NEW YORK SHIELD ACT – EFFECTIVE MARCH 21, 2020

This is being provided for informational purposes only, and not as legal advice. As the employer or user of consumer reports, it is your responsibility to ensure compliance with all of the relevant federal, state and local laws governing this area, including, but not limited to, the FCRA. We strongly recommend that prior to use, you consult with your own attorney.

In July of 2019, New York Governor Andrew Cuomo signed into law, the Stop Hacks and Improve Electronic Data Security Act (the "SHIELD Act"), https://www.nysenate.gov/legislation/bills/2019/s5575, which amended New York's data breach notification law to broaden notification obligations and impose new data security requirements on companies to secure private information. The breach notification provisions took effect in October 2019; the heightened data security requirements take effect on March 21, 2020.

While New York previously adopted the New York Department of Financial Services ("NYDFS") Cybersecurity Regulations effective March 1, 2017, which established heightened security requirements for covered financial entities, the SHIELD Act more broadly covers all businesses that store information of New York residents, regardless of industry.

Summary of SHIELD Act

The SHIELD Act expanded New York's data security law primarily as follows:

- Heightened the data security requirements that must be adopted;
- Broadened what constitutes a "breach" to include unauthorized access, rather than only the unauthorized acquisition of computerized data; and
- Broadened notice requirements, including requiring notice to the New York Attorney General, of breaches involving entities that are regulated by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") or the Health Information Technology for Economic and Clinical Health ("HITECH") Act.

Security Requirements Needed by March 21, 2020

The SHIELD Act requires businesses to implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of private information,[1] the definition of which has been expanded under the SHIELD Act. Entities that are subject to and in compliance with laws like HIPAA, the Gramm-Leach-Bliley Act ("GLBA"), or the NYDFS Cybersecurity Regulations, are deemed to be compliant with SHIELD Act requirements. All other businesses must implement a data security program that includes reasonable administrative, physical and technical safeguards, such as the safeguards set out below, unless the business qualifies as a "small business."[2] GBLA § 899-bb(2)(b)(ii)(a)-(c).

Reasonable *Administrative* Safeguards

- Designate an employee who coordinates the security program;
- Perform assessments that identify reasonably foreseeable external and internal risks;
- Assess the sufficiency of safeguards in place to control identified risks;
- Provide reasonable training and management of employees in the security program practices and procedures;

- Establish procedures to select service providers capable of maintaining appropriate safeguards, and require that the service providers implement those safeguards by contract; and

- Ensure procedures adjust to reflect business changes and new circumstances.

Reasonable *Technical* Safeguards

- Assess risks in network and software design;

- Assess risks in information processing, transmission and storage;

- Detect, prevent and respond to attacks or system failures; and

- Regularly test and monitor the effectiveness of key controls, systems and procedures.

Reasonable *Physical* Safeguards

- Assess risks of information storage and disposal;

- Detect, prevent and respond to intrusions;

- Protect against unauthorized access to, or use of, private information during or after the collection, transportation and destruction or disposal of the information; and

- Properly delete private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

While small businesses are not exempt from the SHIELD Act, they are not held to the same standards as larger businesses for safeguards with respect to what constitutes a reasonable security program. Rather, small businesses must have reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of its activities, and the sensitivity of the personal information collected. GBLA § 899-bb(2)(c).

While the SHIELD Act does not create a private right of action (GBLA § 899-bb(2)(e)), it makes any violation of the data security requirements a violation of GBLA § 349, which prohibits deceptive acts and practices in the conduct of any business. These violations are enforceable by the New York Attorney General, with civil penalties of $5,000 per violation. GBLA § 350-d.

Current Breach Notification Requirements

The breach notification requirement is triggered by a breach of “private information.” Private information is defined as *personal information* in combination with any one or more *enumerated data elements* that are not encrypted, or were encrypted with an encryption key but where the key was accessed or acquired. Further, what constitutes a breach under New York law was expanded by the SHIELD Act.

As amended, a breach occurs when there is unauthorized access or unauthorized acquisition of computerized private information. By enlarging the law’s scope to include “access,” triggering events that require notice to both the individuals affected and the New York Attorney General potentially include instances where an unauthorized actor only *viewed* private information.

Additionally, it is important to note that an entity subject to the HIPAA / HITECH 60-day notification requirement must also provide such notification to the New York Attorney General within five (5) business days of making the HIPAA disclosure. GBLA § 899-bb(9).

Key Points

On or before the effective date of the SHIELD Act's security requirements, businesses should:

- Assess their current safeguards for compliance with the SHIELD Act's data security program requirements;
- Assess vendor relationships and vendor contracting practices to ensure contracts require that vendors maintain appropriate safeguards;
- Comply with the SHIELD Act's expanded data breach notification obligations, including with respect to entities subject to HIPAA, which must notify the New York Attorney General of any data breach affecting New York residents within five (5) business days of notifying the U.S. Department of Health and Human Services; and
- Keep in mind the expanded legal requirements when electing to use New York governing law in contracts. In particular, businesses may find that New York's heightened obligation with respect to security safeguards exceeds their own state's security requirements.

Footnotes

[1] "Private information" shall mean either: (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired: (1) Social Security number; (2) driver's license number or non-driver identification card number; (3) account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account; (4) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or (5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or (ii) a user name or email address in combination with a password or security question and answer that would permit access to an online account. "Personal information" is a defined term and means any information concerning a natural person that, because of name, number, personal mark, or other identifier, can be used to identify such natural person. GBLA § 899-aa(1)(a).

[2] "Small business" is defined as any person or business with (i) fewer than 50 employees; (ii) less than $3 million in gross annual revenue in each of the last three fiscal years; or (iii) less than $5 million in year-end total assets, calculated in accordance with generally accepted accounting principles. GBLA § 899-bb(1)(c).