New York Updates Data Breach Notification Law and Imposes "Reasonable Security" Requirement

July 29, 2019

New York Governor Andrew Cuomo has signed into law a set of amendments to New York's data breach notification law that expands the definition of personal information, outlines "reasonable" data security safeguards that businesses holding New Yorkers' data must implement, and provides that credit reporting agencies must guarantee identity theft protections if their systems are breached.

Debevoise & Plimpton

The Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") expands the definition of personal information and, most significantly, creates new substantive cybersecurity requirements. The SHIELD Act's amendments to the existing data breach notification law requirements take effect on October 23, 2019; the effective date for the new data security requirements is March 21, 2020.

What are the new data security requirements? For regulated entities already required to comply with another cybersecurity legal regime — defined as either the federal Gramm-Leach-Bliley Act ("GLBA"), the federal healthcare standards ("HIPAA/HITECH"), the New York Department of Financial Services' Cybersecurity Regulation ("DFS Part 500"), or any other data security rules and regulations promulgated by the federal or New York State government — compliance with that regime is a safe harbor, meaning the entity is deemed compliant with New York's new "reasonableness" standard.

For everyone else, the SHIELD Act requires any person or business that owns or licenses the computerized personal information of any New York resident to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information including, but not limited to, disposal of data."

The SHIELD Act does not map out a complete definition of what "reasonable" security means. Rather, like California and the dozen or so other states that have written a reasonableness requirement into their cybersecurity laws, New York apparently intends for this to be an evolving standard without rigid definitions. The bar likely will get higher over time as threat vectors evolve, and as the collective sense of what is an objectively appropriate cybersecurity program evolves to match.

That said, the SHIELD Act does set out a partial roadmap of what a business will need to do, including:

Implement reasonable administrative safeguards, such as conducting a cybersecurity risk assessment, designating an employee responsible for cybersecurity, continuously updating its risk assessment and necessary security measures, and training for all employees on the security program.

Implement reasonable technical safeguards sufficient to identify and assess risks to network security and data processing or storage, and regularly test and monitor the technical security of the system.

Implement reasonable physical safeguards that protect against unauthorized access, detect and respond to intrusions, and ensure the safe and timely disposal of data that is no longer needed for business purposes.

A "small business" — one with fewer than 50 employees, less than $3 million in annual revenue, or less than $5 million in assets — is permitted to implement a cybersecurity program that is reasonable for the size and complexity of the business, but is still subject to the reasonable security requirement.

The SHIELD Act does not create a private right of action, but does authorize enforcement proceedings by the New York Attorney General under New York's basic consumer protection statute, section 349 of the General Business Law — for any covered person or entity found to have failed to implement reasonable cybersecurity. By the plain terms of the SHIELD Act, it appears that a lack of "reasonable" security is actionable by the state attorney general with or without a data breach. The state attorney general is empowered under Section 349 to seek injunctive relief and may obtain civil penalties under Section 350(d).

What are the updates to data breach notification requirements?

- The amendments extend the notification requirements to any person or entity with private information of a New York resident. Previously, the notification law only applied to persons or entities conducting business in New York State.

- Unauthorized *access* to personally identifiable information will now trigger the breach notification requirement. Previously, New York limited breach notification to circumstances where personal data was *acquired* without authorization. To determine if personally identifiable information has been accessed, businesses should consider if the information was viewed, communicated with, used, or altered by an unauthorized person. This appears to leave room for businesses to determine,

through investigation, that personal information was only potentially accessed but not actually accessed — meaning that no notifications would be required. Regulated entities that give notice to affected persons pursuant to other regulatory regimes must still give notice to New York State officials, but need not give additional notice to New York residents. The scope of this safe harbor is the same as described above for the "reasonable security" requirement: that is, notice given pursuant to GLBA, HIPAA/HITECH, DFS Part 500, or other federal or New York standards creates a safe harbor from the separate consumer notification requirements of New York's breach notification law.

- The definition of personal information has been expanded to include:
  - An "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 without additional identifying information, security code, access code, or password;"
  - "Biometric information," "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;" and
  - "[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."

How can businesses satisfy the notification requirement?

E-mail notice may be provided, unless the breached information includes an e-mail address in combination with a password or security question permitting access to an online account.

- When a breach involves an e-mail address and password or security question, notification can be provided by posting a "clear and conspicuous notice" on the consumer's account.
- The notice should be accessible only if the consumer is connected to his or her account from an IP address or online location customarily associated with the consumer's online account.

When would notification not be required?

- Notification would not be required if the exposure of personal information was an inadvertent disclosure by persons authorized to access the information, and the person or business determines such exposure likely will not result in (1) misuse of

the information; (2) financial harm to the affected person; or (3) emotional harm in the case of unknown disclosure of online credentials. This clarifies that certain common scenarios, such as inadvertently e-mailing or otherwise providing information to a trusted but unauthorized recipient, will not trigger breach notification requirements.

- Any determination that exposure will not result in misuse, financial harm, or emotional harm must be documented in writing and the writing must be kept for at least five years.

    - If the incident affects more than 500 residents of New York and such a determination was made, the person or business must provide the written determination to the Attorney General within ten days.

Governor Cuomo also signed the **Identity Theft Prevention and Mitigation Services Act**, which outlines requirements for credit reporting agencies following a breach. The Act takes effect on September 23, 2019, and applies to breaches of credit reporting agencies that occurred within the three years prior to the Act's effective date.

What protections must be offered?

If a credit reporting agency experiences a security breach which includes social security numbers, the agency is required to offer reasonable identity theft prevention services to individuals affected by the breach.

If applicable, the agency should also provide free identity theft mitigation services for up to five years.

Are there any exceptions?

Yes, the agency does not have to provide identity theft prevention or mitigation services if it determines that the breach is unlikely to result in harm to consumers.

* * *

Our Cybersecurity and Data Privacy Team would be pleased to discuss these issues with our clients and friends.

Please do not hesitate to contact us with any questions.

NEW YORK


Jeremy Feigelson
jfeigelson@debevoise.com


Jim Pastore
jjpastore@debevoise.com


Stephanie M. Cipolla
smcipolla@debevoise.com


Christopher S. Ford
csford@debevoise.com


Jaime Freilich
jmfreilich@debevoise.com


Alexandra P. Swain
apswain@debevoise.com

WASHINGTON, D.C.


Luke Dembosky
ldembosky@debevoise.com