S T A T E O F N E W Y O R K

6834--B

I N S E N A T E

February 26, 2016

Introduced by Sen. VENDITTO -- read twice and ordered printed, and when printed to be committed to the Committee on Consumer Protection -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- 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. Subdivisions 1, 2, 5, 6, 7, 8 and 9 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 data element is not encrypted, or encrypted with an encryption key that has also been 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 that would permit access to an individual's financial account; OR

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

LBD09470-16-6

(4) BIOMETRIC INFORMATION, MEANING DATA GENERATED BY AUTOMATIC MEASUREMENTS OF AN INDIVIDUAL'S PHYSICAL CHARACTERISTICS, WHICH ARE USED BY THE OWNER OR LICENSEE 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 acquisition 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 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 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] PUBLICLY POSTED ON ITS WEBSITE.

(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, 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.

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, PROVIDED THE BREACHED INFORMATION DOES NOT INCLUDE 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 NOT COMPLY WITH THIS SECTION BY PROVIDING NOTICE TO THAT E-MAIL ACCOUNT, BUT SHALL INSTEAD COMPLY WITH THIS SECTION BY 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 ACCESSES 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 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, 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 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 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.

9. THE DEPARTMENT OF STATE SHALL RECEIVE COMPLAINTS PURSUANT TO SECTION NINETY-FOUR-A OF THE EXECUTIVE LAW RELATING TO ANY BREACH OF THE SECURITY OF THE SYSTEM, MAKE REFERRALS AS APPROPRIATE AND IN COOPERATION WITH THE STATE ATTORNEY GENERAL AND THE OFFICE OF INFORMATION TECHNOLOGY SERVICES DEVELOP, REGULARLY UPDATE AND MAKE PUBLICLY AVAILABLE INFORMATION RELATING TO HOW TO RESPOND TO A BREACH OF THE SECURITY OF THE SYSTEM AND BEST PRACTICES FOR HOW TO PREVENT A BREACH OF THE SECURITY OF THE SYSTEM.

10. The provisions of this section shall be exclusive and shall preempt any provisions of local law, ordinance or code, and no locality shall impose requirements that are inconsistent with or more restrictive than those set forth in this section.

S 2. Paragraphs (a) and (d) of subdivision 1 and subdivisions 2, 6, 7 and 8 of section 208 of the state technology law, paragraphs (a) and (d) of subdivision 1 and subdivision 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: (I) personal 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 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 which would permit access to an individual's financial account; OR

(4) BIOMETRIC INFORMATION, MEANING DATA GENERATED BY AUTOMATIC MEASUREMENTS OF AN INDIVIDUAL'S PHYSICAL CHARACTERISTICS, WHICH ARE USED BY THE OWNER OR LICENSEE 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.

(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 state entities required to make a notification under subdivision two of this section] PUBLICLY POSTED ON ITS WEBSITE.

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, 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.

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 THE WEBSITES FOR 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, 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 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.

S 3. This act shall take effect January 1, 2017.