ECKERT SEAMANS ATTORNEYS AT LAW

February 2020

Data Security & Privacy Alert

New York Shield Act Establishes New Breach Notification and Data Protection Requirements

By Sandy B. Garfinkel and Elizabeth W. Brunins

On July 25, 2019, New York Governor Andrew Cuomo signed the Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act"), expanding the scope of New York's prior data breach notification law. The SHIELD Act: (1) enhances breach notification requirements, and (2) introduces new proactive data security requirements.

Timing

The expanded breach notification measures took effect on October 23, 2019, but the new proactive data security requirements are due to take effect on March 21, 2020.

To Whom Does The SHIELD Act Apply?

The SHIELD Act applies to any person or business that owns or licenses computerized data that includes the private information of a New York resident. This applies regardless of whether the person or business has a physical presence in New York State or does business there.

Notification Requirement

The SHIELD Act expanded the definitions of certain terms that will broaden the breach notification requirements, including expanding the definitions and "Private Information" and "Breach":

- "Private Information" now includes biometric information, e-mail addresses in combination with corresponding passwords or security questions and answers, and financial account numbers or credit/debit numbers, even without a security or access code; and
- "Breach" now includes any unauthorized "access" to personal information. Historically, a breach was defined as unauthorized "acquisition," a narrower threshold.

Data Security Protections

Effective March 21, 2020, the SHIELD Act will require companies to take proactive measures by implementing "reasonable safeguards to protect the security, confidentiality and integrity of [New York residents'] private information." Among other things, each company subject to the SHIELD Act must implement a written data security program containing specific elements designed to protect residents' private information. The elements include:

- Designating an employee or employees to coordinate and oversee a data security program;
- Training employees on data security practices and procedures;
- Assessing internal and external risks;

- Vetting service providers and instituting contractual requirements that safeguard the private information of New York residents; and
- Securely destroying private information that is no longer needed.

Penalties For Noncompliance

While the SHIELD Act does not provide for a private right of action, it extends the period of time in which the New York Attorney General may bring an action from two years to three. In addition, the SHIELD Act: (a) doubles the penalty recoverable by the New York Attorney General for failing to make the proper notifications, from $10 to $20 per instance; (b) increases the cap on notification violations from $100,000 to $250,000; and (c) imposes a new civil penalty of up to $5,000 per violation of the new security program standards.

Other States Could Take Similar Measures

There is a definite state law trend toward expansion of the definition of personal information. California, Florida, North Dakota, Nevada, Wyoming, Nebraska, Rhode Island and Illinois all have expanded the scope of what is considered protected information in the past five years to include things like credentials for online accounts, biometric information and healthcare data. This trend is expected to continue.

A written information security program has been required under Massachusetts law for years, but now that New York has also enacted this requirement, other states may follow.

ECKERT SEAMANS
ATTORNEYS AT LAW