July 31, 2019

New York Governor Signs Data Security Law

SHIELD ACT Expands Notification Obligations for Breaches Affecting New York Residents

On July 25, 2019, New York Governor Andrew M. Cuomo signed into law a new data security law, the Stop Hacks and Improve Electronic Data Security ("SHIELD") Act.[1] The SHIELD Act expands New York's existing data breach notification law by broadening its scope and imposing more stringent notification and procedural requirements on businesses in the aftermath of a data breach. The Act also requires companies to implement "reasonable safeguards" to protect consumer data.

The SHIELD Act

The SHIELD Act comes in the wake of several high-profile data breaches. In his press release announcing the legislation, Governor Cuomo highlighted the data breach of the credit-reporting company Equifax,[2] which recently agreed to pay up to $600 million to resolve federal and state investigations into the 2017 breach that compromised the information of more than 147 million people.[3] The investigations into Equifax revealed that it had been aware of a vulnerability in its security systems months before the breach occurred, and failed to notice the breach or inform consumers of it for 76 days.[4]

The SHIELD Act expands the definition of what constitutes a data breach, requiring companies to notify any resident of New York state when their private information is accessed—not just when it is acquired—by unauthorized third parties.[5] If unauthorized third parties viewed, "communicated with," used, or altered such information, the new law treats these as indications that unauthorized access took place.[6]

Additionally, the SHIELD Act purports to expand the geographic application of New York's data breach notification law to include any person or entity that "owns or licenses computerized data which includes private information" of a New York resident.[7] This is a significant change from prior legislation, which applied only to persons or entities that conducted business in New York state.

Among other notable changes to prior New York law governing data breaches, the SHIELD Act also:

- Requires that companies implement "reasonable safeguards" to protect consumer data, including reasonable administrative safeguards, reasonable technical safeguards, and reasonable physical safeguards; [8]

- Expands the scope of information covered in the definition of a data breach to include account number, credit card number, or debit numbers (in certain circumstances); biometric information; and user names or email addresses in combination with security passwords or security questions and answers;[9] and

- Updates notification and procedural requirements following a data breach by requiring companies to provide, in their notice to consumers, the contact information of "the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information."[10]

- The Act provides that the New York Attorney General may seek injunctive relief, actual damages for persons harmed by a lack of notice of a data breach, and civil penalties.[11] If the court determines that there was a knowing or reckless violation, the court may impose a civil penalty of the greater of $5,000 or up to $20 per instance of failed notification, provided that the latter amount shall not exceed $250,000.[12] The Act also provides that for violations of the new "reasonable safeguard" requirements, the New York Attorney General can seek to enjoin such violations and can seek civil penalties of not more than $5,000 for each violation.[13]

- All provisions of the Act, with one exception, take effect 90 days after enactment. The exception, Section 4, contains provisions requiring companies to implement "reasonable safeguards" to protect consumer data, and takes effect 240 days after enactment.[14]

Implications

The SHIELD Act is representative of the trend towards heightened requirements regarding data handling and data breaches throughout the United States and internationally.[15] With the steady increase in the number of data breaches, lawmakers and regulators are increasingly focused on ensuring that companies provide transparency to affected consumers (and imposing fines for companies unable or unwilling to comply). In a press release announcing the new law, Governor Cuomo stated: "The stark reality is security breaches are becoming more frequent and with this legislation New York is taking steps to increase protections for consumers and holding these companies accountable when they mishandle sensitive data."[16]

In light of the SHIELD Act, companies wherever located should determine whether they hold data pertaining to New York residents and therefore whether the SHIELD Act's terms apply to them. Covered entities may need to update their data security policies and controls and their incident response plans to comply with the new requirements.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

H. Christopher Boehning +1-212-373-3061 cboehning@paulweiss.com	Roberto J. Gonzalez +1-202-223-7316 rgonzalez@paulweiss.com	Jeh Charles Johnson +1-212-373-3093 jjohnson@paulweiss.com
Jonathan S. Kanter +1-202-223-7317 jkanter@paulweiss.com	Brad S. Karp +1-212-373-3316 bkarp@paulweiss.com	Lorin L. Reisner +1-212-373-3250 lreisner@paulweiss.com
Jeannie S. Rhee +1-202-223-7466 jrhee@paulweiss.com	Richard C. Tarlowe +1-212-373-3035 rtarlowe@paulweiss.com	Adam J. Bernstein +1-212-373-3297 abernstein@paulweisss.com

Associates Elana R. Beale and Julie L. Rooney contributed to this client memorandum.

[1] *Governor Cuomo Signs Legislation Protecting New Yorkers Against Data Security Breaches*, Governor's Press Office (July 25, 2019), https://www.governor.ny.gov/news/governor-cuomo-signs-legislation-protecting-new-yorkers-against-data-security-breaches. Also on July 25, 2019, Governor Cuomo signed A.2374/S.3582, a bill that requires consumer credit reporting agencies to offer identity theft prevention and mitigation services for up to five years to consumers who have been affected by a data breach involving their social security numbers. S.B. 3582, 242nd Leg. Sess. (N.Y. 2019). The legislation also requires credit reporting agencies to provide consumers with the right to freeze their credit at no cost.

[2] *Governor Cuomo Signs Legislation Protecting New Yorkers Against Data Security Breaches*, Governor's Press Office (July 25, 2019), https://www.governor.ny.gov/news/governor-cuomo-signs-legislation-protecting-new-yorkers-against-data-security-breaches.

[3] *Attorney General James Holds Equifax Accountable by Securing $600 Million Payment in Largest Data Breach Settlement in History*, New York Attorney General Press Office (July 22, 2019), https://ag.ny.gov/press-release/attorney-general-james-holds-equifax-accountable-securing-600-million-payment-largest.

[4] *Id.*

[5] S.B. 5575, 242nd Leg. Sess. (N.Y. 2019) § 3(1)(c).

[6] *Id.*

[7] *Id.* at § 3(2).

[8] *Id.* § 4. The Act clarifies that small businesses—defined as businesses with fewer than fifty employees, less than $3 million in gross annual revenue during each of the last three fiscal years, or less than $5 million in year-end total assets, calculated in accordance with generally accepted accounting principles—are compliant so long as they implement "reasonable safeguards that are 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."

[9] *Id.* § 3(1)(b).

[10] *Id.* § 3(7). The Act also provides two carve-outs to the notice requirements, for circumstances in which: (1) the "exposure of private information was an inadvertent disclosure by persons authorized to access private information," and the person or business determines that "such exposure will not likely result in the misuse of such information," financial harm or emotional harm to the affected persons; or (2) where notice of the breach is made to affected persons pursuant to certain other New York laws and regulations. *Id.* § 3(2)(A) and (B).

[11] *Id.* § 3(6)(a).

[12] *Id.* In particular, the Act provides that in an enforcement action brought by the New York Attorney General, if the court determines that a "a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to twenty dollars per instance of failed notification, provided that the latter amount shall not exceed two hundred fifty thousand dollars."

[13] *See id.* § 4(IV)(C)(2)(D); N.Y. GEN. BUS. LAW § 350-d.

[14] *Id.* § 6.

[15] *See* https://www.paulweiss.com/media/3978767/12jul19-uk-ico-announcement.pdf.

[16] *Governor Cuomo Signs Legislation Protecting New Yorkers Against Data Security Breaches*, Governor's Press Office (July 25, 2019), https://www.governor.ny.gov/news/governor-cuomo-signs-legislation-protecting-new-yorkers-against-data-security-breaches.