Lowenstein Sandler

Client Alert

Privacy & Cybersecurity

June 20, 2019

New York on Verge of Passing Landmark Data Security Legislation

By Mary J. Hildebrand CIPP/US/E and Kathleen A. McGee

What You Need To Know:

- **If signed into law, New York's SHIELD Act will broaden the definition of protected information to include biometric data, email addresses, and corresponding passwords or security questions and answers.**
- **Unauthorized access, and not just unauthorized acquisition, to protected information would trigger breach notification requirements.**
- **Entities complying with other federal or New York state data security regulations would meet the Act's *de facto* reasonableness standard.**

Bill Amends Existing Law to Expand Consumer Rights and Enhance Cybersecurity

On June 17, 2019, the New York Legislature approved a substantial revision of New York state's data security and breach notification requirements under the Stop Hacks and Improve Electronic Data Security (SHIELD) Act. The bill now awaits Governor Cuomo's signature and, if signed, will substantially impact efforts by public and private organizations to contend with breach incidents and comply with data security requirements across industries.

The SHIELD Act (the "Act") would apply to any person or entity that processes the personal information of a New York state resident, even if such person or entity is located outside of the state. Given the size, population, and extensive business and financial influence of New York state, the Act will have national impact. With the Act, New York joins a growing list of activist states that are enacting new laws to address privacy and cybersecurity concerns.

Data Breach Implications

The Act would amend New York's data breach law (GBL §899-AA and §899-bb) in several key areas. Specifically, the Act broadens the definition of "private information" to include biometric data, account numbers, username/email address with password or security question and answer, and unsecured "protected health information" under HIPAA. The SHIELD Act expands the definition of "data breach" to include unauthorized *access* to private information instead of the current standard of unauthorized *acquisition*. Additionally, as referenced above, the Act applies outside of its geographic boundaries. Taken together, these amendments raise the bar for companies that experience data breaches involving New York state residents by expanding their notification obligations.

There's also some good news for business. The Act provides that inadvertent disclosures by individuals authorized to access the private information do not trigger notification requirements if the exposure will not likely result in misuse or in financial or emotional harm to the affected individuals. This "harm threshold" may operate to exempt very minor breaches from the Act.

Cybersecurity

The Act notably applies a reasonableness standard for evaluating data security standards, and carves out as *de facto* reasonable those entities that can

demonstrate compliance with selected federal and state data security frameworks, including GLBA and HIPAA as well as other New York state data security regulations, such as the Department of Financial Services Cybersecurity Regulation. If, for example, a company meets the notification requirements of those frameworks, no further notification would be required under the Act, with the caveat that entities would still have to provide notice to New York authorities. As approved by the Legislature, the Act includes an interesting placeholder for future federal and New York state data security regulations, likely in anticipation of ongoing legislation at all levels. In a nod to small business, the Act defines "reasonable" data security in light of the size of the covered entity, and provides a suggested but not mandated road map for implementing safeguards.

Enforcement

The Act does not contain a private right of action, but does permit enforcement by the state Attorney General.

If signed, the Act would go into effect in two stages, with the new notification requirements (§ 899-aa) becoming effective 90 days after signature by the governor, and the "reasonableness" standard for data security (§ 899-bb) effective after 240 days. The bill must be signed before the end of the calendar year.

Steps to Take Now

- Ensure that you've covered the basics: Know what data you collect and process, all data sources, location of the data, what you do with the data and why, and any disclosures of data made to third parties.
- Update your Data Breach Plan to reflect the significant departures from current New York law implemented under the Act, including the expanded definition of personal/private information and making unauthorized access to such information a data breach with all its attendant obligations.
- Review your Cybersecurity Program, and make any necessary modifications to ensure that you meet the reasonableness standard, taking into account the size of your business and other factors set forth in the Act.

**During her tenure as Bureau Chief of the Bureau of Internet & Technology for the New York State Attorney General's Office, Kathleen A. McGee was the primary drafter of the SHIELD Act.*

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

MARY J. HILDEBRAND CIPP/US/E
Partner
Chair, Privacy & Cybersecurity
T: 973.597.6308
mhildebrand@lowenstein.com

KATHLEEN A. MCGEE
Counsel
The Tech Group, White Collar Criminal Defense
T: 646.414.6831
kmcgee@lowenstein.com

This Alert has been prepared by Lowenstein Sandler LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship. Lowenstein Sandler assumes no responsibility to update the Alert based upon events subsequent to the date of its publication, such as new legislation, regulations and judicial decisions. You should consult with counsel to determine applicable legal requirements in a specific fact situation. Attorney Advertising.

© 2019 Lowenstein Sandler LLP | One Lowenstein Drive, Roseland, NJ 07068 | +1 973.597.2500