WESTERN NEW YORK
THE DAILY RECORD
Part of the BridgeTower Media network
MARCH 6, 2023

White Collar Corner

The enforcement of New York State's SHIELD Act

SPECIAL TO THE DAILY RECORD **ALAN J. BOZER, ANNA MERCADO CLARK and PAULA P. PLAZA**

The New York State (NYS) "Stop Hacks and Improve Electronic Data Security Act" (SHIELD Act) took effect on March 21, 2020, amending the General Business Law (GBL). Among other things, the SHIELD Act expanded data breach notification requirements, strengthened oversight by the New York Attorney General (NYAG), and required businesses and individuals who own or license NYS residents' private data to use "reasonable safeguards" to protect private information. This article discusses key features of the law and two related NYAG investigations. These two cases indicate that the NYAG intends to enforce the SHIELD Act vigorously. (The SHIELD Act does not confer a private right of action.)

Definition of "Private Information"

"Private information" is defined under the SHIELD Act as personal information (i.e., any information that can be used to identify a natural person) plus one or more of the following:

1. Social Security number
2. Driver's license or non-driver identification card number
3. Account, credit or debit card number combined with any security or access code (or other information to permit access)
4. Account, credit or debit card number alone if no additional information is required to access the account
5. Biometric information (g., fingerprint, voice print or other digital representation of unique attributes) or username or email address along with a password or relevant security information to permit access to the account

"Private information" excludes publicly available information from government records.

Definition of "Data Breach"

A data breach is the unauthorized access to or acquisition of, or access to or acquisition without authorization of, data that compromises the security, confidentiality or integrity of private information maintained by a business. The SHIELD Act provides guidelines to determine whether information has been, or is reasonably believed to have been, wrongfully accessed. This includes considering indications that information was viewed, communicated with, used or altered by an unauthorized person.

Breach Notification Requirements

The SHIELD Act reaches beyond those that conduct business in the state. The law provides that "any person or business" that owns or licenses computerized data containing private information of NYS residents, wherever located, is subject to breach notification requirements.

Alan J. Bozer

Anna Mercado Clark

Paula P. Plaza

Notification to a NYS resident whose private information was, or was reasonably believed to have been, accessed or acquired by a person without authorization must be made without unreasonable delay, subject to the needs of law enforcement or any measures necessary to determine the scope of the breach, and to restore the integrity of the impacted.

Notably, notice to affected persons is not required if private information is inadvertently disclosed in good faith by individuals who are authorized to access the information and a determination is made that misuse or financial or emotional harm are unlikely to result from the disclosure. This determination must be documented, and documentation must be preserved for at least five years. If the breach affects over 500 NYS residents, then this written documentation must be disclosed to the NYAG within 10 days after determination.

Businesses may be excused from individual breach notification if notice is made pursuant to other enumerated statutes, including the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA). However, if certain conditions are met, notice must still be provided to the NYAG, Department of State and State Police as well as consumer reporting agencies.

"Reasonable Safeguards" Requirement

The SHIELD Act requires all businesses to adopt "reasonable safeguards" to protect the security, confidentiality and integrity of private information. Businesses, including small businesses, can comply by implementing a data security program that includes reasonable administrative, technical and physical safeguards. Examples of safeguards are listed in the SHIELD Act.

Small businesses (defined as fewer than 50 employees, less than $3 million in gross annual revenue over the preceding three years, or less than $5 million in year-end total assets) can adopt safeguards proportionate to the size and complexity of the business, nature and scope of its activities and sensitivity of information.

Statute of Limitations and Civil Penalty for Breach Notification Violations

Pursuant to NY Executive Law § 63(12) and GBL §§ 349, 899-bb, the NYAG is authorized to investigate allegations of fraudulent or illegal acts and seek civil penalties. The NYAG has three years to commence an action, from either the date of notice or when the NYAG becomes aware of a breach notification violation (whichever comes first). However, if the entity made efforts to conceal the breach, the NYAG has six years to prosecute. Civil penalties for knowingly or recklessly failing to comply with breach notification obligations are $20 per instance of failed notification (capped at $250,000), or $5,000 per violation, whichever is higher.

Two recent NYAG enforcement cases show the importance of implementing a data protection program. Often, regulators impose penalties on businesses not because a data breach occurred, but because they failed to implement reasonable safeguards to protect consumers and/or prepare for a breach.

The Case of Filters Fast

From July 2019 to July 2020, attackers exploited a vulnerability in the online credit card check-out process of Filters Fast, an online water filtration retailer based in North Carolina. The intrusion allowed the attacker to collect purchasers' cardholder names, billing addresses, expiration dates and validation codes for purchases made within the one-year period. When advised of a problem, the company retained an external forensic investigator and patched the website. The breach affected approximately 324,000 consumers nationwide (including 16,618 NYS residents).

In August 2020, Filters Fast notified consumers and regulators about the data incident. The company offered free identity theft protection services to address the security breach.

The NYAG found that Filters Fast failed to:

1. Develop and implement an incident response and data breach notification plan
2. Adopt personal information safeguards and controls (g., to encrypt and to segment private information, develop testing to identify and remediate security vulnerabilities, to log and to monitor network activity and to adopt anti-virus and multifactor authentication (MFA) policies)
3. Ensure information security assessments were conducted

In addition to these remedial measures, Filters Fast agreed to pay a fine of $200,000.

The Case of EyeMed

In June 2020, an attacker gained access to an EyeMed email account used by clients to provide private information in connection with vision benefits enrollment and coverage. The attacker gained the ability to view emails and attachments dating back six years prior to the attack. These documents held consumers' financial and HIPAA information. The breach was undetected. The following month, the attacker sent approximately 2,000 phishing emails from the compromised email account to clients seeking credentials. EyeMed's IT department discovered the transmissions, blocked access and investigated the incident with assistance of a forensic cybersecurity firm. In September 2020, Ohio-based EyeMed began to notify affected individuals and regulators about the data incident, which affected approximately 2.1 million consumers nationwide (including 98,632 NYS residents). The notification offered free identity theft protection services, among other things.

1. Implement MFA to the affected email account
2. Implement sufficient password management (g., limiting the number of incorrect log-in attempts before locking the account and requiring sufficiently complex passwords)
3. Maintain adequate logging and monitoring of its email accounts
4. Follow data retention requirements

EyeMed agreed to take remedial measures and to pay a fine of $600,000.

The NYAG settlement did not relieve EyeMed of any other legal obligations. For instance, in addition to informing the NYAG, among others, EyeMed was also required to report the breach to the Office for Civil Rights (OCR) pursuant to the HIPAA Breach Notification Rule.

Takeaways

Businesses can mitigate cybersecurity risk and liability by keeping abreast of applicable laws, including the SHIELD Act, and by investing in reasonable security measures.

Alan J. Bozer is a partner at Phillips Lytle LLP and leader of the firm's White Collar Criminal Defense & Government Investigations Practice Team. He is also a member of the firm's Data Security & Privacy Practice Team and can be reached at (716) 504-5700 or abozer@phillipslytle.com.

Anna Mercado Clark, CIPP/E, CIPP/US, CIPM, FIP, is a partner at Phillips Lytle LLP and leader of the firm's Data Security & Privacy Practice Team. She is also a member of the firm's White Collar Criminal Defense & Government Investigations Practice Team and can be reached at (585) 238-2000 x6466 or aclark@phillipslytle.com.

Paula P. Plaza is an associate (admission pending) at Phillips Lytle LLP and member of the firm's Data Security & Privacy and White Collar Criminal Defense & Government Investigations Practice Teams. She can be reached at (716) 847-8324 or pplaza@phillipslytle.com.