



# Governor Cuomo Signs the Stop Hacks and Improve Electronic Data Security (SHIELD) Act and the Identity Theft Prevention and Mitigation Services Act into Law

## Publication:

Riker Danzig Cyber Security & Data Privacy Client Alert July 30, 2019

On Thursday, July 25, 2019, New York Governor Andrew Cuomo signed into law two bills that require businesses to implement more robust data security safeguards, expanded the definition of private information and help guarantee identity theft protections for victims of a breach at a credit reporting agency. New York now joins a number of states revamping their breach notification and data security laws and comes days after the Equifax Inc. settlement with the states and the FTC.

First, the Stop Hacks and Improve Electronic Data Security Act (the "SHIELD Act") amends N.Y. Gen. Bus. Law § 899-aa by expanding the definition of private information to include the following new categories: i) account numbers and credit or debit card numbers without a security code, provided the number could be used to access an individual's financial account; ii) biometric information (including a fingerprint or retina image); and iii) usernames or email addresses together with passwords, or security questions and answers that could permit access to an online account. Additionally, it expands the definition of a breach to include the unauthorized access to private information in addition to unauthorized acquisition of private information. Access can include viewing, copying or downloading private information without valid authorization or by an unauthorized person. Businesses that collect private information will have to maintain "reasonable" data security and implement "reasonable" administrative safeguards. Under the SHIELD Act, businesses are exempt from issuing breach notifications when: i) "the exposure of private information was an inadvertent disclosure by persons authorized to access the private information and the person or business reasonably determines such exposure will not likely result in misuse of such information"

sufficient to pose any financial or emotional harm; and ii) if the business has already sent out data breach notifications as required under other federal or New York law (including GLBA, HIPAA and NYDFS). Furthermore, the SHIELD Act amends N.Y. Gen. Bus. Law § 899-aa to limit the time under which the New York Attorney General may bring action against violators from three (3) years to two (2) years. The SHIELD Act will take effect 240 days after it was signed into law, on March 21, 2020.

Second, the Identity Theft Prevention and Mitigation Services Act amends N.Y. Gen. Bus. Law § 380-t to require credit reporting agencies to provide five (5) years of identity theft prevention and mitigation services and to provide information on credit freezes to victims of a data breach at a credit reporting agency. The Identity Theft Prevention and Mitigation Services Act will take effect 60 days after it was signed into law, on September 23, 2019.

These privacy law updates apply to any person or entity with access to private information of a New York state resident, regardless of whether they conduct business in the state. Companies impacted by these amendments should consider the potential impact on their current policies and procedures. Additionally, companies should ensure that their information security programs comply with the SHIELD Act's required data security safeguards. A copy of the SHIELD Act can be found [here](#) and a copy of the Identity Theft Prevention and Mitigation Services Act can be found [here](#). If you have any questions, please contact one of this Alert's authors: Michael P. O'Mullan at [momullan@riker.com](mailto:momullan@riker.com), Labinot Alexander Berljajolli at [lberljajolli@riker.com](mailto:lberljajolli@riker.com) or Daniel J. Parziale at [dparziale@riker.com](mailto:dparziale@riker.com), or any other attorney in Riker Danzig's Cyber Security & Data Privacy practice.

Riker Danzig's [Cyber Security & Data Privacy](#) Partners:

[Brian E. O'Donnell](#)

[Michael P. O'Mullan](#)

[Maura C. Smith](#)

[Samuel P. Moulthrop](#)

[Robert J. Schoenberg](#)

[Lance J. Kalik](#)

[Jason D. Navarino](#)

[Anthony J. Zarillo, Jr.](#)

## **Attorneys:**

[Brian E. O'Donnell](#) · [Michael P. O'Mullan](#) · [Maura C. Smith](#) · [Samuel P. Moulthrop](#) · [Robert J. Schoenberg](#) · [Lance J. Kalik](#) · [Jason D. Navarino](#) · [Anthony J. Zarillo, Jr.](#) · [Labinot Alexander Berljajolli](#) · [Daniel J. Parziale](#)

## Practice:

Cyber Security & Data Privacy

Headquarters Plaza, One Speedwell Avenue, Morristown, New Jersey 07962-1981 • t: 973.538.0800 f: 973.538.1984

50 West State Street, Suite 1010, Trenton, New Jersey 08608-1220 • t: 609.396.2121 f: 609.396.4578

500 Fifth Avenue, New York, New York 10110 • t: 212.302.6574 f: 212.302.6628

399 Knollwood Road, Suite 201, White Plains, NY 10603 • t: 914.539.3360 f: 914.539.3361

1200 Summer Street, Suite 201C, Stamford, CT 06905 • t: 203.326.6740 f: 914.539.3361

[www.riker.com](http://www.riker.com)