those safeguards by contract; and
  - adjusting the security program in light of business changes or new circumstances;
- reasonable **technical safeguards**, such as:
  - assessing risks in network and software design;
  - assessing risks in information processing, transmission and storage;
  - detecting, preventing and responding to attacks or system failures; and
  - regularly testing and monitoring the effectiveness of key controls, systems and procedures;
- reasonable **physical safeguards**, such as:
  - assessing risks of information storage and disposal;
  - detecting, preventing and responding to intrusions;
  - protecting against unauthorized access to or use of private information during or after the collection, transportation, and destruction or disposal of the information; and
  - disposing of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

To determine a baseline level of reasonable security, covered entities should conduct gap assessments of current security practices and vendor agreements against the act's exemplary lists, relying on existing compliance efforts where possible.

Are There Any Exemptions?

The SHIELD Act offers some flexibility for certain types of businesses. Regulated entities 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 cybersecurity regulations shall be deemed in compliance with the SHIELD Act.

There is also an exception for small businesses (organizations with fewer than 50 employees, less than $3 million in annual gross revenue or less than $5 million in year-end total assets). A small business can comply with the SHIELD Act by implementing reasonable administrative, technical and physical safeguards that are appropriate for 1) the size and complexity of their business, 2) the nature and scope of the small business's activities, and 3) the sensitivity of the personal information the small business collects from or about consumers.

The original draft of the SHIELD Act also provided a safe harbor for entities that could demonstrate certified compliance with industry-recognized security standards like the NIST Cybersecurity Framework or ISO 27001 (in addition to the safe harbor for compliant-regulated entities discussed above), but this provision was removed before the SHIELD Act was signed into law. This change makes it clear that while adopting industry-recognized security standards can help companies comply with the SHIELD Act, it does not guarantee compliance. Generally, all organizations subject to the SHIELD Act will have to demonstrate compliance with applicable data security laws or the SHIELD Act's own data security program requirements in order to avoid violating the law.

What Are the Penalties?

Compliance with the law requiring an appropriate information security program is enforced by the New York State Attorney General, and failure to comply may result in injunctive relief and civil penalties (up to $5,000 for knowing or reckless violations of the SHIELD Act's data security requirement). While the SHIELD Act provides that nothing in the security safeguards section "shall create a private right of action," any violation of the statute is deemed a violation of New York's Deceptive Acts & Practices law. We can expect that private litigants will look to this language to bring violations of the safeguards section into a data breach lawsuit or other claims.

If you have any questions about the SHIELD Act or are looking for resources to conduct an assessment of your security practices, please reach out to a member of Loeb's Privacy team.

Related Professionals

For more information, please contact:

Jessica Lee	jblee@loeb.com
Chanda Marlowe	cmarlowe@loeb.com
Jeffrey A. Hamburg	jhamburg@loeb.com

6282 REV1 03-25-2020