LEGAL UPDATES

Data Security and the New York SHIELD Act: Going Beyond New York Companies

With the Covid-19 crisis, many companies that may have traditionally only done business offline are transitioning and expanding into e-commerce. Others are starting new businesses and innovating new technologies and platforms. There are a multitude of considerations that go into these new ventures, an important one of which is security.

07/14/2020 | 5 minute read

By Chiara Portner

With the Covid-19 crisis, many companies that may have traditionally only done business offline are transitioning and expanding into e-commerce. Others are starting new businesses and innovating new technologies and platforms. There are a multitude of considerations that go into these new ventures, an important one of which is security.

For any new or established business, the company must look to evaluate its existing security procedures and policies as compared to both legal requirements and best practices. While many state laws include a rather vague obligation to maintain "reasonable security measures" without a clear definition, some state laws go into more detail as to what security measures are required. In 2010, Massachusetts was first to set forth more specific security requirements for businesses that maintain electronic data on any residents of Massachusetts with the Massachusetts Standards for the Protection of Residents of the Commonwealth. In short, the Massachusetts law required: user authentication; access control measures; encryption; system monitoring; firewalls and security patching; anti-malware and virus mechanisms; and employee training.

Prior to the Massachusetts law going into effect, it was seen as groundbreaking, but language requiring the security measures to be implemented only if "technically feasible" provided a lot of wiggle room and Massachusetts simply was not a focus of many companies. Now, fully effective this past March, the New York SHIELD Act has even more detailed requirements around data security that apply to a broader set of companies (even if not located in New York).

The New York SHIELD Act prioritizes the safeguard and security of personal information of New York residents. Unlike the California Consumer Privacy Act ("CCPA"), which carries security requirements but does not spell those out specifically, the SHIELD Act's focus is security and it provides ample detail on steps that must be taken in order to comply.

The SHIELD Act's obligations apply to "[a]ny person or business which owns or licenses computerized data which includes private information" of a resident of New York. This definition is similar to the security breach statutes of most states

Related People

Chiara Portner, CIPP/US

Partner

Redwood Shores

650.804.7672

chiara.portner@lathropgpm.com

Related Services

Data Privacy & Cybersecurity Compliance

Corporate & Business

Related Sectors

Retail & E-Commerce

that apply to any businesses regardless of location if they retain any electronic personal data. Thus, the SHIELD Act includes businesses that are not located in New York.

The SHIELD Act uses the term "private information" to refer to the key data elements to be protected under the statute. In other words, "private information" is a subset of "personal information."

- Personal information is *any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person*.

- Private information is defined as follows (again, this is very similar to the definitions of data subject to security breach laws in other states):

1. personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired:

    - social security number;

    - driver's license number or non-driver identification card number;

    - 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;

    - account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or

    - biometric information, meaning 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 of biometric data which are used to authenticate or ascertain the individual's identity;

OR

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

Under the SHIELD Act, any person or business that owns or licenses computerized data that includes private information of a resident of New York is required to 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 person or business is deemed to be in compliance if it implements a data security program that includes the following:

(A) Reasonable Administrative Safeguards by which the person or business:

(1) designates one or more employees to coordinate the security program;

(2) identifies reasonably foreseeable internal and external risks;

(3) assesses the sufficiency of safeguards in place to control the identified risks;

(4) trains and manages employees in the security program practices and procedures;

(5) selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and

(6) adjusts the security program in light of business changes or new circumstances.

(B) Reasonable Technical Safeguards by which the person or business:

(1) assesses risks in network and software design;

(2) assesses risks in information processing, transmission and storage;

(3) detects, prevents and responds to attacks or system failures; and

(4) regularly tests and monitors the effectiveness of key controls, systems and procedures

and

(C) Reasonable Physical Safeguards by which the person or business:

(1) assesses risks of information storage and disposal;

(2) detects, prevents and responds to intrusions;

(3) protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and

(4) disposes 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.

*NOTE that a person or business is also deemed compliant if it is a "compliant regulated entity", meaning that it is subject to, and in compliance with, certain specified data security requirements, including under GLBA, HIPAA or other enumerated regulations.

Under the SHIELD Act, certain "small businesses" may adjust their data security obligations based on certain factors.

A "small business" still must adopt reasonable administrative, technical, and physical safeguards, however, those safeguards can be adjusted according to:

- 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.

However, there are no exceptions for small businesses in the breach notification rule. A small business that experiences a data breach affecting the private information of New York residents must notify the affected persons as would any business.

Businesses that fail to comply with the SHIELD Act's security requirements face civil penalties of up to $5,000 per violation and there are no penalty caps. By contrast, there is a penalty cap of $250,000 per violation for failing to notify authorities when a breach occurs. The SHIELD Act does not include a limited private right of action like the CCPA. However, unlike the CCPA, which applies only to certain businesses that meet certain thresholds, all businesses that own or license computerized data that includes "private information" of a resident of New York must implement appropriate cyber security measures, in addition to complying with the administrative, technical, and physical safeguards spelled out in the SHIELD Act. Security should always be a top priority, no matter whose personal information is collected and with the various state security breach and protection laws, care should be taken to comply with all applicable laws, with an emphasis on the most proscriptive and comprehensive laws.