corsica technologies

NEW YORK SHIELD ACT CHEAT SHEET

What is it?

On March 21, 2020 the state of New York enacted the "**S**top **H**acks and **I**mprove **E**lectronic **D**ata Security Act" (SHIELD Act) which broadens and strengthens the state's data breach notification requirements and requires businesses covered by this act to have reasonable data security safeguards. The Act applies to any person or business, even those outside of the state, that own or license computerized data that includes "private information" of a New York resident.

What does this mean?

The SHIELD Act is similar, in many regards, to HIPAA for healthcare providers or Graham-Leach-Bliley (GLBA) for financial institutions. It is an attempt to enforce a standard, in the absence of them, on every business, not just regulated/compliance ones, to safeguard the private data of New York residents.

What is considered personal or private information?

As with some of the other regulatory standards, personal information consists of the things that you would expect. Included are social security numbers, driver's license number, account numbers, credit or debit card numbers, passwords, biometric information and other data that may be considered private. Information that is not included would be data that is publicly available or made lawfully available for federal, state, or local government records.

Why are they doing this?

While regulations like HIPAA and GLBA protect data in those institutions, there have not been broad applications of data security across all businesses. Like GDPR in Europe, the SHIELD Act creates a standard, based on reasonable measures, that all businesses must meet to protect the residents of New York.

Is this hard to accomplish?

This is not really a new set of standards, but an adoption of existing standards from other areas. To comply with the SHIELD Act, an entity must have a compliant data security program under GLBA, HIPAA/HITECH, New York DFS cyber regulations or other applicable Federal cybersecurity regulations. Or, compliance can be achieved by having a data security program with "reasonable" administrative, technical, and physical safeguards.

Who decides what is "reasonable"?

The standard lays out three areas where reasonable safeguards should be employed to meet the standard. They are:

- Reasonable administrative safeguards- this requires that the company designate someone to coordinate all the security measures.They should identify risks, determine if the safeguards effectively mitigate that risk, train other employees in the security practices and procedures, select vendors that can maintain appropriate safeguards, requiring those in the contract, and having a process of continual improvement for the safeguards.
- Reasonable technical safeguards- this requires the entity to assess risk in their technology environment, monitor their systems for attacks or failures, and regularly test the effectiveness of the safeguards.
- Reasonable physical safeguards- this requires the entity to assess risks relating to information storage and disposal, protecting against unauthorized access, disposing of information in a timely fashion, and detecting and responding to intrusions.

I'm a small business, I don't have to do all that do I?

Small businesses are NOT exempt from implementing data security safeguards, but the safeguards only need to be "appropriate for the size and complexity of the small business, that nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers." The SHIELD Act defines a small business as any person or business with-

- Fewer than 50 employees
- Less than three million dollars in gross annual revenue in each of the last three years
- Less than five million dollars in year-end total assets, calculated in accordance with GAAP.

If you are a small business and your customer interactions are largely transactional, compliance should be relatively easy. If you are a small business, but you maintain significant records about your customers and they are New York residents, compliance will be more complicated.

Is that all?

Not quite! The statute also contained amendments that expanded the breach notification rules that were already on the books. The amendments went into effect in October of 2019. If there is a breach that exposes private information under the SHIELD Act there are requirements for notification and could carry a fine. If notification is required, it must be made "in the most expedient time possible and without unreasonable delay."

So, what should I do?

First, you should do an audit of your current environment to determine what data you have that would meet the standard of "private information of a New York resident." Then, you would need to determine the best approach to achieve compliance. Should you attempt to adhere to an existing standard that achieves compliance or pursue the reasonable safeguards approach? Then, you would begin to enact an action plan for compliance.