New York SHIELD Act FAQs

By Joseph J. Lazzarotti, Jason C. Gavejian, Mary T. Costigan, Delonie A. Plummer and Damon W. Silver

March 11, 2020

Over the past few months, businesses across the country have been focused on the California Consumer Privacy Act (CCPA) which dramatically expands privacy rights for California residents and provides a strong incentive for businesses to implement reasonable safeguards to protect personal information. Their focus should turn back east as the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), becomes effective in less than two weeks. With the goal of strengthening protection for New York residents against data breaches affecting their private information, the SHIELD Act imposes more expansive data security and updates its existing data breach notification requirements.

This Special Report highlights some features of the SHIELD Act. Given the complexities involved, organizations would be well-served to address their particular situations with experienced counsel.

When does the SHIELD Act become effective?

The SHIELD Act has two effective dates:

- October 23, 2019 – Changes to the existing breach notification rules
- March 21, 2020 – Data security requirements

Which businesses are covered by the SHIELD Act?

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. Previously, the obligation to provide notification of a data breach under New York's breach notification law applied only to persons or businesses that conducted business in New York.

Are there any exceptions for small businesses?

As before the SHIELD Act, 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. The same is true for persons or businesses that *maintain* (but do not own) computerized data that includes private information of New York residents. Persons or businesses that experience a breach affecting that information must notify the information's owner or licensee.

However, the SHIELD Act's data security obligations include some relief for small businesses, defined as any person or business with:

1. fewer than fifty employees;
2. less than three million dollars in gross annual revenue in each of the last three fiscal years; *or*
3. less than five million dollars in year-end total assets, calculated in accordance with generally accepted accounting principles.

Covered small businesses still must maintain a security program, but the nature and extent of that program can be modified based on certain factors. While a small business must adopt reasonable administrative, technical, and physical safeguards, those safeguards can be shaped and made appropriate for:

- 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.

What is "Private Information" under the SHIELD Act?

Unlike many other states that use the term "personal information" to define the data set to be

Meet the Authors

Joseph J. Lazzarotti

Principal
Berkeley Heights 908-795-5205
Email

Jason C. Gavejian

Principal
Berkeley Heights 908-795-5139
Email

Mary T. Costigan

Of Counsel
Berkeley Heights 908-795-5135
Email

Delonie A. Plummer

Associate
New York Metro
White Plains 914-872-6923
Email

protected, the SHIELD Act uses the term "private information" to refer to the key data elements to be protected under the statute. Businesses that had to apply the breach notification law in New York before the SHIELD Act should become familiar with the new law's expanded definition of private information.

The SHIELD Act defines "private information" the same way for both the breach notification and the data security protection requirements. Private information is, in part, 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."

However, the SHIELD Act expands the definition of "private information" to include either:

(i) 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*

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

This definition is significantly broader than the previous law. For example, the new definition adds biometric information, as well as account numbers and credit/debit card numbers that can be used to access a financial account *without* other identifying information. The definition also adds online account credentials to the definition.

Like the CCPA, private information excludes publicly available information that is lawfully made available to the general public from federal, state, or local government records. The SHIELD Act's expansive definition of "private information" is still not as broad as the definition of the analogous term under the laws of other states. For example, California, Illinois, Oregon, and Rhode Island have expanded the applicable definitions in their laws to include not only medical information, but also certain health insurance identifiers.

Does the SHIELD Act apply to health information, HIPAA-covered entities?

No, the SHIELD Act generally does not apply to health information. However, covered entities and business associates subject to the privacy and security rules issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) need to be aware of the SHIELD Act. Remember, the HITECH Act empowered state attorneys general to enforce HIPAA.

If a covered entity must provide notice of a breach of the security of the system to affected persons under the HIPAA breach notification rule, the SHIELD Act will not require an additional notification, although the covered entity still must notify the applicable state agencies and the consumer reporting agencies as otherwise required under the law.

In addition, HIPAA-covered entities required to notify the Secretary of Health and Human Services of a breach of information that is not "private information" (as defined above) also must provide notification to the New York State Attorney General's office within five business days of notifying the Secretary.

As for the data security protections added by the SHIELD Act, a person or business can comply with those requirements if the person or business is a "compliant regulated entity." That is, a person or business subject to and in compliance with a designated data security regulatory framework will be deemed to be in compliance with the data security requirements under the SHIELD Act. The regulatory framework under HIPAA and HITECH is one of the frameworks designated by the New York SHIELD Act.

Thus, any HIPAA-covered entity or business associate compliant with HIPAA will be deemed to satisfy

Damon W. Silver

Associate
New York Metro
New York City 212-545-4063
Email

the data security requirements under the SHIELD Act. However, this does not mean that any HIPAA-covered entity is exempted from the SHIELD Act. The entity *must be compliant with* the applicable provisions of HIPAA and HITECH to be deemed to satisfy the SHIELD Act's data security requirements.

Does the SHIELD Act apply to employee data?

There was some uncertainty on this question under the CCPA due to the broad definition of "consumer" under that law. Ultimately, albeit temporarily, the CCPA was amended to clarify its application to employees.

Under the SHIELD Act, there does not appear to be as much controversy, but a similar issue exists. The term "personal information," upon which private information is largely based, means any information concerning a *natural person* which, because of name, number, personal mark, or other identifier, can be used to identify such natural person. Employees are natural persons and, if they are New York residents, likely will be protected by the SHIELD Act.

Has the definition of the term "breach of security of the system" changed?

Yes, and the change will make notifications of data incidents affecting New York residents more likely.

The term "breach of the security of the system" is important under the SHIELD Act because, if a data incident meets that definition, notifications to affected persons or businesses likely will have to be made. The SHIELD Act alters the definition of "breach of the security of the system" in two significant ways.

First, it broadens the circumstances that qualify as a "breach" by including within the definition incidents that involve "access" to private information. Under the previous law, only "acquisitions" of private information could trigger a notification requirement. The new law also adds several factors for determining whether there has been unauthorized "access" to private information, including "indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person."

Second, the new law expands one of the terms used to define "breach of the security of the system" — "private information." By expanding the definition of private information, as discussed above, the new law effectively expands the situations that could result in a breach of the security of the system. The SHIELD Act retains the "good faith employee" exception to the definition of "breach."

Did the SHIELD Act add any exceptions to the breach notification requirements?

The changes to the definition of "breach of the security of the system" (see above) likely will increase the circumstances under which notifications of a breach will need to be made to New York residents. However, the SHIELD Act also added a significant exception to the notification requirement, sometimes called the "risk of harm" exception.

Under this exception, notice to affected persons is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines that exposure likely will not result in misuse of that information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials.

Similar to the rule in Florida and a few other states, if a person or business believes this exception applies, it must document that determination in writing and retain that documentation for at least five years. In addition, if the incident affects more than 500 residents of New York, the person or business also must provide the written determination to the state attorney general within 10 days after the determination.

Did the SHIELD Act change the notification content requirements in the event of a reportable breach?

Before the SHIELD Act, New York's breach notification law required the notification to include contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specifying which of the elements of personal information and private information were, or are reasonably believed to have been, acquired.

Under the new law, notifications also must include the telephone numbers and websites of the relevant state and federal agencies that provide information on security breach response and identity theft prevention and protection information. The SHIELD Act also requires the notices encompass access of private information, not just acquisition. Finally, the new law adds another requirement when notifying state agencies, including the Attorney General. In addition to the content and distribution of the notices and approximate number of affected persons, persons and businesses now must include a copy of the template of the notice to be sent to affected persons.

What rights do New York residents have over their personal information under the SHIELD Act?

Unlike the CCPA and certain other laws, such as HIPAA and the General Data Protection Regulation (GDPR) in the EU, the SHIELD Act does not create affirmative rights for New York residents. Under the CCPA, for example, natural persons residing in California ("consumers") have the right to request that businesses covered by the law delete their personal information. There is no such right under the SHIELD Act, although efforts are underway (*see* Senate Bill 5642) to create similar rights concerning personal information.

What are "reasonable" data security requirements?

As with the notification requirements, the SHIELD Act requires any person or business that owns or licenses computerized data that includes private information of a resident of New York to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information. Again, certain "compliant regulated entities" that satisfy other regulatory obligations they have, such as HIPAA and the Gramm-Leach-Bliley Act, will be considered in compliance with this section of the law. Additionally, as mentioned above, small businesses as defined by the SHIELD Act can consider certain factors to shape its data security program.

The SHIELD Act does not mandate specific safeguards, but it provides several examples of practices that are considered reasonable administrative, technical and physical safeguards. These examples suggest the kinds of safeguards businesses should be adopting, but they are not the only safeguards companies should be adopting.

Administrative Safeguards

- Designate individual(s) responsible for security programs;
- Conduct a risk assessment process one that identifies reasonably foreseeable internal and external risks and assesses the sufficiency of safeguards in place to control those risks;
- Train and manage employees in security program practices and procedures;
- Select capable service providers and require safeguards by contract; and
- Adjust program(s) in light of business changes or new circumstances.

Physical Safeguards

- Assess risks of information storage and disposal;
- Detect, prevent, and respond to intrusions;
- Protect against unauthorized access/use of private information during or after collection, transportation, and destruction/disposal; and
- Dispose of private information within a reasonable amount of time after it is no longer needed for business purposes.

Technical Safeguards

- Assess risks in network and software design;
- Assess risks in information processing, transmission, and storage;
- Detect, prevent, and respond to attacks or system failures; and
- Regularly test and monitor the effectiveness of key controls, systems, and procedures.

In addition to the safeguards in the new law, organizations should consider others, such as:

- Developing access management plans;
- Maintaining written policies and procedures;
- Applying sanctions to individuals who violate the organization's data privacy and security policies and procedures;
- Implementing facility security plans;
- Maintaining and practicing disaster recovery and business continuity plans;
- Tracking inventory of equipment and devices;
- Deploying encryption and data loss prevention tools;
- Develop and practice an incident response program;
- Regularly updating antivirus and malware protections;
- Utilizing two-factor authentication; and
- Maintaining and implementing a record retention and destruction policy.

Do New York residents have a private right of action under the SHIELD Act?

The SHIELD Act does not create a private right of action. This means that if a New York resident believes a business subject to the SHIELD Act failed to comply with the law's data protection requirements and caused the individual harm as a result, that individual could not sue the business under the SHIELD Act. Of course, the individual might be able to sue under theories of negligence or breach of contract.

By contrast, the CCPA expressly provides a private right of action and statutory damages if a data breach is caused by the lack of reasonable safeguards, even if there were no actual harm.

What are the penalties for failing to comply with the SHIELD Act?

Although the SHIELD Act does not authorize a private right of action, the Attorney General may bring an action to enjoin violations of the law and obtain civil penalties.

For data breach notification violations that are *not* reckless or knowing, a court may award damages for actual costs or losses incurred by a person entitled to notice, including consequential financial losses. For knowing and reckless violations, a court may impose penalties of the greater of $5,000 or up to $20 per instance with a cap of $250,000. For reasonable safeguard requirement violations, a court may impose penalties of not more than $5,000 per violation.

***

The SHIELD Act will have far-reaching effects, as any business that holds private information of a New York resident — regardless of whether the organization does business in New York — must comply the new law. The SHIELD Act also shows how seriously New York, like other states across the nation, is taking privacy and data security matters. Regardless of their location, organizations should be assessing and reviewing their data breach prevention and response activities, building robust data protection programs, and investing in written information security programs (WISPs).

Jackson Lewis attorneys are available to answer inquiries regarding the SHIELD Act and assist employers in their compliance efforts.