DAVIS GILBERT

New York Amends Security Breach Notification Law and Imposes New Security Obligations

The Bottom Line

- *Companies that own or license New Yorkers' private information must develop a data security program that is compliant with the SHIELD Act.*
- *The program should be documented in a written information security policy and other policies that are drafted specifically to reflect the company's business, data and operations.*
- *In addition, companies should be aware that the obligation to notify an individual of a security breach has now been expanded.*

New York Governor Andrew M. Cuomo has signed into law a bill that strengthens the state's existing security breach notification rules and imposes significant new obligations on companies that own or license the "private information" of New York residents.

New Security Requirement

The new law, known as the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), requires that any business — not just a company operating in New York — that owns or licenses computerized data that includes the private information of even one New York resident must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of that information.

A business must meet this requirement by implementing a data security program that includes the following:

1. Reasonable administrative safeguards, such as by:

- 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's 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.

2. Reasonable technical safeguards, such as by:

- 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.

3. Reasonable physical safeguards, such as by:

- 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.

Regulated entities that are subject to, and in compliance with, certain specified laws (such as the federal Gramm-Leach-Bliley Act [GLBA], the Health Insurance Portability and Accountability Act of 1996 [HIPAA] and NYDFS Cybersecurity Regulation) are considered in compliance with this requirement.

In addition, a small business is deemed in compliance if its 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.

A small business is defined as a business with fewer than 50 employees and a business with:

1. Less than $3 million in gross annual revenue in each of the last three fiscal years; or
2. Less than $5 million in year-end total assets.

As a best practice, companies should meet this complex new security requirement — and avoid the substantial civil penalties that can be imposed for failing to do so — by developing written policies clearly setting forth how they are complying with this requirement.

Expanded Definition of "Private Information"

In addition to imposing a new security requirement on businesses that hold New Yorkers' private information, the SHIELD Act makes other important changes to prior law governing notification to affected New Yorkers of a security breach.

For example, before the enactment of the SHIELD Act, New York required notification when a breach involved an individual's private information, which was defined as "personal information" (i.e., any information concerning a natural person which, because of name, number, personal mark or other identifier, can be used to identify such natural person) in combination with certain data elements, including a Social Security number, driver's license number or an account, credit and debit card number in combination with any required security code, access code or password permitting access to the individual's financial account.

The new law broadens the definition of private information to include additional data elements such as:

1. An account, credit or debit card number standing alone, if the number can be used to access an individual's financial account without any additional identifying information, security code, access code or password.

2. Biometric information:

- Data generated by electronic measurements of an individual's unique physical characteristics such as a fingerprint, voice print, retina or iris image; or
- Other unique physical representation or digital representation which is used to authenticate or ascertain the individual's identity.

3. A username or e-mail address in combination with a password or security question and answer that would permit access to an online account.

The SHIELD Act did not amend the definition of "Personal information."

Notice Exceptions

The new law provides some exceptions to the notification requirement, such as a 'risk of harm' carve-out. For example, a business does not need to notify affected persons — but must notify the state attorney general if the incident affects over 500 New York residents — if:

1. The exposure of private information was an inadvertent disclosure by persons authorized to access private information; and
2. The business reasonably determines that the exposure will not likely result in the misuse of such information or financial or emotional harm to the affected persons.

Moreover, the new law clarifies that an additional notice of a breach does not need to be made to a New York resident if the business suffering the breach is subject to certain other specified laws (as noted above) and it follows the notification requirements under those laws. These businesses would, however, still be required to notify the state Attorney General, Department of State Division of Consumer Protection and Division of State Police, as was required under the prior law.

Attorney General Lawsuit

Although the SHIELD ACT states that no private right of action is authorized, the Attorney General can still bring an action to enjoin violations and obtain civil penalties. Under prior law, the Attorney General had two years to bring an action against a company that failed to properly notify affected individuals of a security breach involving their personal information. The new law lengthens that period to three years, and in certain instances up to six years, or even more if a company takes steps to hide a breach.

Related People

Gary Kibel
Partner
212 468 4918
gkibel@dglaw.com