STATE OF NEW YORK

5232

2017-2018 Regular Sessions

IN ASSEMBLY

February 7, 2017

Introduced by M. of A. DINOWITZ, GOTTFRIED, GALEF, TITONE, COOK, ABINANTI, ENGLEBRIGHT, OTIS, FAHY, COLTON -- read once and referred to the Committee on Consumer Affairs and Protection

AN ACT to amend the general business law, in relation to the protection of personal information by businesses

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

Section 1. 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, is amended to read as follows:

§ 899-aa. **Safeguarding personal information;** [~~Notification;~~] **notification,** person without valid authorization has acquired private information. 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 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;

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

LBD03435-01-7

"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 information maintained by a business. Good faith acquisition of personal 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 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 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.

2. Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall**:**

(a) develop, implement, and maintain a comprehensive information security program which must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal laws or regulations by which the person who owns or licenses such information may be regulated, and that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

(1) the size, scope, and type of business of the person obligated to safeguard the personal information under such comprehensive information security program;

(2) the amount of resources available to such person or business;

(3) the amount of stored data; and

(4) the need for security and confidentiality of information of customers and employees of the business.

(b) 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. 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~~] **five** of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

3. Without limiting the generality of the foregoing, every comprehensive information security program pursuant to paragraph (a) of subdivision two of this section shall include, but not be limited to:

(a) designating one or more employees to maintain the comprehensive information security program;

(b) identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information, and evaluating and improving, where necessary, the current safeguards for limiting such risks, including, but not limited to:

(1) providing ongoing employee training;

(2) monitoring employee compliance with policies and procedures; and

(3) identifying means for detecting and preventing security system failures.

(c) developing security policies for employees relating to the storage, access, and transportation of records containing personal information outside of business premises;

(d) imposing disciplinary measures for violations of the comprehensive information security program rules;

(e) preventing terminated or former employees from accessing records containing personal information;

(f) overseeing third-party service providers by:

(1) taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these provisions and any applicable federal laws or regulations; and

(2) requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until October first, two thousand eighteen, a contract a person or business has entered into with a third-party service provider to perform services for or functions on behalf of such person or business satisfies the provisions of this subparagraph even if the contract a person or business has entered into with a third-party service provider does not include a requirement that the third-party service provider maintains such appropriate safeguards, as long as said person or business entered into the contract no later than October first, two thousand sixteen.

(g) placing reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas, or containers;

(h) ensuring that the comprehensive information security program is separating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information, and upgrading information safeguards as necessary to limit risks;

(i) reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably jeopardize the security or integrity of records containing personal information; and

(j) documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

[~~3.~~]4. Any person or business which maintains computerized data which includes private information which such person or business does not own shall:

(a) include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, include the following elements:

(1) secure user authentication protocols including:

(i) control of user identifications and other identifiers;

(ii) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

(iii) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;

(iv) restricting access to active users and active user accounts only; and

(v) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

(2) secure access control measures that:

(i) restrict access to records and files containing personal information to those who need such information to perform their job duties; and

(ii) assign unique identifications plus passwords, which are not vendor-supplied default passwords, to each person with computer access that are reasonably designed to maintain the integrity of the security of the access controls;

(3) encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly;

(4) reasonable monitoring of systems for unauthorized use of or access to personal information;

(5) encryption of all personal information stored on laptops or other portable devices;

(6) for files containing personal information on a system that is connected to the internet, firewall protection and operating system security patches reasonably designed to maintain the integrity of the personal information;

(7) system security agent software which must include malware protection and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis; and

(8) education and training of employees on the proper use of the computer security system and the importance of personal information security.

(b) 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.

[~~4.~~] 5. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

[~~5.~~] 6. 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;

(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.

[~~6.~~] 7. (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 dollars per instance of failed notification, provided that the latter amount shall not exceed one 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 the date of the act complained of or the date of discovery of such act.

[~~7.~~] 8. Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

[~~8.~~] 9. (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 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.

(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.~~] 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.

§ 2. This act shall take effect immediately; provided, however, that the provisions of this act shall apply to any person or business who owns or licenses personal information about a resident of New York within eighteen months after such effective date, provided, further, that any person or business may come into compliance before such effective date.