THE NEW YORK SHIELD ACT: ARE YOU READY?

Hodgson Russ Cybersecurity & Privacy Alert
February 24, 2020

On March 21, 2020, the New York SHIELD Act (Stop Hacks and Improve Electronic Data Security Act) goes into effect. Yet—one month before it becomes effective—many businesses are just learning about the SHIELD Act and its implications for conducting business.

The SHIELD Act significantly expands the existing data breach notification law in New York State. Under the existing law, businesses are required to notify individuals (as well as certain state agencies) if their private information is "acquired" without valid authorization. As described below, the definition of "private information" is broadened by the SHIELD Act and a business will have to notify individuals if their private information is merely accessed (i.e., information that is viewed, communicated with, or altered without valid authorization or by an unauthorized person), even if it is not acquired (i.e., information that was used, possessed, downloaded or copied).

In addition to the breach notification requirements, the SHIELD Act requires businesses to implement specific data security safeguards. In the past, healthcare providers, insurance companies, and financial institutions were required to satisfy rigorous security standards to safeguard certain nonpublic information obtained from patients and consumers. Now, under the SHIELD Act, businesses and organizations must safeguard "private information." Specifically, the law applies to any person or business that handles New York residents' private information regardless of whether that person or business conducts business in New York.

To qualify as "private information" under New York law, the data at issue must contain "personal information" in combination with another unique data element that is identified in the statute. "Personal information" is defined as "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person." Such personal information must be combined with any one or more of the following data elements that were not encrypted, or was encrypted with an encryption key that was accessed or acquired without authorization: (1) social security number; (2) driver's license number or non-driver ID card; (3) account number, credit or debit card number in combination with any required security code, access code, password or other information that would permit access to an individual's financial account; or (4) biometric information such as a fingerprint, voiceprint, retina or iris image, or other unique physical representation or digital representation of biometric data used to

Attorneys

William Ciszewski III
Alfonzo Cutaia
Patrick Fitzsimmons
Michael Flanagan
Michelle Merola
Gary Schober
Amy Walters

Practices & Industries

Cybersecurity & Privacy

authenticate or ascertain the individual's identity. Private information can also be a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

Thus, if a person or business owns or licenses computerized data which includes private information of a resident of New York, that person or business 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 data. Entities that are regulated by other data security rules and regulations—like HIPAA, Gramm-Leach-Bliley and Part 500 of Title 23 of NYCRR—are deemed compliant. However, all other business must implement reasonable administrative, technical and physical safeguards.

Rather than setting forth detailed safeguards for private information, the SHIELD Act states that a business will be deemed to be "in compliance" if it implements a data security program having reasonable *administrative* safeguards. Thus, the program should:

- designate one or more employees to coordinate the security program;
- identify reasonably foreseeable internal or external risks;
- assess the sufficiency of safeguards in place to control the identified risks;
- train and manage employees in the security program practices and procedures;
- select service providers capable of maintaining appropriate safeguards, and require those safeguards by contract; and
- adjust the security program in light of business or new circumstances.

Under the SHIELD Act, a business must also implement a data program that has reasonable *technical* safeguards. The program should:

- assess risks in network and software design;
- assess risks in information processing, transmission, and storage;
- detect, prevent and respond to attacks or system failures; and
- regularly test and monitor the effectiveness of key controls, systems and procedures.

Finally, the data program must include reasonable *physical* safeguards, which:

- assess risks of information storage and disposal;
- detect, prevent and respond to intrusions;
- protect against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and
- dispose 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.

However, a small business (fewer than 50 employees, less than $3 million in gross annual revenue in each of the last 3 fiscal years, or less than $5 million in year-end total assets) will be deemed in compliance if the small business's security program contains reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers. Although there is no private right of action, compliance is not merely aspirational. The New York Attorney General may bring an action seeking an injunction and civil penalties against any business for failure to comply with these security requirements.

The SHIELD Act may be a game-changer for your organization. Although many businesses in New York already have technology systems in place that satisfy these requirements—especially those businesses that operate in highly regulated environments—others do not. For organizations in the latter category, it is critical to assemble a team, which includes legal and technical expertise, to assess your existing data program and whether it satisfies the reasonable administrative, technical and physical safeguards required under the SHIELD Act.

If you received this alert from a third party or from visiting our website, and would like to be added to our Cybersecurity & Privacy mailing list or any other of our mailing lists, please visit us at: https://forms.hodgsonruss.net/subscription-center-hr.html