

6834

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

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:

1     Section 1. Subdivisions 1, 2, 6, 7, 8 and 9 of section 899-aa of the  
2     general business law, as added by chapter 442 of the laws of 2005, para-  
3     graph (c) of subdivision 1, paragraph (a) of subdivision 6 and subdivi-  
4     sion 8 as amended by chapter 491 of the laws of 2005 and paragraph (a)  
5     of subdivision 8 as amended by section 6 of part N of chapter 55 of the  
6     laws of 2013, are amended to read as follows:  
7     1. As used in this section, the following terms shall have the follow-  
8     ing meanings:  
9     (a) "Personal information" shall mean any information concerning a  
10    natural person which, because of name, number, personal mark, or other  
11    identifier, can be used to identify such natural person;  
12    (b) "Private information" shall mean EITHER: (I) personal information  
13    consisting of any information in combination with any one or more of the  
14    following data elements, when either the personal information or the  
15    data element is not encrypted, or encrypted with an encryption key that  
16    has also been acquired:  
17    (1) social security number;  
18    (2) driver's license number or non-driver identification card number;  
19    [or]  
20    (3) account number, credit or debit card number, in combination with  
21    any required security code, access code, or password that would permit  
22    access to an individual's financial account; OR  
23    (4) BIOMETRIC INFORMATION, MEANING DATA GENERATED BY AUTOMATIC MEAS-  
24    UREMENTS OF AN INDIVIDUAL'S PHYSICAL CHARACTERISTICS, WHICH ARE USED BY  
25    THE OWNER OR LICENSEE TO AUTHENTICATE THE INDIVIDUAL'S IDENTITY;  
26    (II) A USER NAME OR EMAIL ADDRESS IN COMBINATION WITH A PASSWORD OR  
27    SECURITY QUESTION AND ANSWER THAT WOULD PERMIT ACCESS TO AN ONLINE  
28    ACCOUNT; OR

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

LBD09470-07-6

(III) ANY UNSECURED PROTECTED HEALTH INFORMATION 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 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] PUBLICLY POSTED ON ITS WEBSITE.

(E) "CREDIT CARD" SHALL HAVE THE SAME MEANING AS IN 15 U.S.C. S 1602.

(F) "DEBIT CARD" SHALL HAVE THE SAME MEANING AS IN 15 U.S.C. S 1681A.

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.

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

1 damages for actual costs or losses incurred by a person entitled to  
2 notice pursuant to this article, if notification was not provided to  
3 such person pursuant to this article, including consequential financial  
4 losses. Whenever the court shall determine in such action that a person  
5 or business violated this article knowingly or recklessly, the court may  
6 impose a civil penalty of the greater of [five] TEN thousand dollars or  
7 up to [ten] TWENTY dollars per instance of failed notification, provided  
8 that the latter amount shall not exceed [one] TWO hundred fifty thousand  
9 dollars.

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

12 (c) no action may be brought under the provisions of this section  
13 unless such action is commenced within [two] THREE years [immediately]  
14 after EITHER the date [of the act complained of or the date of discovery  
15 of such act] THE ACT WAS DISCOVERED OR, THE DATE OF NOTICE SENT PURSUANT  
16 TO PARAGRAPH (A) OF SUBDIVISION EIGHT OF THIS SECTION.

17 7. Regardless of the method by which notice is provided, such notice  
18 shall PRECEDE THE ISSUANCE OF ANY REPLACEMENT CREDIT CARD OR DEBIT CARD  
19 TO ANY AFFECTED PERSON AS A RESULT OF ANY BREACH OF THE SECURITY OF THE  
20 SYSTEM ABSENT ANY DOCUMENTED EVIDENCE OF UNAUTHORIZED USE OF SUCH CREDIT  
21 CARD OR DEBIT CARD AND SHALL include contact information for the person  
22 or business making the notification, THE TELEPHONE NUMBERS AND WEBSITES  
23 OF THE RELEVANT STATE AND FEDERAL AGENCIES THAT PROVIDE INFORMATION  
24 REGARDING SECURITY BREACH RESPONSE AND IDENTITY THEFT PREVENTION AND  
25 PROTECTION INFORMATION, and a description of the categories of informa-  
26 tion that were, or are reasonably believed to have been, acquired by a  
27 person without valid authorization OR BY AN UNAUTHORIZED PERSON, includ-  
28 ing specification of which of the elements of personal information and  
29 private information were, or are reasonably believed to have been, so  
30 acquired.

31 8. (a) In the event that any New York residents are to be notified,  
32 the person or business shall notify the state attorney general, the  
33 department of state and the [division of state police] OFFICE OF INFOR-  
34 MATION TECHNOLOGY SERVICES as to the timing, content and distribution of  
35 the notices [and], approximate number of affected persons AND PROVIDE A  
36 COPY OF THE TEMPLATE OF THE NOTICE SENT TO AFFECTED PERSONS. Such  
37 notice shall be made without delaying notice to affected New York resi-  
38 dents.

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

44 9. THE DEPARTMENT OF STATE SHALL RECEIVE AND RESPOND TO COMPLAINTS AND  
45 INQUIRIES RELATING TO ANY BREACH OF THE SECURITY OF THE SYSTEM, MAKE  
46 REFERRALS AS APPROPRIATE AND IN COOPERATION WITH THE STATE ATTORNEY  
47 GENERAL AND THE OFFICE OF INFORMATION TECHNOLOGY SERVICES DEVELOP, REGU-  
48 LARLY UPDATE AND MAKE PUBLICLY AVAILABLE INFORMATION RELATING TO HOW TO  
49 RESPOND TO A BREACH OF THE SECURITY OF THE SYSTEM AND BEST PRACTICES FOR  
50 HOW TO PREVENT A BREACH OF THE SECURITY OF THE SYSTEM.

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

55 S 2. Paragraphs (a) and (d) of subdivision 1 and subdivisions 2, 6, 7  
56 and 8 of section 208 of the state technology law, 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 EMAIL 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 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. 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

1 BREACH RESPONSE AND IDENTITY THEFT PREVENTION AND PROTECTION INFORMATION  
2 and a description of the categories of information that were, or are  
3 reasonably believed to have been, acquired by a person without valid  
4 authorization, including specification of which of the elements of  
5 personal information and private information were, or are reasonably  
6 believed to have been, so acquired.

7 7. (a) In the event that any New York residents are to be notified,  
8 the state entity shall notify the state attorney general, the department  
9 of state and the state office of information technology services as to  
10 the timing, content and distribution of the notices and approximate  
11 number of affected persons AND PROVIDE A COPY OF THE TEMPLATE OF THE  
12 NOTICE SENT TO AFFECTED PERSONS. Such notice shall be made without  
13 delaying notice to affected New York residents.

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

19 8. THE STATE OFFICE OF INFORMATION TECHNOLOGY SERVICES SHALL DEVELOP,  
20 UPDATE AND PROVIDE REGULAR TRAINING TO ALL STATE ENTITIES RELATING TO  
21 BEST PRACTICES FOR THE PREVENTION OF A BREACH OF THE SECURITY OF THE  
22 SYSTEM.

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

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