LOCKE LORD® QUICK Study
Privacy & Cybersecurity Practice
July 24, 2019

New York SHIELDs Private Information

By: Laura L. Ferguson and Paul B. Sudentas

We recently reported on New York's latest attempt to strengthen its breach notification requirements to protect New York residents' private information[1] —the Stop Hacks and Improve Electronic Data Security Act, commonly referred to as the SHIELD Act (S5575-B)—following in the footsteps of other states who have already revamped their data security laws. The SHIELD Act amends N.Y. Gen. Bus. Law § 899-aa and N.Y. State Tech. Law § 208, and adds new Gen. Bus. Law § 899-bb. As of the date of this publication, the SHIELD Act is waiting for the Governor's signature and will go into effect on the ninetieth day after it is signed into law.

Key Changes to the Breach Notification Obligations

Below is a quick summary of the key changes to the breach notification obligations made as a result of the SHIELD Act:

- Broadens the notification obligations as a result of a breach to include notification to residents whose private information was, or is reasonably believed to have been, *accessed* by an unauthorized individual (instead of just notification to those residents whose information was *acquired*).
- Exempts breach notifications when the exposure to private information was inadvertent and the covered entity[2] "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 covered entity must maintain documentation of the determination for at least five years, and in the event there were over 500 New York residents impacted by the inadvertent disclosure, the State Attorney General must be notified within 10 days of the determination.
- Expands the definition of "private information" to include (i) the combination of a user name or email address with a password or security question and answer thereto that would allow access to an online account, and (ii) personal information in combination with the following newly added data elements:
    1. account, credit or debit card numbers *without* additional identifying information if the number may be used to access the individual's financial account (before this amendment, the definition already captured account, credit or debit card numbers *with* additional identifying information); and
    2. biometric information such as fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data.

- Exempts individual notifications if notice was already provided in accordance with:
    1. the Gramm-Leach-Bliley Act (GLBA),
    2. the Health Information Portability and Accountability Act (HIPAA),

1 *See* https://www.insurereinsure.com/2019/07/10/new-york-jumps-on-the-data-security-bandwagon/.

2 A "covered entity" is any person, business or state entity that owns or licenses computerized data which includes private information.

3. part 500 of title 23 of the official compilation of codes, rules and regulations of the state of New York, or
4. any other data security rules and regulations of any official department, division, commission or agency of the federal or New York state government.
   Note that the notifications to the state attorney general, the state department of state and the division of state police are still required.

- Amends the content requirements for the individual notification to include the provision of telephone numbers and websites of the relevant state and federal agencies that provide information on security breach response and identity theft prevention and protection.
- Amends the notification obligation with respect to the state attorney general, the department of state and the division of state police by requiring a copy of the form of the individual notification.
- Requires that a HIPAA covered entity that is required to provide notification of a breach of unsecured PHI to the Secretary of the Department of Health and Human Services ("HHS") provide a copy of the notification to the state attorney general within 5 business days after notifying HHS, even if the breach does not include "private information".

New Data Security Obligations

The SHIELD Act adds a requirement that covered entities implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of private information, including the disposal of data. In order to be in compliance, a business must implement a data security program that includes reasonable administrative, technical and physical safeguards, including:

- **Administrative safeguards:** (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 safe guards, and requires those safeguards by contract; and (6) adjusts the security program in light of business changes or new circumstances.
- **Technical safeguards:** (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.
- **Physical safeguards:** (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.

Small businesses are permitted to scale the above reasonable security requirements as appropriate for the size and complexity of the business, the nature and scope of the business' activities, and the sensitivity of the personal information the business collects. In addition, a business is deemed to be in compliance with the above reasonable security requirements if the business is subject to and in compliance with GLBA, HIPAA, part 500 of title 23 of the official compilation of codes, rules and regulations of the state of New York, or any other data security rules and regulations of any official department, division, commission or agency of the federal or New York state government.

Next Steps

In order to be in a position to comply with the requirements of the SHIELD Act when it becomes effective (likely before the end of 2019), covered entities should begin to:

1. Understand what "private information," including the newly added data elements, of New York residents is in the business' possession, and how the information is processed and maintained.
2. Review the business' physical, technical, and administrative safeguards to determine whether they satisfy the enumerated requirements of the SHIELD Act.
3. Update incident response procedures related to the SHIELD Act's various changes to the notification obligations for data breaches impacting New York residents. Amend or add a procedure for documenting a determination of inadvertent exposure of "private information" of New York residents that is not a reportable incident, including retention requirements for the documentation and the attorney general notification obligation if over 500 New York residents were impacted.

For more information on the matters discussed in this *Locke Lord QuickStudy*, please contact the authors.

Laura L. Ferguson | 713-226-1590 | lferguson@lockelord.com
Paul B. Sudentas | 646-217-7716 | psudentas@lockelord.com