Linklaters

August 2019

# New York State Expands Data Breach Notification Law and Requires Businesses to Have More Rigorous Cybersecurity Safeguards

Contents



On July 25, 2019, Governor Andrew Cuomo signed New York's latest cybersecurity bill – the Stop Hacks and Improve Electronic Data Security Act (the "**SHIELD Act**" or the "**Act**"), amending the state's existing data breach law to impose more rigorous data breach notification requirements on companies.[1] The SHIELD Act is New York's latest answer to the increasing prevalence in the digital age of data breaches that threaten the protection of private information. Speaking on the heels of the SHIELD Act's enactment, New York Attorney General Letitia James remarked that hacks of financial institutions are becoming far too commonplace, raising the question of whether companies are doing enough to prevent future data breaches. "We cannot allow hacks of this nature to become every day occurrences," James said.[2]

The SHIELD Act's provisions relating to notification requirements will begin to take effect October 23, 2019, while requirements relating to data security protections will be effective on March 21, 2020.

## The SHIELD Act Expands New York's Data Breach Notification Laws

The SHIELD Act expands the scope of New York's data breach laws in multiple ways. Among other things, the Act broadens the scope of information subject to New York's data breach notification requirements, expands the definition of data breach under New York law, and increases the jurisdictional reach of New York's data breach laws.

[1] 2019 New York Senate Bill No. 5575. The SHIELD Act amends N.Y. GEN. BUS. LAW § 899-aa and N.Y. STATE TECH. LAW § 208, and adds N.Y. GEN. BUS. LAW § 899-bb. For the text of the SHIELD Act, see https://www.nysenate.gov/legislation/bills/2019/s5575.

[2] Press Release, N.Y. State Office of the Att'y Gen., Attorney General James' Statement on Capital One Security Breach (July 30, 2019), https://ag.ny.gov/press-release/attorney-general-james-statement-capital-one-security-breach.

## Broader Definition of "Private Information"

The SHIELD Act broadens the existing definition of "private information" contained in New York's privacy laws. The "private information" definition identifies the different types of data that, if implicated in a data breach, trigger a notification requirement. Under the Act, "private information" will now include, in combination with a name, number, personal mark, or other identifier used to identify a person, (1) an account, credit or debit card number, if that number could be used to access an individual's financial account without any additional identifying information, like a security code or password; or (2) biometric information, such as a fingerprint, voice print or retina or iris image. Additionally, the Act adds to the definition of private information "a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account."[3]

## Expanded Definition of What Constitutes a Breach

The SHIELD Act also revises the definition of "breach of the security system" by lowering the threshold for what qualifies as a "breach." Specifically, while the original law covered only the unauthorized "acquisition" of private information, the amended law reaches incidents that involve mere "access" to private information, regardless of whether such unauthorized access resulted in "acquisition" of that information.[4] Under the Act, an incident that involves a hacker merely viewing personal information may qualify as a "breach of the security of the system" and require the company to provide notice of the data breach. In assessing whether personal information has been "accessed," a company or person may consider, among other things, "indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person."[5] Good faith access to or acquisition of private information by an employee or agent of the business – so long as such access or acquisition was for the purposes of the business – would not constitute a breach of the security of the system.[6]

## Broader Jurisdictional Reach of the Data Breach Notification Requirements

Significantly, while New York's original data breach notification requirement covered only persons and businesses "conduct[ing] business in New York state," the SHIELD Act provides even broader protections to New York residents. The Act requires that any person or business that owns or licenses computerized data that includes New York residents' private information (each such person or business, a "**covered entity**") must comply with the Act's breach notification requirements,

[3] N.Y. GEN. BUS. LAW § 899-aa(1)(b).
[4] N.Y. GEN. BUS. LAW § 899-aa(1)(c).
[5] *Id.*
[6] *Id.*

regardless of whether the person or business conducts business in New York state.[7]

## When Notice is Required

Under the SHIELD Act, once a covered entity discovers a breach in the security of their system (irrespective of whether such breach involves mere "access" or "acquisition"), such covered entity is required to notify any New York resident whose private information was, or is reasonably believed to have been, accessed or acquired, as well as the New York Attorney General, the Department of State Division of Consumer Protection, and the Division of State Police.[8] Additionally, if over 5,000 New York residents are required to be notified at one time, a covered entity must also report the breach to consumer reporting agencies.[9]

The Act provides for certain exceptions to the breach notification requirements. For instance, notice is not required if "exposure of private information" was inadvertent or unlikely to result in harm. To qualify for this exception, a covered entity must reasonably determine that "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."[10]

Additionally, separate notice is not required when notice has already been provided pursuant to certain other state or federal cybersecurity laws – like the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"),[11] the NY Department of Financial Services Cybersecurity Regulation (the "**NYDFS Regulations**"),[12] and the Gramm-Leach-Bliley Act ("**GLBA**").[13] However, where notice to affected persons is not required pursuant to this exception, notice must still be provided to the New York Attorney General, the Department of State Division of Consumer Protection and the Division of the State Police and, as referenced above, if over 5,000 New York residents are notified, to consumer reporting agencies.[14]

## Implementing Cybersecurity Safeguards

In addition to its expanded notification requirements, the SHIELD Act requires covered entities to develop, implement, and maintain "reasonable safeguards" to protect the security, confidentiality, and integrity of private information.[15] Reasonable safeguards, as articulated by the law, include risk assessments, employee training, selecting vendors capable of maintaining appropriate

[7] N.Y. GEN. BUS. LAW §§ 899-aa(2), 899-bb.
[8] *Id.* § 899-aa(8)(a).
[9] *Id.* § 899-aa(8)(b).
[10] *Id.* § 899-aa(2)(a).
[11] 45 C.F.R. §§ 160, 164.
[12] 23 NYCRR 500.
[13] 15 U.S.C. §§ 6801-6809.
[14] N.Y. GEN. BUS. LAW § 899-aa(2)(b).
[15] *Id.* § 899-bb.

safeguards and implementing contractual obligations for those vendors, and disposal of private information within a reasonable time.[16] A small business (i.e., any business with (1) fewer than 50 employees, (2) less than $3 million in gross annual revenue in each of the last three years, or (3) less than $5 million in year-end total assets) will be deemed compliant if its data security program is appropriate in light of 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."[17] Again, companies in compliance with laws such as HIPAA, the NYDFS Regulations, and GLBA are considered in compliance with this requirement.[18]

## Enforcement and Rights of Action

Significantly, the SHIELD Act does not authorize a private right of action for affected consumers. Instead, the New York 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 under the Act, including consequential financial losses. By contrast, for knowing or reckless notice violations, a court may impose penalties against a covered entity equal to the greater of $5,000 or up to $20 per instance of failed notification, with a cap of $250,000 per covered entity – increasing the maximum penalty of $150,000 provided for under New York's existing data protection law.[19]

## Identity Theft Prevention and Mitigation Services Act

On the same day that Governor Cuomo signed into law the SHIELD Act, he also signed the Identity Theft Prevention and Mitigation Services Act, requiring New York consumer credit reporting agencies that have experienced unauthorized acquisition of, or access to, Social Security numbers to provide to affected customers, at no cost, 5 consecutive years of identity theft prevention and mitigation services.[20] The law, which becomes effective on September 23, 2019, also requires these credit reporting agencies to provide affected consumers with information on how to freeze their credit.

[16] *Id.* § 899-bb(2)(b)(ii).
[17] *Id.* § 899-bb(1)(c).
[18] *Id.* § 899-bb(2)(b)(i).
[19] N.Y. GEN. BUS. LAW § 899-aa(6)(a).
[20] 2019 New York Senate Bill No. 3582.

Linklaters

The SHIELD Act is but one piece of an evolving landscape of cybersecurity requirements and related enforcement actions. But by both expanding the scope of covered entities required to notify New York residents whose personal information has been implicated in a data breach and lowering the standard for determining when a notification is required, the Act has particularly broad-reaching effects. It is critical that persons and entities – wherever located – that collect, process or store private information of New York residents continually assess and review their incident response plans and data security programs to ensure compliance with the SHIELD Act's rigorous requirements. By remaining informed about, and vigilant against, new types of hacks and threats, covered entities may better protect not only consumers' personal information, but also their own reputations within the market.

Author: Adam Lurie, Doug Davison, Joshua Ashley Klayman, Caitlin Potratz Metcalf, and Aviva Kushner



## Contacts

For further information please contact:

**Adam Lurie**
Partner, Head of the U.S. Dispute Resolution Practice

(+1) 202 654 9227

adam.lurie@linklaters.com

**Doug Davison**
Partner

(+1) 202 654 9244

doug.davison@linklaters.com

**Joshua Ashley Klayman**
Senior Counsel, U.S. Head of FinTech and Head of Blockchain and Digital Assets

(+1) 212 903 9047

joshua.klayman@linklaters.com

**Caitlin Potratz Metcalf**
Senior US Associate

(+1) 202 654 9240

caitlin.potratz@linklaters.com

**Aviva Kushner**
Law Clerk

(+1) 202 654 9217

aviva.kushner@linklaters.com

Linklaters LLP

Linklaters.com