New York State Doubles Down on Data Privacy, Sets High Bar for “Reasonable Safety Standards”

Wednesday, September 18, 2019

On July 25, 2019, New York governor Andrew Cuomo signed into law two bills aimed at increasing the obligations of entities handling computerized private data. The Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) expands the requirements for notifying affected parties in the event of a data breach and sets forth a demanding list of security measures that must be implemented to “maintain reasonable safeguards” to protect private information. Businesses handling the private data of New York residents should consider reviewing the SHIELD Act and existing policies and procedures to ensure compliance before the new privacy requirements go into effect.

The SHIELD Act amends New York’s existing data breach notification law in the following ways:

- The act expands the definition of “private information” to include:
  - financial account numbers in circumstances where the information can be
used independently to access an individual’s account;
- biometric information, which includes fingerprints, voice prints, retina or iris images, or other unique physical representations or digital representations of biometric data that are used to authenticate or ascertain the individual’s identity; or
- a username or email address in combination with a password or security question and answer that would permit access to an online account.

- It expands the definition of a covered data breach to include:
  - “access to,” in addition to acquisition of, computerized data that is detrimental to the security of private information.
- The act expands the list of factors considered by covered businesses when evaluating a data breach to include “indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an authorized person.”

The act’s amendments to New York’s data breach notification law take effect on October 23, 2019. The expanded language evidences a continued effort by state legislatures nationwide to increase the scope of data breach notification obligations. In addition to expressly including an expansive definition for “biometric information,” New York’s changes make clear that data breach notification obligations may activate in situations in which an individual has only accessed or viewed private information, rather than actually possessed or changed the data.

Most significant among the changes is the addition of a list of requirements for maintaining “reasonable safeguards” under New York’s general business law. This “reasonable safeguards” portion of the SHIELD Act takes effect on March 1, 2020. While many employers may already be compliant with these directives, companies that have not implemented comprehensive data privacy measures may want to act quickly to ensure compliance before the effective date. For example, the act directs the implementation of a “data security plan” and lays out detailed requirements for reasonable administrative safeguards, reasonable technical safeguards, and reasonable physical safeguards. Excluded from these demanding requirements are businesses that comply with existing privacy regulations—such the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act—and entities that qualify as a “small business” under the Act. Businesses that do not fall within these exceptions and employ New York residents should review the act’s “reasonable safeguards” closely with their legal, human resources, and information technology departments to fully understand and comply with the new data security directives.

The second bill signed into law by Governor Cuomo requires credit reporting agencies that suffer data breaches to provide five-year identity theft protection services and, if applicable, identity theft mitigation services to affected customers. The Identity Theft Prevention and Mitigation Services Act also requires credit reporting agencies to inform consumers of a breach of data involving a Social Security number, and it provides consumers with the right to freeze their credit at no cost. The law takes effect on September 23, 2019.

With the enactment of the SHIELD Act and the Identity Theft Prevention and Mitigation Services Act, New York joins a long list of states, such
as California, Maine, Maryland, and Alabama, working aggressively to expand the data privacy and data security obligations of businesses collecting and maintaining private information from their constituents. Employers should remain vigilant in their compliance efforts and closely monitor the rapidly changing legislative landscape related to data privacy and data security.
