PROGRAM MATERIALS
Program #3032
January 16, 2020

March 2020: How to Be Ready for New York's New Data Protection Law (the SHIELD Act)

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

Fox Rothschild LLP
ATTORNEYS AT LAW

March 2020: How to Be Ready for New York's New Data Protection Law (the SHIELD Act)

Caroline A. Morgan, Esq.

Nawa A. Lodin, Esq.

The Stop Hacks and Improve Electronic Data Security Act (the SHIELD Act)

- Part 1 went into effect October 23, 2019
- The New York law imposes data breach notification requirements on any business that owns or licenses certain private information of New York residents, regardless of whether it conducts business in New York
- Part 2 goes into effect on March 21, 2020, requiring businesses to develop, implement and maintain a data security program to protect private information

PART ONE: BREACH NOTIFICATION

- When must you notify a person of a breach?

- Disclose any breach to any resident of New York state whose **private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization**.

- The SHIELD Act provides that a business may consider the following factors to determine if a breach has occurred:
  - indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person.

Breach Notification Post SHIELD Act

- SHIELD Act **deletes** the language “conducts business in New York”
- Breach notification now applies to any person or business who “owns or licenses computerized data” which includes private information of any New York resident

See pg. 3, numbered paragraph 2, Senate Bill 5575B (provided in your CLE materials).

Mere **access** can trigger reporting rather than just acquisition

See pg. 2, lines 31-39, Senate Bill 5575B.

What does the SHIELD Act apply to?

Private Information =

(1) Personal information (any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person) PLUS any one of the following data elements:

- SSN
- Driver's license number
- account number, credit card number, in combination with any security code or access code
- Account number
- Biometric information

(2) Username/email with the password or security question answers that would permit access to an online account

See pg. 2, lines 1-30, Senate Bill 5575B

What is not Private Information?

- Publicly available information which is lawfully made available to the general public from federal, state, or local government records.

  See pg. 2, lines 28-30, Senate Bill 5575B

- A data element that is encrypted and the encryption key has not been accessed or acquired.

  See pg. 2, lines 4-9, Senate Bill 5575B

Breach Notification not required

- Notice to persons impacted by an exposure not required if:
  - Exposure was “inadvertent” and,
  - It is “reasonably determined” that the exposure will not “likely result in”
    - the “misuse” of the information,
    - Financial harm or
    - emotional harm
- **BUT** your determination must be in writing and maintained for at least 5 years **PLUS** if the incident affects over 500 residents of New York, you must give the written determination to the State Attorney General within 10 days after the determination.

See pg. 3, lines 22-33, Senate Bill 5575B.

Breach Notification not required

- SHIELD Act recognizes regulatory overlaps- relieves entities that provide notice in accordance with other regulations from the reporting obligations:
  - New York's Department of Financial Services regulations (DFS Cybersecurity Rule)
  - Health Insurance Portability and Accountability Act (HIPAA)
    - HOWEVER, any covered entity required to provide notification to HHS under HIPAA must still notify the NY AG within 5 business days of notifying HHS.

See pg. 3, Senate Bill 5575B.

How is breach notification given to affected persons?

- The disclosure shall be made in the most expedient time possible and without unreasonable delay consistent with the legitimate needs of law enforcement … or any measures necessary to determine the scope of the breach and restore the integrity of the system.

Breach Notification by E-mail

- The SHIELD Act creates a new exception where notice by e-mail is prohibited when the breached information includes the e-mail address in combination with a password or security question and answer.
- This prevents businesses from notifying by e-mail when the notification itself may be sent to a compromised account.

See pg. 4, lines 25-33, Senate Bill 5575B.

How is breach notification given to the State?

- In the event that any New York residents are to be notified, the business shall notify the state attorney general, the department of state and the state office of information technology services as to:
  - the timing, content, distribution of the notices,
  - approximate number of affected persons, and
  - a copy of the template of the notice sent to affected persons.

See pg. 5 at ¶ 8, Senate Bill 5575B.

Hypothetical

1. A covered entity in California discovers that a box with a hard copy list of social security numbers of 600 patients (not including NY residents) was taken from the covered entity's premises.
   - Does the SHIELD Act apply?
2. A covered entity in Connecticut discovers that a list of social security numbers of 600 patients (including NY residents) in the covered entity's internal database has been accessed by an unauthorized person.
   - Is notification required to the persons impacted?
   - Is notification required to the NY AG?
   - Is notification required to Office of Civil Rights HHS?

PART 2: DATA SECURITY PROGRAM

DATA SECURITY PROGRAM (March 21, 2020)

3 takeaways:

- Requires reasonable administrative, technical and physical safeguards
- Brand new component
- Different treatment for “small businesses”

REASONABLE ADMINISTRATIVE SAFEGUARDS

Have you implemented a data security program that includes ALL of the following:

(1) designation of one or more employees to coordinate the data security program;
(2) identify reasonably foreseeable internal and external risks;
(3) assess the sufficiency of safeguards in place to control the identified risks;
(4) train and manage employees in the security program practices and procedures;
(5) select service providers capable of maintaining appropriate safeguards, and require those safeguards by contract; and
(6) adjust the security program in light of business changes or new circumstances

See pg 6, Senate Bill 5575B.

REASONABLE TECHNICAL SAFEGUARDS

Have you implemented a data security program that includes ALL of the following:

(1) assess risks in network and software design;
(2) assess risks in information processing, transmission, and storage;
(3) detect, prevent and respond to attacks or system failures; and
(4) regularly test and monitor the effectiveness of key controls, systems and procedures

See pg. 6, Senate Bill 5575B.

REASONABLE PHYSICAL SAFEGUARDS

Have you implemented a data security program that includes ALL of the following:

(1) assess risk of information storage and disposal;

(2) detect, prevent and respond to intrusions;

(3) protect against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and

(4) 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.

See pg. 6, Senate Bill 5575B.

ARE YOU A “SMALL BUSINESS”

Do you meet any of the following requirements to qualify as a “small business” under the Act?

a. you have fewer than fifty employees;

b. you had less than three million dollars in gross annual revenue in each of the last three fiscal years, or

c. you have less than five million dollars in year-end total assets, calculated in accordance with generally accepted accounting principles.

See pg. 6 lines 3-7, Senate Bill 5575B.

COMPLIANCE FOR A SMALL BUSINESS

Does your security program contain reasonable administrative, technical and physical safeguards that are appropriate for:

a. the size and complexity of your small business;

b. the nature and scope of your small business's activities; and

c. the sensitivity of the personal information your small business collects from or about consumer?

See pg. 6 lines 49-56, Senate Bill 5575B.

CARVE OUTS

- a. regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time (“GLBA”);

- b. regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time (collectively, “HIPAA”);

- c. part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time (“NYDFS Cybersecurity Rules”); or

- d. any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts (“Data Security Rules”)?

OTHER KEY POINTS

- The SHIELD Act does not provide a private right of action

- Governor Cuomo also signed Senate Bill S3582, which requires a credit reporting agency that suffers a breach containing Social Security numbers to offer consumers identity theft prevention and mitigation services.

PENALTIES FOR NON-COMPLIANCE

Civil monetary penalties for noncompliance

Up to $250,000 for breach notification violations

An uncapped amount for failure to comply with data security standards

BIG PICTURE CYBERSECURITY BEST PRACTICES

- Cyber training for staff
- Update policies and procedures
- Designate a key person to coordinate the data security program and breach notifications
- Review how you store and dispose information

TAKEAWAYS AND QUESTIONS

Resources Links

- NYSBA Cybersecurity Guide for Attorneys (6 ways to protect yourself/firm/clients) https://www.nysba.org/nysbacyber/
- The SHIELD Act Senate Bill https://legislation.nysenate.gov/pdf/bills/2019/S5575B
- Senate Bill S3582 https://legislation.nysenate.gov/pdf/bills/2019/S3582 (requirement to offer consumers identity theft protection and mitigation services)
- *The SHIELD Act: How Businesses Across the US Can Comply with New York's New Data Security Law*, Caroline A. Morgan, Fox Rothschild LLP Alert, November 1, 2019.

  https://www.foxrothschild.com/caroline-a-morgan/publications/the-shield-act-how-businesses-across-the-us-can-comply-with-new-yorks-new-data-security-law/
- *Three Key Actions Attorneys Should Take After a Data Breach*, Caroline A. Morgan, The Legal Intelligencer, May 21, 2019. https://www.foxrothschild.com/caroline-a-morgan/publications/three-key-actions-attorneys-should-take-after-a-data-breach/

Caroline A. Morgan, Esq.
646-601-7613
cmorgan@foxrothschild.com
https://www.foxrothschild.com/caroline-a-morgan/

Fox Rothschild LLP
ATTORNEYS AT LAW

Nawa A. Lodin, Esq.
212-878-7969
nlodin@foxrothschild.com
https://www.foxrothschild.com/nawa-a-lodin/

Fox Rothschild LLP
ATTORNEYS AT LAW