Schulte Roth&Zabel

Alert

Data Security: Update for Private Fund Managers — NY SHIELD Act

March 18, 2020

Numerous data protection laws call for "reasonable" or "adequate" security controls, but are not specific about what those terms mean. New York's Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act"),[1] **the data security requirements of which become effective March 21, 2020**, stands out among data protection laws because it provides specific safeguards that should be taken as part of a "reasonable" information security program.[2]

What Is the SHIELD Act?

The SHIELD Act is a data security law that takes effect on March 21, 2020, and requires businesses that own or license electronic "private information"[3] of a New York resident, regardless of where that business is located or conducts business, to meet specific data security requirements.[4]

Most Private Fund Managers Are Not Covered by the SHIELD Act's Data Security Requirements

The SHIELD Act's data security requirements exempt businesses that are subject to, and maintain data security programs that are in compliance with, the Privacy Rule of the Gramm-Leach-Bliley Act ("GLBA").[5] This means that *most private fund managers will not be required to comply with these requirements of the SHIELD Act*.[6]

---

[1] Stop Hacks and Improve Electronic Data Security Act, N.Y. Gen Bus. Law §§ 899-aa & 899-bb.

[2] The SHIELD Act also amends New York's breach notification law, effective Oct. 23, 2019, to expand the scope of information and the persons and businesses covered by the existing law. *Id.* § 899-a

[3] The definition of "private information" was expanded under the SHIELD Act to mean either (i) any unencrypted (or encrypted with a key that has been accessed) information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person in combination with any one or more of the following data elements: (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 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 information); or (5) biometric information; or (ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

[4] The reach of the data security requirements of the SHIELD Act are broader than New York's prior cybersecurity regulations, the New York Department of Financial Services Cybersecurity Regulations, 23 NYCRR Part 500, both in the expanded definition of what type of information is covered and in reaching companies whose only connection to New York is that they have private information of New York residents.

[5] Privacy of Consumer Financial Information Rule, 16 C.F.R. Part 313 ("Privacy Rule").

[6] Most fund managers are subject to the Privacy Rule, as financial institutions that collect "nonpublic personal information" about natural persons to provide a financial product or service. Fund managers that are not subject to, or are uncertain whether they are subject to the Privacy Rule, will want to consult legal counsel to determine what requirements they may have under the data security requirements of the SHIELD Act.

Fund managers do, however, remain subject to New York's breach notification requirements, as amended by the SHIELD Act.[7] Managers who experience a cybersecurity incident will want to consult these updated requirements.

The SHIELD Act Still Provides Useful Guidance for Exempted Fund Managers

While most private fund managers will be exempted from the data security requirements of the SHIELD Act, it can serve as a helpful point of reference for what a regulator would view as "reasonable" safeguards under federal or other state laws.

The Elusive "Reasonable" Standard in Data Security

Several existing data security regulations call on those private fund managers to develop and implement "reasonable" or "appropriate" security procedures and practices, but provide no guidance as to what that means. For example, the California Consumer Privacy Act ("CCPA") creates a private right of action for consumers whose personal information has been subject to unauthorized access or disclosure as a result of the covered business' failure to maintain reasonable security procedures. The CCPA, however, does not define "reasonable security procedures."[8] Similarly, the European Union's General Data Protection Regulation ("GDPR") requires a level of security that is "appropriate" to the risks presented by processing, but does not specify the security measures that should be in place.

The SHIELD Act requires covered businesses to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity" of private information. A business that implements "reasonable" administrative, technical and physical security measures will be deemed to be in compliance with the statute.[9] Unlike other statutes and regulatory guidance, however, the SHIELD Act goes further to delineate the following 14 specific examples of "reasonable" measures.

Reasonable Administrative Safeguards:

- Designate an employee to coordinate the security program;
- Identify reasonably foreseeable internal and external risks;
- Assess the sufficiency of safeguards in place to control the identified risk;
- Train and manage employees in the security program procedures;
- Select service providers capable of maintaining appropriate safeguards, and require those safeguards by contract; and
- Adjust the security program in light of the business changes or new circumstances.

Reasonable Technical Safeguards:

- Assess risks in network and software design;

[7] N.Y. Gen Bus. Law § 899-aa.

[8] *See* our Dec. 6, 2019, *Alert* for a more general overview of CCPA-related considerations for private fund managers.

[9] The SHIELD Act does not provide a private right of action. Only the New York Attorney General can bring an action to enjoin violations and to obtain civil penalties (which can be up to $5,000 per violation).

- Assess risks in information processing, transmission, and storage;
- Detect, prevent, and respond to attacks or system failure; and
- Regularly test and monitor the effectiveness of key controls and 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
- Dispose of 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.

Private fund managers can compare the specific safeguards above to their current information security program and consider what updates would be (or, if they are covered by the SHIELD Act, are) needed to satisfy the SHIELD Act standards.[10]

Authored by Brian T. Daly, Marc E. Elovitz, Edward H. Sadtler and Kelly Koscuiszka.

If you have any questions concerning this *Alert*, please contact your attorney at Schulte Roth & Zabel or one of the authors.

Schulte Roth & Zabel
New York | Washington DC | London
www.srz.com

[10] The NIST cybersecurity framework, a voluntary framework developed through collaboration between the government and private sector, is another helpful resource for fund managers seeking more detailed operational guidance.