CARLTON FIELDS

Are You in Compliance With New York's Newest Requirement to Develop, Maintain, and Implement Reasonable Safeguards to Protect New Yorkers' Private Information?

CYBERSECURITY AND PRIVACY | TECHNOLOGY | TECHNOLOGY & TELECOMMUNICATIONS | APRIL 2, 2020

Michael L. Yaeger

Katelyn M. Sandoval

The new data security requirements provision of New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act went into full force as of March 21, 2020, and all people and businesses, regardless of the state in which they reside, must comply with the new rules if they handle the private information of New York residents. *See* N.Y. Gen. Bus. Law § 899-bb. The SHIELD Act does not provide for a private right of action, but it does require that covered people and businesses adhere to a more robust data security program, and the state attorney general has the power to enforce the statute. With this last piece of the SHIELD Act recently taking effect, people and businesses everywhere are now on the hook for failing to safeguard their New York customers' private information properly.

The SHIELD Act requires that any "person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data." The act, unsurprisingly, does not mandate what "reasonable safeguards" a person or business must develop, maintain, and implement. However, it does provide examples of some reasonable administrative, technical, and physical safeguards, including:

Administrative safeguards:

1. Designating one or more employees to coordinate the security program;
2. Identifying reasonably foreseeable internal and external risks;
3. Assessing the sufficiency of safeguards in place to control the identified risks;
4. Training employees;
5. Selecting service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and
6. Adjusting the security program in light of business changes or new circumstances.

Technical safeguards:

1. Assessing risks in network and software design;
2. Assessing risks in information processing, transmission, and storage;
3. Detecting, preventing, and responding to attacks or system failures; and
4. Regularly testing and monitoring the effectiveness of key controls, systems, and procedures.

Physical safeguards:

1. Assessing risks of information storage and disposal;
2. Detecting, preventing, and responding to intrusions;
3. Protecting against unauthorized access to or use of private information during or after the collection, transportation, and destruction or disposal of the information; and
4. 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.

Small businesses are afforded some leeway here. Companies with fewer than 50 employees, or less than $3 million in gross annual revenue in the last three fiscal years, or less than $5 million in year-end total assets (under GAAP) qualify as small.

They may adapt the above “reasonable safeguards” to appropriately match the size and nature of their business and the sensitivity of personal information that they collect about consumers.

In addition, businesses will be deemed to be compliant with the reasonable safeguards requirement if they are in compliance with another state or federally mandated data security program, including the Gramm-Leach-Bliley Act, HIPAA, or New York Department of Financial Services’ Cybersecurity Regulation.

If you have not yet examined your compliance with the SHIELD Act, here are a few tips to help jumpstart the process:

- Assemble a multidisciplinary team, which should include not just information technology personnel but also people from other functions, such as legal, to review your compliance.
- Determine if you are already following recognized data security standards, such as the National Institute of Standards and Technology (NIST) or the Center for Internet Security (CIS). If so, you may already be following the SHIELD Act’s “reasonable safeguards” requirements.
- Consider hiring an outside vendor to conduct a risk assessment of your business and identify the threats and vulnerabilities of your data security program.

As businesses increase their use and dependence on remote work and information technology — a trend accelerated by the current coronavirus pandemic — privacy and cybersecurity becomes more important, and more important to regulators.

By focusing on the development and enforcement of their cybersecurity and data privacy policies, businesses can take comfort in knowing they are serving their urgent business and regulatory needs at the same time.