STATE OF NEW YORK

6933--A

2017-2018 Regular Sessions

IN SENATE

November 1, 2017

Introduced by Sen. CARLUCCI -- read twice and ordered printed, and when printed to be committed to the Committee on Rules -- recommitted to the Committee on Consumer Protection in accordance with Senate Rule 6, sec. 8 -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the general business law and the state technology law, in relation to notification of a security breach

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. This act shall be known and may be cited as the "New York Data Security Act".

§ 2. The article heading of article 39-F of the general business law, as added by chapter 442 of the laws of 2005, is amended to read as follows:

NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION**; DATA SECURITY PROTECTIONS**

§ 3. Subdivisions 1, 2, 3, 5, 6, 7 and 8 of section 899-aa of the general business law, as added by chapter 442 of the laws of 2005, paragraph (c) of subdivision 1, paragraph (a) of subdivision 6 and subdivision 8 as amended by chapter 491 of the laws of 2005 and paragraph (a) of subdivision 8 as amended by section 6 of part N of chapter 55 of the laws of 2013, are amended and a new subdivision 5-a is added to read as follows:

1. As used in this section, the following terms shall have the following meanings:

(a) "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;

(b) "Private information" shall mean **either: (i)** personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD13619-05-8

data element is not encrypted, or encrypted with an encryption key that has also been **accessed or** acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number; [~~or~~]

(3) account number, credit or debit card number, in combination with any required security code, access code, [~~or~~] password **or other 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 identifying information, security code, access code, or password; or

(5) biometric information, meaning data generated by automatic measurements of an individual's physical characteristics, which are used to authenticate the individual's identity;

(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; or

(iii) any unsecured protected health information held by a "covered entity" as defined in the health insurance portability and accountability act of 1996 (45 C.F.R. pts. 160, 162, 164), as amended from time to time.

"Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

(c) "Breach of the security of the system" shall mean unauthorized **access to or** acquisition **of,** or **access to or** acquisition without valid authorization**,** of computerized data that compromises the security, confidentiality, or integrity of [~~personal~~] **private** information maintained by a business. Good faith **access to, or** acquisition of [~~personal~~]**, private** information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, such business may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others:

(1) indications that the information is in the physical possession and control of **a person without valid authorization or by** an unauthorized person, such as a lost or stolen computer or other device containing information; or

(2) indications that the information has been downloaded or copied; or

(3) indications that the information was used by **a person without valid authorization or** an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(d) "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of

furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to any person or business required to make a notification under subdivision two of this section.

(e) "Credit card" shall mean any card or other credit device issued by a financial institution to a consumer for the purpose of providing money, property, labor or services on credit.

(f) "Debit card" shall mean any card or other device issued by a financial institution to a consumer for use in initiating an electronic fund transfer from the account of the consumer at such financial institution, for the purpose of transferring money between accounts or obtaining money, property, labor or services.

2. Any person or business which [~~conducts business in New York state, and which~~] owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system 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 **or by an unauthorized person**. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the [~~reasonable~~] integrity of the system.

3. Any person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization **or by an unauthorized person**.

5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

(a) written notice;

(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction.

(c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or

(d) substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when such business has an e-mail address for the subject persons**, except if the breached information includes an e-mail address in combination with a password or security question and answer that would permit access to the online account, in which case the person or business shall instead provide clear and conspicuous notice delivered**

to the consumer online when the consumer is connected to the online account from an internet protocol address or from an online location which the person or business knows the consumer customarily uses to access the online account;

(2) conspicuous posting of the notice on such business's web site page, if such business maintains one; and

(3) notification to major statewide media.

5-a. Any credit or debit card issuer that issues a new credit or debit card as a result of a breach of the security of the system pursuant to paragraph (c) of subdivision one of this section, shall provide the consumer notice that the issuance of the replacement credit or debit card is due to a potential compromise of the prior card absent any evidence of actual or potential unauthorized use of such credit or debit card or other circumstances precipitating the issuance of a replacement card.

6. (a) whenever the attorney general shall believe from evidence satisfactory to him that there is a violation of this article he may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation. In such action, preliminary relief may be granted under article sixty-three of the civil practice law and rules. In such action the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this article, if notification was not provided to such person pursuant to this article, including consequential financial losses. Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to [~~ten~~] twenty dollars per instance of failed notification, provided that the latter amount shall not exceed [~~one~~] two hundred fifty thousand dollars.

(b) the remedies provided by this section shall be in addition to any other lawful remedy available.

(c) no action may be brought under the provisions of this section unless such action is commenced within [~~two~~] three years [~~immediately~~] after either the date [~~of the act complained of or the date of discovery of such act~~] on which the attorney general became aware of the violation, or the date of notice sent pursuant to paragraph (a) of subdivision eight of this section, whichever occurs first.

7. Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information, and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization or by an unauthorized person, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.

8. (a) In the event that any New York residents are to be notified, the person or business shall notify the state attorney general, the department of state and the [~~division of state police~~] office of information technology services as to the timing, content and distribution of the notices and approximate number of affected persons and shall provide a copy of the template of the notice sent to affected persons. Such

notice shall be made without delaying notice to affected New York residents.

(b) In the event that more than five thousand New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

§ 4. The general business law is amended by adding a new section 899-bb to read as follows:

§ 899-bb. Data security protections. 1. Definitions. (a) "Compliant regulated entity" shall mean any person or business that is subject to, and in compliance with, any of the following data security requirements:

(i) 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;

(ii) 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;

(iii) 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; or

(iv) 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.

(b) "Certified compliant entity" shall mean any person or business that:

(i) is compliant with any of the data security requirements in paragraph (a) of this subdivision or with the most up to date version of the International Standards Organization Standard 27002 or with the most up to date version of National Institute of Standards and Technology Special Publication 800-53, as it relates to the protection of electronic private information; and

(ii) has such compliance certified annually by an independent, third-party assessment organization that is authorized to provide such certifications by the official department, division, commissioner or agency or standards body that promulgates the data security regulations or standards being certified.

(c) "Private information" shall have the same meaning as defined in section eight hundred ninety-nine-aa of this article.

(d) "Small business" shall mean any person or business with (i) fewer than fifty employees, including any independent contractors, of the business; (ii) less than three million dollars in gross annual revenue in each of the last three fiscal years; or (iii) less than five million dollars in year-end total assets, calculated in accordance with generally accepted accounting principles.

2. Reasonable security. (a) Any person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data.

(b) Small businesses subject to the requirements of paragraph (a) of this subdivision shall be deemed to be in compliance with such requirement if they implement and maintain reasonable safeguards that are appropriate to the size and complexity of the small business to protect

the security, confidentiality and integrity of the private information including, but not limited to, disposal of data.

(c) A person or business shall be deemed to be in compliance with paragraphs (a) and (b) of this subdivision if it either:

(i) is a compliant regulated entity as defined in subdivision one of this section;

(ii) is a certified compliant entity as defined in subdivision one of this section; or

(iii) implements a data security program that includes the following:

(A) administrative safeguards such as the following, in which the person or business:

(1) designates one or more employees to coordinate the security program;

(2) identifies reasonably foreseeable internal and external risks;

(3) assesses the sufficiency of safeguards in place to control the identified risks;

(4) trains and manages employees in the security program practices and procedures;

(5) selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and

(6) adjusts the security program in light of business changes or new circumstances; and

(B) technical safeguards such as the following, in which the person or business:

(1) assesses risks in network and software design;

(2) assesses risks in information processing, transmission and storage;

(3) detects, prevents and responds to attacks or system failures; and

(4) regularly tests and monitors the effectiveness of key controls, systems and procedures; and

(C) physical safeguards such as the following, in which the person or business:

(1) assesses risks of information storage and disposal;

(2) detects, prevents and responds to intrusions;

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

(4) disposes 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.

(d) Any person or business required to comply with paragraph (a) or (b) of this subdivision that fails to comply with such subdivisions shall be deemed to have violated section three hundred forty-nine of this chapter, and the attorney general may bring an action in the name and on behalf of the people of the state of New York to enjoin such violations and to obtain civil penalties under section three hundred fifty-d of this chapter.

(e) Nothing in this section shall create a private right of action.

3. Safe harbor for certified compliant entities. A certified compliant entity shall not be subject to an enforcement action by the attorney general pursuant to subdivision two of this section if:

(a) it provides copies of its certifications of compliance to the attorney general; and

(b) there is no evidence of willful misconduct, bad faith or gross negligence.

§ 5. Paragraph (a) of subdivision 1 and subdivisions 2, 3, 6, 7 and 8 of section 208 of the state technology law, paragraph (a) of subdivision 1 and subdivisions 3 and 8 as added by chapter 442 of the laws of 2005, subdivision 2 and paragraph (a) of subdivision 7 as amended by section 5 of part N of chapter 55 of the laws of 2013 and subdivisions 6 and 7 as amended by chapter 491 of the laws of 2005, are amended to read as follows:

(a) "Private information" shall mean **either: (i)** personal information **consisting of any information** in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been **accessed or** acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number; [~~or~~]

(3) account number, **or** credit or debit card number, in combination with any required **identifying information,** security code, access code, or password which would permit access to an individual's financial account**;**

(4) account number, or credit or debit card number, if circumstances exist wherein such number could be used to access to an individual's financial account without additional identifying information, security code, access code, or password; or

(5) biometric information, meaning data generated by automatic measurements of an individual's physical characteristics, which are used to authenticate the individual's identity;

(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; or

(iii) any unsecured protected health information held by a "covered entity" as defined in the health insurance portability and accountability act of 1996 (45 C.F.R. pts. 160, 162, 164), as amended from time to time.

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

2. Any state entity that owns or licenses computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system 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 **or an unauthorized person**. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the [~~reasonable~~] integrity of the data system. The state entity shall consult with the state office of information technology services to determine the scope of the breach and restoration measures. **Within ninety days of the notice of the breach, the office of information technology services shall deliver a report on the scope of the breach and recommendations to restore and improve the security of the system to the state entity.**

3. Any state entity that maintains computerized data that includes private information which such agency does not own shall notify the owner or licensee of the information of any breach of the security of

the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization **or an unauthorized person**.

6. Regardless of the method by which notice is provided, such notice shall include contact information for the state entity making the notification**, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information** and a description of the categories of information that were, or are reasonably believed to have been, **accessed or** acquired by a person without valid authorization **or an unauthorized person**, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so **accessed or** acquired.

7. (a) In the event that any New York residents are to be notified, the state entity shall notify the state attorney general, the department of state and the state office of information technology services as to the timing, content and distribution of the notices and approximate number of affected persons **and provide a copy of the template of the notice sent to affected persons**. Such notice shall be made without delaying notice to affected New York residents.

(b) In the event that more than five thousand New York residents are to be notified at one time, the state entity shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

8. **The state office of information technology services shall develop, update and provide regular training to all state entities relating to best practices for the prevention of a breach of the security of the system.**

9. Any entity listed in subparagraph two of paragraph (c) of subdivision one of this section shall adopt a notification policy no more than one hundred twenty days after the effective date of this section. Such entity may develop a notification policy which is consistent with this section or alternatively shall adopt a local law which is consistent with this section.

§ 6. This act shall take effect on the first of January next succeeding the date on which it shall have become a law.