akerman

Practice Update

Getting Ready for New York's SHIELD Act

August 14, 2019
By Christy S. Hawkins

Recently, New York enacted the SHIELD (Stop Hacks and Improve Electronic Data Security) Act. The SHIELD Act becomes effective on March 21, 2020. This Practice Update provides a quick overview of:

- When the SHIELD Act applies,
- What violating the SHIELD Act may cost,
- What the SHIELD Act requires, and
- How to prepare for its March 21, 2020 effective date.

When Does the SHIELD Act Apply?
The SHIELD Act applies to ANY person or business that owns or licenses computerized data including a New York resident's private information. The SHIELD Act expands New York law, extending protection of New York residents data—even when the person or business does not do business in New York.

Protected New York resident private information includes the following:

- A user name or email address in combination with a password or security question and answer that would permit access to an online account; or
- A person's name or other information that can be used to identify a specific person, in combination with any of the following:

Related People

Christy S. Hawkins

Related Work

Healthcare
Litigation

Related Offices

Dallas

- Social Security number;
- Driver's license number or non-driver identification card number;
- Account number, credit or debit card number, in combination with any required security code, access code, password, or other information which would permit access to an individual's financial account;
- Account number, or credit or debit card number, if the number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or
- Biometric information, specifically data generated by electronic measurements of an individual's unique physical characteristics, including fingerprint, voiceprint, or retina or iris image, or other unique physical representation or digital representations used to authenticate or ascertain the individual's identity.

What Does Violating the SHIELD Act Cost?
The cost for violating the SHIELD Act is unclear. If an operation fails to have "reasonable" administrative, technical, and physical safeguards to protect and securely dispose of New York residents' private information, the New York Attorney General may prosecute the offending conduct as an unfair business practice, and may seek an injunction.

If an operation fails to comply with the SHIELD Act's breach notification requirements, the New York Attorney General may impose a civil penalty of the greater of (a) $5,000 or (b) $20 per instance of failed notification, not to exceed $250,000.

The SHIELD Act does not specify what counts as an "instance" of failed notification. For example, is an "instance" of failed notification all of the letters issued for a single incident, or is each notification letter issued to a New York resident an "instance", or

is it something else? Without any legal precedent interpreting the SHIELD Act, the cost of violating this law is not clear.

What Does the SHIELD Act Require?
The SHIELD Act requires breach notification to impacted New York residents' whose personal information has been accessed without authorization. Notice also must be provided to certain regulators. Acquisition of protected personal information is not required. The SHIELD Act also updates the required content of breach notice communications.

Most significantly, the SHIELD Act requires "reasonable" safeguards to protect New York residents' private information. Specifically, the SHIELD Act requires any person or business holding a New York resident's private information to develop, implement, and maintain "reasonable" administrative, technical, and physical safeguards to protect and securely dispose of New York residents' private information.

How to Comply with the SHIELD Act Before its March 21, 2020 Effective Date
The most important step to take to comply with the SHIELD Act is to make certain that your organization can show that it has "reasonable" safeguards to protect private information. It sounds simple, but the SHIELD Act's requirement for "reasonable" safeguards creates many questions that are not answered by the wording of the law. For example:

- What safeguards are "reasonable?"
- What specific administrative, technical, and physical safeguards are required?
- How should we determine what we must do to comply?

The short answer to these questions: it depends. A variety of factors impact the technical and legal analysis needed to show that specific safeguards are

"reasonable," including the size and scope of the operation, the technical and practical requirements of the involved computer systems, and the kinds and volume of New York residents' private information that require protection.

There are many options for efficiently preparing to comply with the SHIELD Act before March 21, 2020. The options have differing costs and risks, and they present different opportunities.

To get started, describe your administrative, technical, and physical safeguards to protect and securely dispose of information about people. Are they reasonable? How will you be able to convince someone that your safeguards are reasonable—especially after a data breach or other incident happens? Having defended breached organizations since California enacted the first breach notification law in 2003, Akerman is positioned to offer guidance.

While you are preparing to comply with the SHIELD Act, also consider other laws, regulations, and contractual data and privacy protection requirements that may apply. Working toward compliance with the all of your relevant data privacy and security regulations and contract terms tends to be more cost-effective and prudent than addressing one regulation at a time.

Frequently, contracts include data security and privacy requirements—especially when a contracting party has operations outside of the United States as many other countries' laws effectively require data protection contracting terms. Data and privacy protection laws apply based on the residency of each individual whose private information you hold. To determine which jursidictions' laws apply to your organization, start by determining the residency of the individuals whose private information your organization holds.

In the United States, each of the 50 States has its own data security and privacy laws. In addition to state laws, a variety of federal regulations also may apply. For example:

- Healthcare information is subject to HIPAA (Health Insurance Portability and Accountability Act) and HITECH (Health Information Technology for Economic and Clinical Health Act).
- Financial information is subject to the Gramm-Leach-Bliley Act (GLBA).
- Section 5 of the Federal Trade Commission (FTC) Act prohibits unfair methods of competition, so the FTC addresses complaints of misleading communications to consumers, including communications about data collection and protection.

Many countries have data privacy and protection laws. For example:

- Personal information concerning residents of countries in the European Union (EU) and the European Economic Area (EEA) is subject to the General Data Protection Regulation (GDPR) which carries fines of up to the greater of €20 million (approximately $22,398,925) or 4 percent of the prior year's global turnover (similar to gross revenue).
- Brazil has enacted its Lei Geral de Protecao de Dados (LGPD) which takes effect in February 2020 and carries fines of up to 50 million BRL (approximately $12,719,500).
- Japan's Act on Protection of Personal Information has strict guidelines and may result in criminal prosecution.
- Thailand's Personal Data Protection Act takes effect on May 27, 2020 and also may result in criminal prosecution.

Adding our expertise to yours, Akerman can help companies position their operations to more safely

gain the benefits of emerging technologies in a world that is disrupted by digital transformation.

Please contact Akerman's Privacy, Cybersecurity and Emerging Technologies Team with any questions about New York's SHIELD Act or other developments in this continuously changing area of the law.

This Akerman Practice Update is intended to inform firm clients and friends about legal developments, including recent decisions of various courts and administrative bodies. Nothing in this Practice Update should be construed as legal advice or a legal opinion, and readers should not act upon the information contained in this Practice Update without seeking the advice of legal counsel. Prior results do not guarantee a similar outcome.