VORYS

Publications

Client Alert: New York State Greatly Expands Data Protections for Consumers

Related Attorneys

John L. Landolfi

Christopher L. Ingram

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 7.26.2019

Governor Cuomo signed the Stop Hacks and Improve Electronic Data Act (SHIELD) on July 25, 2019, providing stronger protections for New Yorkers by imposing strict cybersecurity requirements on all companies, broadening the Attorney General's oversight over data breaches, and expanding data breach notification requirements. The SHIELD Act will go into effect in 240 days after becoming law.

The SHIELD Act lowers the threshold for when entities must provide notification of a breach. Now, entities must provide notification where "unauthorized access" of private information has taken place. This change replaces the previous threshold of unauthorized "acquisition" of the information. What information constitutes "private information" subject to mandatory reporting duties has also expanded and now includes:

- Biometric data;
- Protected health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA);
- Financial account numbers that can be used to access a financial account (even without a security code or PIN); and
- Username or e-mail address in combination with a password or security question and an answer that permits access to an online account.

Consumer notification of the unauthorized access is not required if the data exposure was inadvertent, and the business determines that misuse of such information, or financial or emotional harm to the affected individuals, is unlikely. That determination, however, must be documented in writing, and the business must notify the determination to the Attorney General within ten (10) days of making the decision.

Under the SHIELD Act, all persons or businesses that own or license the private information of a New York resident must comply with obligations to maintain "reasonable security safeguards to protect the

security, confidentiality, and integrity of private information." Except for certain entities (such as those subject to federal financial or health authorities), a business is deemed compliant with the SHIELD Act's security requirements when it creates the following administrative, technical, and physical safeguards:

Administrative Safeguards:

- Have employee(s) designated to coordinate the security program;
- Identify reasonably foreseeable internal and external risks;
- Assess safeguards to control identified risks;
- Train and manage employees in the security program;
- Contractually require service providers to be capable of maintaining appropriate safeguards; and
- Adjust the security program to reflect business changes.

Technical Safeguards:

- Assess the risks of the network and the software design;
- Assess the risks in information processing, transmission, and storage;
- Detect, prevent, and respond to attacks or system failures; and
- Test and monitor the effectiveness of key controls, systems, and procedures regularly.

Physical Safeguards:

- Assess the risk of information storage and disposal of same;
- Detect, prevent, and respond to intrusions;
- Protect against unauthorized access to, or use of PI during or after, the collection, transportation, and destruction or disposal of said information; and
- Properly dispose of PI within a reasonable amount of time after it is no longer needed for business purposes.

Companies should update their incident response plans to incorporate the expanded definition of private information and provide a procedure to document inadvertent exposure. Companies should also review their safeguards to determine whether they satisfy the substantive safety requirements. For assistance with compliance questions, policy review, or incident response preparation, please contact John Landolfi, Christopher Ingram, Sarah Boudouris, or your Vorys attorney.