Craig Stewart

Partner
303.295.8478
Denver
cstewart@hollandhart.com

Safe Harbor for Data Security: New York's Proposed Changes Could Be Followed by Other States

Publication — 11/07/2017

New York Attorney General Eric Schneiderman has endorsed the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)--an amendment to the state's data security statute that includes a safe-harbor provision insulating companies that obtain a data security certification from litigation by the state.

The legislation, introduced last week in the New York State Assembly, would require any company that handles a New York resident's private data to put in place certain administrative, technical, and physical safeguards. The administrative safeguards include:

- designating employees to coordinate a security program
- identifying internal and external risks
- assessing the sufficiency of safeguards to control risks
- training employees in security practices
- selecting capable service providers

The technical safeguards include:

- assessing risks in software and network design
- assessing risks in information processing, transmission, and storage
- detecting, preventing, and responding to incidents
- testing and monitoring systems, controls, and procedures

The physical safeguards include:

- assessing risks of information storage and disposal
- detecting, preventing, and responding to intrusions
- protecting against unauthorized access or use of private information
- reasonably disposing of private information after it is no longer needed

Importantly, the SHIELD Act also would create a safe harbor under which a "certified compliant entity" would be immune from state enforcement action for violation of the statute unless there is evidence of willful misconduct, bad faith, or gross negligence.

"Certified compliant entity" is defined as an entity that is subject to and in compliance with certain federal regulatory schemes (including the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act), New York's cybersecurity regulation for financial institutions, other

federal or New York data security rules or regulations, ISO Standard 27002, or NIST 800-53, and has that compliance certified annually by an independent, authorized third-party assessment organization. Companies that invest the time, money, and effort to achieve such certification would be rewarded with a safe harbor--removing the risks, costs, and uncertainty of enforcement litigation by the attorney general.

When it comes to cybersecurity, states tend to follow the leaders. California enacted the first data breach notification statute in 2003. Three years later, 33 other states had enacted such statutes, and this year New Mexico became the 48th state (Alabama and South Dakota are the holdouts). Illinois added to its data breach notification statute protection of biometric data such as fingerprints, retinas, irises, and facial geometry/recognition. Texas and most recently Washington have done the same. This year in March, New York enacted heightened cybersecurity regulations for financial institutions. Colorado followed in July with similar regulations for investment advisors and broker dealers. (See our prior alerts here and here.)

Businesses should stay informed about the emergence of comprehensive cybersecurity compliance requirements. Even if not technically applicable, these requirements serve as good starting points for reasonable cybersecurity practices.

For more information, please contact Craig Stewart (303.295.8478 / cstewart@hollandhart.com) and Romaine Marshall (801.799.5922 / rcmarshall@hollandhart.com).