Overview
Last month, New York Gov. Andrew Cuomo signed into law the Stop Hacks and Improve Electronic Data Security Act (Shield Act). The Shield Act expands the type of personal information covered by New York's data breach notification law, amends the definition of a "breach of security of the system" and the notification requirement itself, enhances the state attorney general's enforcement authority of the data breach notification law, and introduces data security requirements for the first time. The Shield Act was passed by the New York Legislature in June. The Act goes into effect on October 23, 2019, with the exception of the Act's data security requirements, which go into effect on March 21, 2020.

Expanded Definitions of Personal Information and Breach the Security of the System
New York's data breach notification requirement applies to "private information," which 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 a natural person" in combination with certain other specified data elements. The Shield Act expands the list of data elements to include biometric information and an "account number, credit or debit card number… wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password." Previously, account and payment card numbers were included only if the security code or password were also breached. The Shield Act also expands the definition of "private information" to include, by itself and not in combination with any additional information, "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."

In addition, the Shield Act amends the definition of "breach of the security of the system," the event triggering a business's data breach notification requirement. "Breach" now includes not just unauthorized acquisition of private information, but also unauthorized "access" to such information. In addition, the new definition allows businesses to consider certain factors in assessing whether unauthorized access has occurred, including "indications that the information was viewed, communicated with, used, or alerted by a person without valid authorization or by an unauthorized person."

Changes to Data Breach Notification Requirement
The Shield Act also introduces changes to New York's data breach notification requirement itself. First, the requirement no longer is limited to businesses that "conduct business in New York state," but now extends to any business that owns or licenses computerized data including private information of New York residents. Second, the Act exempts a business from notifying affected individuals if the exposure was an inadvertent disclosure by someone authorized to access private information and the business "reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials." The business's determination must be documented in writing and maintained for five years and, if the incident affects more than 500 New York residents, the business must provide the written documentation to the state attorney general within 10 days of the determination being made.

In addition, the Shield Act provides that businesses are exempt from notifying affected individuals pursuant to New York's law if notification is made pursuant to certain other federal or New York state laws, rules, or regulations, including the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Health Information Technology for Economic and Clinical Health (HITECH) Act. However, even under such circumstances, notification must still be provided to the state attorney general and the state police. The Shield Act also mandates that a business required to provide notification under HIPAA or the HITECH Act regarding information that is not "private information" also provide notification to the state attorney general within five days of providing government notification under those statutes.

The Shield Act also addresses the method and content of the notification to affected individuals. The Shield Act restricts the ability of a business to provide substitute notice to affected individuals through e-mail where the breached information includes an e-mail address in combination with a password or security question and answer that would permit access to an online account. Under such circumstances, the business is directed to provide notice to the individual on his or her online account when the individual logs into his or her account from an IP address or online location that the person is known to customarily use. With respect to the content of the notification, the Shield Act requires businesses to include the telephone numbers and websites of the state and federal agencies that provide information regarding security breach response and identity theft prevention.

The Attorney General's Enforcement Authority

The Shield Act expands the attorney general's authority to enforce violation of the state's data breach law. The Act increases the monetary penalties for knowing and reckless violations from $10 to $20 "per instance of failed notification" and expands the cap on monetary penalties under such circumstances from $150,000 to $250,000. The Shield Act also amends the timeframe during which the attorney general is able to bring an enforcement action, from two to three years after becoming aware of the violation or from the date notice of a breach is sent to the attorney general, whichever occurs first. However, the attorney general may not bring an enforcement action more than six years after the breach is discovered by the business, unless the business is found to have taken steps to hide the breach.

Data Security Measures

Perhaps the most significant development in the Shield Act is the introduction of a requirement that businesses that own or license computerized data that includes private information of a New York resident "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." A business is deemed complaint if it adopts a security program which includes the following:

- "Reasonable administrative safeguards," such as:
  - Designating one or more employees to coordinate the security program;
  - Identifying reasonably foreseeable internal and external risks;
  - Assessing the sufficiency of safeguards in place to control the 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.

Small businesses are exempt from these requirements, and must instead only implement a data security program that “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[1] the small business collects from or about consumers.” A “small business” is defined as a business with (1) fewer than 50 employees; (2) less than 3 million dollars in gross annual revenue in each of the previous three fiscal years; or (3) less than 5 million dollars in year-end total assets. In addition, businesses that comply with other federal and state data security requirements, such as the Gramm-Leach-Bliley Act, HIPAA, and the HITECH Act, are deemed to be in compliance with the Shield Act’s data security requirements.

Violations of the data security requirements are deemed to be a violation of New York’s law prohibiting deceptive acts or practices. The attorney general may bring an enforcement action for violations, with each violation carrying a penalty of up to $5,000. The Act explicitly excludes a private right of action under this section.

[1] “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 a natural person.” “Personal information” by itself does not constitute “private information” under New York law, although, as noted above, in conjunction with other data elements it may constitute “private information.”

Practices
Privacy & Cybersecurity