New York SHIELD Act Now Requires Your Compliance

The deadline to implement state mandated minimum cybersecurity requirements has arrived. Last July, Governor Cuomo signed the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) into law. The SHIELD Act, codified at Gen. Bus. Law § 899-bb, establishes new minimum security requirements for all persons and entities, both for-profit and not-for-profit businesses that hold protected computerized information. Compliance is required as of March 21, 2020.

New York State has not delayed implementation in the face of the statewide and national emergencies declared as a result of the COVID-19 pandemic.

Protected Data

The SHIELD Act is meant to protect the following private data concerning New Yorkers:

- Unencrypted copies of:
  - Social security numbers
  - Driver's license numbers or non-driver identification card numbers
  - Account numbers, credit or debit card numbers, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account
  - Account numbers, credit or debit card numbers, 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
  - 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
  - User names or e-mail addresses in combination with passwords or security questions and answers that would permit access to an online account

Cybersecurity Program Requirements

Businesses in possession of such data, be it customer data or employee data, must take steps to ensure it is physically and technologically secure and disposed of in a reasonable amount of time and in a safe manner. They must further enact a written cybersecurity program that addresses the following areas:

- Administrative Safeguards
  - Designating one or more employee responsible for the cybersecurity program
  - Identifying foreseeable internal and external risks
  - Assessing existing safeguards to address identified risks
  - Training and managing employees on practices and procedures to address risk
  - Selecting service providers capable of maintaining appropriate safeguards (and requires those safeguards to be in place in a contract)
  - Adjusting the cybersecurity program to reflect business changes

- Technical Safeguards
  - Assessing risk in network and software design
  - Assessing risk in information processing, transmission and storage
  - Detecting, preventing and responding to attacks and system failures
  - Regularly testing and monitoring effectiveness of key controls
- Physical Safeguards
  - Assessing risk of information storage and disposal
  - Detecting, preventing and responding to intrusions
  - Protecting against unauthorized access to or use of private information during collection, transportation and destruction or disposal of information
  - Disposing of private information within a reasonable amount of time, and erasing electronic media so it cannot be read or reconstructed

Small Businesses

Small businesses, those with fewer than fifty employees; less than three million dollars in gross annual revenue in each of the last three fiscal years; or less than five million dollars in year-end total assets, calculated in accordance with GAAP, are considered compliant if they take reasonable steps, similar to those outlined above, consistent with the nature and scope of business operations and the sensitivity of data collected from or about consumers.

Compliance with Other Cybersecurity Regulations

Entities that are compliant with HIPAA, Graham-Leach-Bliley Act, or New York Department of Financial Services cybersecurity regulations are deemed compliant with the SHIELD Act. However, Bond recommends that all such businesses assess their compliance with those other regulations to ensure that policies and procedures put in place are also separately SHIELD Act compliant.

Risks of Noncompliance

The SHIELD Act does not contain a reporting requirement such that businesses must certify their compliance with a governmental entity. However, the New York Attorney General has the power to enforce the SHIELD Act upon its discovery that an entity is not compliant, including through the assessment of civil penalties. The Attorney General is most likely to discover non-compliance when an entity suffers a reportable data breach, which breach must be reported to the Attorney General and other state entities.

If you have any questions about this memo, please contact any of the attorneys in the Cybersecurity and Data Privacy Practice Group, or the attorney in the firm with whom you are regularly in contact.

BOND SCHOENECK & KING ATTORNEYS