Client Alert

New York Continues State's Charge to Protect Consumer's Personal Information

August 2019

Authors: **Steven R. Chabinsky**, **F. Paul Pittman**

New York recently amended its existing data breach notification law to expand the data breach notification obligations of persons and businesses (and state agencies) and impose specific data security requirements on persons and businesses to protect its residents' personal information. Under SB 5575 or the "Stop Hacks and Improve Electronic Data Security Act" ("SHIELD Act"), New York continues a growing trend of regulators and lawmakers to increase consumer privacy and data security protections. States such as California and Massachusetts have long required that organizations implement "reasonable" security over the sensitive personal data of their residents, and the SHIELD Act represents New York's determination of what "reasonable cybersecurity" requires of persons and businesses (regardless of where they are located) when it comes to protecting "computerized data" of New York residents.

The SHIELD Act requirements supplement existing New York data security regulations previously set forth under the state's general business law, and are separate and apart from the New York Department of Financial Services ("NYDFS") Cybersecurity Requirements for financial institutions ("Cybersecurity Regulation") that became effective March 1, 2017. Many of the requirements under the SHIELD Act will be effective on October 23, 2019 (90 days after the act became a law), with an effective date of March 21, 2020 for implementation of its specific and demanding data security protections requirements.

As a notable show of force, on the same day New York passed the SHIELD Act it also passed another bill (S3582, "Identity Theft Prevention and Mitigation Services") which requires credit reporting agencies that have suffered a data breach involving social security numbers to provide free credit monitoring and/or identity theft mitigation services to affected consumers.

Expanded Notification Obligations

Specifically, the SHIELD Act expands New York's existing data breach notification law (NY Gen Bus § 899-aa) to include additional "private information"[1] data types such as biometric data, as well as user name or email address in combination with a password or security question and answer that permits access to an online account. Additional key amendments include:

- Expanding activities that are considered a "breach of the security of the system" to include "access to" computerized data, in addition to the existing "acquisition of" computerized data. Factors indicating access include whether information was viewed, communicated with, used, or altered without valid authorization;
- Exceptions to data breach notice requirements where notice is provided under other breach notification laws (*i.e.* HIPAA), or where inadvertent disclosure occurs at the hands of persons authorized to access private information and disclosure will not likely result in misuse or harm. This "risk of harm" determination must be documented and where more than 500 New York residents are affected a copy of the documented risk of harm analysis must be provided to the New York Attorney General ("NY AG") within ten days of the determination;
- Clarification that data breach notification may not be provided by email where the information that is the subject of the data breach includes an email address in combination with a password or security question and answer. Instead, data breach notification must be provided through the consumers' online account;
- Increasing the limitations period for the NY AG to bring an enforcement action for failure to notify up to three years (increased from two years) following the date on which the NY AG becomes aware of the violation or date the NY AG is notified (whichever occurs first), but not later than six years following the discovery of the breach by the company (unless the company took steps to hide the breach);
- Requiring disclosure of contact information for relevant state and federal agencies that provide guidance on security breach response and identity theft prevention and protection in consumer data breach notifications; and
- Extending data breach notification requirements to any "person or business" that owns or licenses the private information of a New York resident (rather than to persons or businesses conducting business in New York, as currently limited).

New "Reasonable Security" Requirements

The SHIELD Act extends data security obligations to all persons and businesses that own or license computerized data that includes the private information of residents of New York, continuing New York's leadership in cybersecurity following the promulgation of the NYDFS Cybersecurity Regulation in 2016. As we have previously described, under the NYDFS, Cybersecurity Regulation financial institutions are required to establish and maintain a cybersecurity program designed to protect financial institution company systems and non-public information. Similarly, the SHIELD Act requires that a person or business implement reasonable

[1] New York's data breach notification law (NY Gen Bus § 899-aa) applies to "private information" which is defined as either: "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: (1) social security number; (2) driver's license number or non-driver identification card number; (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; (4) 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 (5) 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 (ii) a user name or email address in combination with a password or security question and answer that would permit access to an online account." Personal information is defined broadly 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."

safeguards to protect the confidentiality, integrity and availability of the private information of New York residents. The SHIELD Act provides that a business is compliant with its "reasonable security" requirements where it implements administrative, technical and physical safeguards that consist of the following:

- *Administrative safeguards,* including (1) designating one or more employees to coordinate its security program; (2) identifying reasonably foreseeable internal and external risks; (3) assessing the sufficiency of safeguards in place to control the identified risks; (4) training and managing employees in its security program practices and procedures; (5) selecting service providers capable of maintaining appropriate safeguards, and requiring those safeguards by contract; and (6) adjusting its security program in light of business changes or new circumstances;

- *Technical safeguards,* including (1) assessing risks in network and software design; (2) assessing risks in information processing, transmission and storage; (3) detecting, preventing and responding to attacks or system failures; and (4) regularly testing and monitoring the effectiveness of key controls, systems and procedures; and

- *Physical safeguards,* including (1) assessing risks of information storage and disposal; (2) detecting, preventing and responding to intrusions; (3) protecting against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and (4) 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.

The act provides for an exception to the express "reasonable security" requirements for small businesses whose security programs contain "reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of small business's activities, and the sensitivity of the personal information the small business collects from or about consumers." In addition, persons or businesses that are compliant with existing state or federal data security laws (such as HIPAA or GLBA) will be considered compliant with the SHIELD Act's "reasonable security" requirements. Unlike the other amendments to the NY Gen Bus § 899-aa, the data security protections requirements do not go into effect until 240 days after the act became a law, or March 21, 2020.

Stiffer Civil Penalties

The existing right of the NY AG to bring an action for injunctive relief for failure to notify of a data breach remains unchanged under the SHIELD Act. However, the maximum civil penalty that a court can issue for knowing or reckless failure to notify an affected resident is increased. Civil penalties can now top out at US$20 (up from US$10) per affected individual for a maximum of US$250,000 (up from US$150,000). Significantly, persons or businesses that fail to comply with the "reasonable security" requirement may be subject to enforcement actions by the state AG for injunctive relief and civil penalties of up to US$5,000 for each violation, irrespective of whether a data breach has occurred.

Conclusion

We are witnessing the states with the largest economic markets on both coasts taking the initiative in establishing expanded privacy rights (California) and rigorous cybersecurity protections (New York) in a manner that is certain to reverberate within and beyond the United States. Given the share of the overall consumer market held by residents of California and New York, companies worldwide should prepare to comply with these expanded requirements. The continued trend in the United States towards increased data subject rights (see also Nevada's recent privacy law) and cybersecurity standards at the state level, rather than nationally, further exacerbates the complexities of US compliance programs, especially in comparison to Europe's uniform General Data Protection Regulation. We encourage organizations to conduct (or engage a third party to conduct) data privacy and information security assessments against both state and federal regulatory requirements, identify gaps in compliance, and obtain participation and buy-in from officers and directors to make enterprise risk determinations and implement required changes. Because introducing new security measures to an organization's existing information technology systems can increase business friction and cause unintended disruptions, organizations

that are subject to New York's SHIELD Act requirements are encouraged to begin this process as soon as possible to ensure compliance by the March 21, 2020 deadline while maintaining steady operations.

White & Case LLP
701 Thirteenth Street, NW
Washington, District of Columbia 20005-3807
United States

T + 1 202 626 3600