August 1, 2019

New York Shields Consumer Data With Broader Breach Notification, Security, and Identity Theft Protection Laws

On July 25, New York Governor Andrew Cuomo signed two laws to protect individuals against security breaches: the Stop Hacks and Improve Electronic Data Security (SHIELD) Act (S3575B/A5635) and an amendment to provide for certain identify theft protection and mitigation services (A2374/S3582).

The SHIELD Act

The SHIELD Act places additional obligations on businesses that collect "private information" (broadly, personal information, excluding publicly-available information) from or about New York residents by expanding the reach and application of the state's breach notification law, and by imposing new notice and security obligations.

Expanded Scope and Broader Definitions. The SHIELD Act expands the reach of New York's breach notification law by:

- broadening the scope to apply to any person or business that collects private information of a New York resident (not just those doing business in New York);

Key Takeaways:

- Personal information subject to New York's breach notification law now includes biometric data, online credentials and account numbers (even without a PIN/code if the account could be used without those).
- Breach notification obligations now apply to all businesses that collect private information of New York residents (whether or not doing business in New York).
- Regulated entities, such as Covered Entities, are now required to notify the New York AG of a breach affecting New York residents in addition to regulatory notification requirements.
- Requires businesses to implement a data security program that includes reasonable safeguards to protect the security, confidentiality and integrity of private information.

For more information on data protection and privacy laws, please contact your Katten attorney, the firm's **Privacy, Data and Cybersecurity** group or any of the following:

Doron S. Goldstein
+1.212.940.8840
doron.goldstein@kattenlaw.com

Matthew R. Baker
+1.415.293.5816
matthew.baker@kattenlaw.com

Megan Hardiman
+1.312.902.5488
megan.hardiman@kattenlaw.com

Dagatha L. Delgado, an Intellectual Property staff attorney in Katten's New York office, contributed to this advisory.

- expanding the definition of private information to include biometric information, online credentials (i.e., usernames or email addresses with their corresponding passwords and/or security questions and answers), and account numbers or debit or credit card numbers, alone, if the number could be used without a PIN or security code; and
- expanding the definition of "data breach" to include data that may have been accessed, not just acquired.

AG Notification by Regulated Entities. Entities regulated under the Gramm–Leach–Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or other regulations with breach notification requirements will now be required to notify the New York Attorney General (AG), state department, state police and consumer reporting agencies (CRAs). HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH) covered entities have five days to notify the AG after notifying the secretary of Health and Human Services.

Risk of Exposure Analysis. If private information was inadvertently disclosed, but the business reasonably determines that risk of misuse or harm (financial or emotional) is not likely, notice is not required.

Data Security Program. The SHIELD Act also imposes a new obligation on businesses, including small businesses, to implement a security program containing reasonable administrative, technical and physical safeguards (e.g., risk assessments, training, and service provider contractual requirements). Regulated entities are deemed in compliance with this requirement provided they comply with their applicable regulatory security requirements.

Increased Penalties. The law does not create a private right of action, but increases penalties for failure to comply with notification obligations to the greater of $5,000 or up to $20 per instance (capped at $250,000). Additionally, the AG can bring an action to enjoin any business that fails to implement a reasonable data security program and can obtain civil penalties of up to $5,000 per violation.

Identity Theft Protection

Governor Cuomo also signed an amendment requiring CRAs that experience a breach involving social security numbers to offer affected individuals reasonable identity theft prevention services and, if applicable, identity theft mitigation services for up to five years. The new requirement takes effect 60 days after it was signed into law, and will retroactively apply to any CRA breach that occurred in the past three years from the effective date.