Cybersecurity, Privacy and Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

New York Enacts SHIELD Act with Expansive Data Breach Notification and Data Security Requirements

August 2, 2019

Key Points:

- New York recently enacted the Stop Hacks and Improve Electronic Data Security (SHIELD) Act, which expands data breach notification requirements and imposes new data security obligations on businesses that own, license or, in some cases, maintain computerized data that includes any New York resident's private information.
- The new "reasonable security requirement" requires businesses that are not regulated by and compliant with another New York state or federal data security regime to adopt a program that includes certain data security safeguards.
- In a significant departure from prior New York law, the SHIELD Act expands the definition of "breach of the security of the system" to include "unauthorized access to," in addition to unauthorized acquisition of, computerized data that compromises the security, confidentiality or integrity of private information maintained by a business.

I. Background and Overview

On July 25, 2019, Governor Andrew Cuomo signed the Stop Hacks and Improve Electronic Data Security (SHIELD) Act (S5575B/A5635), which ushers in new data breach notification and data security requirements that will affect many businesses. The Act is likely to have a far-reaching impact, given that it protects New York residents' private information regardless whether the business that owns, licenses or maintains that information is located or doing business in New York. It also applies to businesses of all sizes.

The Act expands the New York Attorney General's authority to bring enforcement actions, including by seeking higher civil penalties. It does not permit individuals to bring private rights of action. Affected businesses should anticipate the potential for active enforcement when the Act go into effect.

Contact Information

If you have any questions concerning this alert, please contact:

Natasha Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Jo-Ellyn Klein
Senior Counsel
jsklein@akingump.com
Washintong, D.C.
+1 202.887.4220

Diana Schaffner
Counsel
dschaffner@akingump.com
San Francisco
+1 415.765.9507

Zak Newman
Associate
znewman@akingump.com
New York
+1 212.872.7445

The SHIELD Act does two main things:

1. ***Data Breach Notification*** – The Act requires that persons and businesses (collectively, "businesses"), as well as New York state government agencies, meet expanded notice requirements when they own, license, or maintain computerized data that includes any New York resident's private information and that information is affected by a data breach. The data breach notification provisions go into effect in October 2019.

2. ***Data Security Requirements*** – The Act requires that businesses develop, implement, and maintain reasonable security safeguards if they own or license computerized data that includes any New York resident's private information. The data security provisions go into effect in March 2020.

Businesses that own or license computerized data that includes any New York resident's private information must comply with both the Act's data breach notification and data security provisions, though some accommodations are made for entities that are already subject to (and in compliance with) certain existing data security regulatory regimes. Businesses that are not data controllers, but instead only maintain such information as a vendor, for example, are only required by the Act to notify the data controller of breaches, not the end consumer. Similarly, the data security protections will extend to service providers via contracts required of businesses that are data controllers, but will not apply to service providers directly.

The Act protects the information of New York residents by linking its various provisions to the ownership, license, or maintenance of computerized data that includes any "private information" of a New York resident. As under prior New York law, "private information" is a more sensitive subset of "personal information."[1] The SHIELD Act leaves in place the prior definition of personal information, but expands the definition of private information to include biometric information and information that would enable access to an online account. Information can be "private information" if it is either: (1) personal information plus a sensitive data element (e.g., Social Security number); or (2) information that would permit access to an online account (e.g., username or email address plus a password or security question).

Businesses that are subject to and compliant with another New York state or federal data security regime, including the three data security regimes specified in the Act, may be deemed either compliant with the Act or face limited or tailored requirements. This includes the data security regimes implemented under the Gramm Leach Bliley Act (GLBA); the Health Insurance Portability and Accountability Act and Health Information Technology for Economic and Clinical Health Act (together with their implementing regulations, HIPAA); or the New York State Department of Financial Services (NYDFS) Cybersecurity Regulation.

II. The SHIELD ACT - Key Provisions and Practical Guidance

a. Key Data Breach Notification Provisions

The SHIELD Act changes and expands the existing New York data breach notification law in several significant ways. We discuss the most important below.

Access Alone Can Be A "Breach" – The SHIELD Act expands the definition of "breach of the security of the system" to include unauthorized ***access*** or acquisition of

computerized data that compromises the security, confidentiality or integrity of private information maintained by a business. This change expands businesses' potential liability. Factors to consider in determining unauthorized *access* include indications that a person without valid authorization viewed, communicated with, altered or used the information.[2]

No Need for Duplicate Notice to Affected Residents – A business does not have to provide additional notice to affected New York residents under the Act if it is already required to, and does, provide notice to affected residents pursuant to any other New York state or federal data security regime (including those implemented pursuant to GLBA, HIPAA or the NYDFS Cybersecurity Regulation). The business does still have to provide notice of the disclosures under the other data security regimes to the New York Attorney General, Department of State and State Division of Police.[3]

Exceptions for Certain Harmless Mistakes – The Act includes two exceptions that provide businesses a bit of breathing room for harmless mistakes. First, the definition of "breach of the security of the system" expressly carves out good faith access to, or acquisition of, private information by an employee or agent of the business (for business purposes), as long as the information is not used or subject to unauthorized disclosure. This helps businesses where an employee accidentally accesses a part of the system they are not supposed to see. Second, notice to affected individuals is explicitly not required where the private information was exposed as a result of "inadvertent disclosures by persons authorized to access" such data, if certain criteria are met. A business has to document in writing (and keep for five years) its determination that the exposure: (1) was an inadvertent disclosure; (2) by persons authorized to access private information; and (3) that the exposure is not likely to result in (a) misuse of the information, (b) financial harm to the affected persons, or (c) emotional harm in the case of unknown disclosure of online credentials. Importantly, if the incident affects over 500 residents, the business has to provide the determination to the Attorney General within 10 days.

Additional Notice Content Required – Once it has determined that a breach occurred, New York residents were affected and it is obligated to provide notice under the Act, a business must provide notice that includes: (1) its contact information; (2) the telephone numbers and websites of the relevant government agencies that provide information regarding breach response and identity theft protection issues (e.g., relevant local or state agencies to call); and (3) a description of the categories of information accessed or acquired without authorization together with specifics on which elements of personal and private information were accessed or acquired in the breach. The second requirement is new as a result of the Act.

New Restrictions on Use of Email Notice – The SHIELD Act grants businesses the option of providing notice to New York residents in one of three ways (written, electronic or telephone) and, if certain circumstances apply, includes three additional options for providing substitute notice. These are the same general methods of notice permitted under prior New York law. The Act adds new limitations on the use of email substitute notice. In order to use email notice, a business must have the affected individual's email address and the information exposed cannot have included email addresses and other information necessary to gain access to online accounts. If email addresses and account information were exposed, businesses are required to provide notice via the individual's online account when the individual logs in from a location the business knows is associated with the individual. This last requirement raises practical

issues for businesses that may make the other options for substitute notice a better choice in many breaches.

New Breach Notification Obligations – The Act updated breach notification obligations. For example, a business now has to provide a copy of its template notice to affected residents to various New York State agencies when it notifies those agencies of its outreach to New York residents. The chart at the end of this alert summarizes businesses' revised notice obligations.

Burdens for HIPAA Covered Entities – The Act contains language targeting HIPAA covered entities. First, when a business or state entity that is a HIPAA covered entity is required under the HIPAA breach notification rule to provide notification of a breach to the Secretary of the U.S. Department of Health and Human Services (HHS),[4] the notification must also be provided to the New York Attorney General within five business days of notifying the Secretary. This expressly applies even if the breach involves information that is protected by HIPAA but is not "private information" under the SHIELD Act. This requirement could be interpreted to extend to smaller breaches as well as to breaches affecting 500 or more individuals. The Act contains no exception for smaller breaches that are required under the HIPAA breach notification rule to be reported to the Secretary of HHS in annual breach logs. As a result, based on the plain language of the statute, annual logs providing the Secretary of HHS notification of smaller breaches of unsecured protected health information, as well as more contemporaneously provided notifications of breaches affecting 500 or more individuals, could be interpreted as within scope. Also, despite the name of the Act, based on the plain language of the statute, it seems unclear whether the New York Attorney General must be alerted to breach notifications involving non-computerized data that are provided to the Secretary of HHS pursuant to the HIPAA breach notification regulations. Further, when a HIPAA covered entity discovers a data incident but, upon investigation and assessment, determines that breach notification is not required under HIPAA, the covered entity will still need to comply with the SHIELD Act's requirements. This may create challenges for some HIPAA covered entities.

b. Key Reasonable Security Provisions

The SHIELD Act also imposes a reasonable security requirement on businesses. The Act requires any business that owns or licenses computerized data that includes any New York resident's "private information" to "implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information." In doing so, New York joins other states like California and Massachusetts in adopting minimum data security requirements.

Compliance with Another Data Security Regime is Compliance with the Act – A business can establish its compliance with the reasonable security requirement by establishing its compliance with another New York state or federal data security regime. These businesses are called "compliant regulated entities." The SHIELD Act does not specify what a business has to show to establish that it is compliant with another regime. It does suggest that the standards of the agency responsible for overseeing the other regime will be used to judge compliance.

What is "Reasonable" Depends on Size – Although small businesses are not exempted from the Act, the reasonableness of a small business's safeguards is evaluated in light of its size and complexity, the nature and scope of its activities and

the sensitivity of the personal information it collects from or about consumers. To qualify as a "small business," a business must: (1) employ fewer than 50 people; (2) have earned less than $3 million in gross annual revenue in each of the last three fiscal years; or (3) have less than $5 million in year-end total assets. Small businesses should evaluate how their data security safeguards compare to peers, and whether they meet industry best practices for businesses of their size.

Data Security Safeguards to Implement – A business must, if not a compliant regulated entity, implement a data security program that includes the specific administrative, technical and physical safeguards the Act dictates. Most of the required safeguards are already considered industry best practices. Among other things, the Act requires businesses to dispose of private information within a reasonable amount of time after the information is no longer needed. Disposal includes taking steps to ensure the information cannot be read or reconstructed. Limiting collection to only so much personal or private information as is actually needed can ease protection and disposal obligations down the line. Also of note, the Act requires businesses to select service providers capable of maintaining appropriate safeguards and require those safeguards by contract. The following chart outlines the safeguards businesses must adopt.

Administrative Safeguards	Technical Safeguards	Physical Safeguards
• Designate one or more employees to coordinate the security program. • Identify reasonably foreseeable internal and external risks. • Assess the sufficiency of implemented safeguards to control identified risks. • Train employees on the security program practices and procedures. • Select service providers capable of maintaining appropriate safeguards and require those safeguards by contract. • Adjust the security program in light of new business circumstances.	• Assess risks in network and software design and in information processing, transmission and storage. • Detect, prevent and respond to attacks or system failures. • Regularly test and monitor the effectiveness of key features of the security program.	• Assess risks associated with information storage and disposal. • Detect, prevent and respond to intrusions. • Protect against unauthorized access to or use of private information during or after collection, transportation or destruction of information. • Dispose of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing any media so that the information cannot be read or reconstructed.

III. Attorney General Enforcement

The New York Attorney General has sole authority to enforce the SHIELD Act. No private right of action is available. The Attorney General may bring an action to enjoin violations and seek civil penalties. For data breach notification violations, a court may award damages for actual costs or losses incurred by the person entitled to notice, including consequential financial losses. For knowing or reckless data breach notification violations, a court may impose civil penalties of the greater of $5,000 or up to $20 (up from $10) per "instance of failed notification" up to $250,000 (up from $150,000). The Act also extends the statute of limitation to three years, from two.[5] For reasonable security violations, a court may impose civil penalties of not more than $5,000 per violation.

IV. Conclusion and Proactive Steps to Take Now

New York now stands beside California, Massachusetts, and other states that have expanded the scope of their data protection powers beyond their borders to go after businesses that own or license their residents' private information regardless if the businesses are located or doing business in their state. Businesses should begin to act soon to try to minimize the risk of a future enforcement action. The following are practical steps businesses can take now:

- Determine if you own, license, or maintain computerized data that includes any New York resident's private information, and evaluate how you process that information.
- If your data includes any New York resident's private information, identify which other state or federal data security rules or regulations may apply to your specific industry and business. Determine if your compliance with any such regimes may provide a basis for claiming compliance under data security provisions of the SHIELD Act.
- Work with internal and external stakeholders to develop and document an information security program, or to update your existing program, to address the new requirements. For some businesses, it may make sense to develop and document a cross-walk mapping existing information security controls to the standards set forth in the SHIELD Act.
- Gather and review service provider agreements to identify contracts that may need to be amended to comply with the Act's reasonable security requirements.
- Create a protocol for determining whether a "breach of the security of the system" occurred under the SHIELD Act and whether notice is required. Update any existing breach response plans accordingly. Ensure you document and maintain the determination.
- If you have not done so already, establish a role within your organization to coordinate, monitor and regularly update your information security program. If the role exists, ensure those responsible are aware of the SHIELD Act's requirements.
- HIPAA covered entities should review their policies and procedures relating to data incidents and breach notification, and update as needed to address the SHIELD Act's requirements. Privacy officers, security officers, and others involved in incident response may need to be trained on the SHIELD Act's requirements.

- If applicable, determine if you are a “small business” and, if so, understand what may constitute reasonable safeguards given your size, industry and the relevant information.
- Carefully follow the state Attorney General’s enforcement actions under the SHIELD Act to assess the new law’s further implications for your business.

APPENDIX – Chart of Key Revised Notice Obligations and Deadlines

Recipient of Notice	Requirements	Deadlines
Affected New York Residents	When a business that *owns or licenses* data that includes a New York resident’s private information suffers a breach, it must inform any New York resident whose information was, or is reasonably believed to have been, affected.	Notice must be provided “in the most expedient time possible and without unreasonable delay.” Delay is permissible: (1) if consistent with legitimate law enforcement needs; or (2) if consistent with any measures necessary to determine the scope of the breach and restore the integrity of the system.
Upstream Notice to Data Owner or Licensee	When a business suffers a breach and data that it *maintains* but does not own or license (e.g., a vendor maintaining data on behalf of another entity), that includes a New York resident’s private information is exposed, the business must inform the owner or licensee of the information, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.	Upstream notice must be provided *immediately* following discovery.
NY Attorney General, Dept. of State, Div. of State Police	When a business’s obligation to provide notification under the SHIELD Act is triggered and the business provides notice to New York residents (whether under the SHIELD Act or under a different data security regime), it must also provide notice to the Attorney General, Department of State, and Division of State Police. Notice must include information on the timing, content, and distribution of the notices to residents, the approximate number of residents affected, and a copy of the template notice.	The Act does not specify a deadline. Notice must be made without delaying notice to affected residents.

Recipient of Notice	Requirements	Deadlines
NY Attorney General (Only)	When a business provides notification of a breach to the HHS as required under HIPAA, it must also provide notice to the Attorney General. This applies even if the breach involves information that is not "private information." The Act contains no express exemption for smaller breaches reported to HHS in annual breach logs as required by HIPAA, so the plain language of the law could be interpreted to require Attorney General notices for smaller HIPAA breaches as well as for breaches affecting 500 or more individuals.	Notice must be provided within five business days of giving notice to HHS.
Consumer Reporting Agencies (CRAs)	When a business notifies more than 5,000 New York residents at once, it must also notify CRAs. Notice must include information on the timing, content and distribution of the notices to residents, and the approximate number of residents affected.	The Act does not specify a deadline. Notice to CRAs must be made without delaying notice to affected residents.

1 The Act leaves in place the prior definition of "personal information" 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."

2 The factors to consider in determining unauthorized acquisition remain the same as in the prior law and include indications that a person without valid authorization has physical possession and control over, downloaded or copied, or used the information.

3 Businesses that *maintain* (but do not own or license) computerized data that includes private information of any New York resident retain their upstream notification obligations under the Act, regardless of their compliance with other New York state or federal data security regimes.

4 *See* 45 C.F.R. § 164.408 (Notification to the Secretary).

5 The Act provides a maximum limitations period of six years, unless the business took steps to hide its violation.

akingump.com