BEECHER CARLSON

NEW YORK'S SHIELD ACT

Following the path of California, New York has expanded its data privacy and compliance regulations by passing the Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act"), which will go into effect March 21, 2020. The SHIELD Act will impose additional data security requirements on subject entities and will simultaneously broaden what is considered "Private Information" and what constitutes a "Breach."

The SHIELD Act will also expand what businesses the Act will apply to. Going forward, New York's breach notification requirements will apply to any person or business that owns or licenses private information of a New York resident. The Act will help enrich the protections for New York residents and will extend additional data security requirements to businesses that do not maintain a physical presence within New York or a nexus to the state. The law previously only applied to those conducting business in New York.

NEW CYBERSECURITY SAFEGUARDS

Who Must Comply with the Safeguards?

The Act's new cybersecurity safeguards will likely affect most businesses in New York or those that maintain the data of New York residents with few exceptions. Currently, there is no such requirement under New York law; however, entities that are already subject to and comply with the requirements of HIPAA, Hi-TECH, Gramm-Leach-Bliley, New York's Title 23, Part 500, or any other federal or New York State data security rule or regulations will be required to also comply with the SHIELD Act. There are some exceptions in the Act for "small businesses." The Act defines "small businesses" as ones with fewer than 50 employees, less than $3 million in gross annual revenue over the past three years, or less than $5 million in year-end total assets.

What is Required?

Businesses will be required to develop, implement, and maintain "reasonable safeguards to protect the security, confidentiality, and integrity" of New York residents' data, including its disposal. The Act identifies three essential parts of a data security program:

1. **"Reasonable administrative safeguards:"** employing qualified personnel; adopting data security policies and procedures, employee training programs, and third-party service provider cyber risk management controls

2. **"Reasonable technical safeguards:"** installing network and software design controls; implementing procedures for detecting, preventing, and responding to system attacks and failures; conducting regular testing of system vulnerabilities

3. **"Reasonable physical safeguards:"** maintaining procedures for information storage and disposal and for physical equipment theft or facility intrusion

For "small businesses," the Act allows for compliance exceptions via a less onerous data security program by putting into place "reasonable" administrative, technical, and physical safeguards that are appropriate to the business's size, complexity, and sensitivity of data.

Result for Failure to Comply

Failure to comply with the Act will be deemed a "deceptive business practice" under General Business Law section 349. Non-compliance will result in an investigation and potential imposition of civil penalties up to the greater of $5,000 or $20 per instance of failed notification (provided the latter may not exceed $250,000) by the New York State Attorney General's Office.

EXPANSIONS OF BREACH REQUIREMENTS

Private Information

As the law currently stands, "private information" includes the combination of any information that can be used to identify a consumer in addition to one or more other sensitive data elements (such as a social security number or driver's license number). The SHIELD Act expands this definition to add other data elements including the following:

1. Biometric information
2. Account numbers where such numbers may be used to access a consumer's financial account (without additional identifying information or access codes)
3. User names or email addresses, if accompanied by corresponding passwords or security questions or answers

Scope of a Breach

The Act lowers the threshold for triggering breach notification obligations by expanding the definition of a breach to include unauthorized access to computerized data that comprises the security, confidentiality, or integrity of consumers' private information. Conversely, as the law currently stands, breach notification obligations are triggered, under the current law, only if there has been an actual acquisition of private information.

Carve Backs to Consumer Breach Notification Requirements

Though breach notification requirements have broadened, the Act contains two limited exceptions. First, notification is not required where a person with authority to access private information has inadvertently exposed fewer than 500 records and that exposure has been determined unlikely to result in a misuse of information or financial or emotional harm. Such a circumstance must be documented in writing and records must be kept for a minimum of five years. The second exception to notification is where a breach of New York residents' data has also triggered notification pursuant to Title V of the Gramm-Leach Bliley Act, HIPAA, Hi-TECH, or Part 500.

For more information about the Act, click here.

BEECHER CARLSON