Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY

AUGUST 6, 2019

New York Enacts Sweeping New Cybersecurity Mandates For Businesses

On July 25, 2019, Governor Cuomo signed the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) into law. The SHIELD Act establishes new minimum security requirements for all persons and entities, both for-profit and not-for-profit (Business or Businesses) that hold computerized private information and are not already covered by other federal or state cybersecurity mandates. Effective on March 21, 2020, these new cybersecurity mandates require Businesses within and outside the State to assess their cybersecurity programs for compliance with the SHIELD Act.

The SHIELD Act also significantly expands the information covered and the reach of New York's breach notification act beyond entities that conduct business in the State to all persons and businesses that possess computerized information about New York State residents. This Memorandum focuses on the significant changes in cybersecurity requirements adopted in the SHIELD Act. A second memorandum addresses the breach notification provisions.

New Statute Created Under SHIELD Act

The SHIELD Act puts in place, for the first time in New York State, standards for cybersecurity safeguards that generally apply to all persons and Businesses possessing private computerized information about New York residents. Specifically, the SHIELD Act creates Gen. Bus. Law § 899-bb which provides that any person or Business that licenses or owns private computerized data that includes certain information[1] about a New York State resident (Private Information) shall "develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the privacy information, including disposal of data." The SHIELD Act sets forth specific cybersecurity program elements that will be deemed compliant with the Act.

Both New York and the federal government have long imposed industry specific cybersecurity regulations, such as New York's Department of Financial Services regulations (DFS Cybersecurity Rule) and the Federal Graham-Leach-Bliley Act (GLBA), applicable to banks, financial institutions and insurance companies, and the Health Insurance Portability and Accountability Act (HIPAA) which applies to health care providers and plans. The SHIELD Act is far broader in its application. New York now regulates all persons and Businesses at any location possessing Private Information about New York residents. Entities regulated by another federal or state cybersecurity law or regulation can comply with the SHIELD Act by complying with those other applicable cybersecurity requirements. Persons and Businesses not bound by other cybersecurity laws or regulations must implement what the SHIELD Act calls reasonable, administrative, technical and physical safeguards. Failure to do so is a violation of Gen. Bus. Law § 349 and can expose Businesses to a lawsuit by the Attorney General and penalties under Gen. Bus. Law § 350-d.

Consistent with the prevailing framework for security safeguards, the SHIELD Act specifies safeguards in each of three categories: administrative, technical and physical. In each category, the SHIELD Act lists "reasonable" safeguards identified as "such as," suggesting that while each safeguard is not specifically mandated, each will be considered in evaluating compliance with the SHIELD Act and that, taken together, the designated safeguards may not be sufficient. Persons and Businesses will be held to a standard of reasonableness that will depend on a host of factors, including the size and resources of the entity as well as the sensitivity of the Private Information that they collect, use and retain.

1 Information covered by the SHIELD Act is defined to include social security numbers, driver's license number, or non-driver identification card number, account number, credit card or debit card number with or without additional access codes or other information, biometric data, and user names or email addresses in combination with a password or security question that would allow access to a person's online account.

Administrative Safeguards

Persons and Businesses possessing Private Information must now implement reasonable administrative safeguards, as listed in the SHIELD Act:

- Designation of one or more employees to coordinate the Businesses' security program;
- Identification of internal and external security risks;
- Assessment of the sufficiency of safeguards in place to control identified risks;
- Training and management of employees in the security program practices and procedures;
- Selection of service providers capable of maintaining appropriate safeguards, and requiring those safeguards by contract; and
- Adjustment of the security program to address business changes and new circumstances.

Reasonable Technical Safeguards

Newly imposed technical safeguards specified in the SHIELD Act are:

- Assessment of risk in network and software design;
- Assessment of information processing, transmission and storage risk;
- Detection, prevention and response to attacks and system failures; and
- Regular testing and monitoring the effectiveness of key controls, systems and procedures.

Reasonable Physical Safeguards

The following physical safeguards are listed in the SHIELD Act:

- Assessment of risks of information storage and disposal;
- Detection, prevention and response to physical intrusions;
- Protection against unauthorized access to or use of private information during and after its collection, transportation and destruction or disposal; and
- Disposal of Private Information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that information cannot be read or reconstructed.

Scaling the Requirements for Small Businesses

Cognizant of the strain the new cybersecurity requirements could place on small businesses, the Legislature provided a more general cybersecurity standard for small businesses defined as companies with: (i) fewer than fifty employees; (ii) less than $3 million in gross annual revenue in the last three fiscal years; or (iii) less than $5 million in year-end total assets, calculated using GAAP. Businesses that meet this definition can comply with the SHIELD Act by establishing administrative, technical and physical safeguards appropriate for the size and complexity of each Business, taking into account the nature and scope of the small Business' activities and the sensitivity of Personal Information the small Business collects about consumers.

What is Reasonable? Only Time Will Tell

The SHIELD Act's requirements, referencing "such as", provide some flexibility but also underscore that compliance with the security elements enumerated in the Act may not be sufficient for all Businesses. Clarification about what the Attorney General considers "reasonable," and what courts will require of Businesses and persons possessing Private

Information, will only occur once the Attorney General brings enforcement actions or as judicial decisions emerge that interpret the statute. Enforcement actions by other regulatory bodies, including the Federal Trade Commission and the United States Department of Health and Human Services, however, provide a record of increasing penalties and fines for actions ranging from the failure to enter into third party agreements to protect private information to the failure to take reasonable measures to detect and eliminate the source of a security breach. Notably, recent court decisions in New York and Pennsylvania reflect the courts' willingness to hold employers accountable for security lapses that allowed the breach of data for thousands of employees. In a 2017 New York United States District court case, the court held that employees could pursue a class action suit under New York Labor Law § 203-d against their employer for failure to take reasonable precautions to prevent a breach.[2]

Concrete Steps Towards Compliance

The SHIELD Act was adopted in response to heighted cybersecurity attacks across industries in New York and other states, and major breaches that have disclosed the personal information of millions of individuals. The Act fills a gap by imposing obligations for a cybersecurity program on all entities in the State not already governed by another cybersecurity regulatory framework. Businesses and not-for-profit organizations not bound by other cybersecurity requirements are advised to conduct a risk assessment to identify the sensitive information the organization receives, generates and stores, and weaknesses in their security safeguards. Organizations should keep in mind that the specific safeguards identified in the SHIELD Act are a good baseline for the assessment, but not necessarily sufficient. Businesses in other states that possess Private Information about New York residents should determine whether compliance with regulatory schemes in their home state satisfies New York's new requirements or whether they already comply with the SHIELD Act by meeting the demands of other cybersecurity laws or regulations.

If you have any questions about the SHIELD Act, contact Tracy E. Miller, Co-Chair of the Cybersecurity and Data Privacy Practice, Curtis A. Johnson, a member of the Practice Group, or the attorney in the Firm with whom you are regularly in contact.

2 *Sackin v. Transperfect*, 278 F.Supp 3d 739 (S.D.N.Y. 2017).

BOND SCHOENECK & KING ATTORNEYS