

6834--A

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

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, 5, 6, 7, 8 and 9 of section 899-aa of
2 the general business law, as added by chapter 442 of the laws of 2005,
3 paragraph (c) of subdivision 1, paragraph (a) of subdivision 6 and
4 subdivision 8 as amended by chapter 491 of the laws of 2005 and para-
5 graph (a) of subdivision 8 as amended by section 6 of part N of chapter
6 55 of the 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;

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

LBD09470-10-6

1 (II) A USER NAME OR E-MAIL ADDRESS IN COMBINATION WITH A PASSWORD OR
2 SECURITY QUESTION AND ANSWER THAT WOULD PERMIT ACCESS TO AN ONLINE
3 ACCOUNT; OR

4 (III) ANY UNSECURED PROTECTED HEALTH INFORMATION HELD BY A "COVERED
5 ENTITY" AS DEFINED IN THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABIL-
6 ITY ACT OF 1996 (45 C.F.R. PTS. 160, 162, 164), AS AMENDED FROM TIME TO
7 TIME.

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

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

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

23 (1) indications that the information is in the physical possession and
24 control of A PERSON WITHOUT VALID AUTHORIZATION OR BY an unauthorized
25 person, such as a lost or stolen computer or other device containing
26 information; or

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

28 (3) indications that the information was used by A PERSON WITHOUT
29 VALID AUTHORIZATION OR an unauthorized person, such as fraudulent
30 accounts opened or instances of identity theft reported.

31 (d) "Consumer reporting agency" shall mean any person which, for mone-
32 tary fees, dues, or on a cooperative nonprofit basis, regularly engages
33 in whole or in part in the practice of assembling or evaluating consumer
34 credit information or other information on consumers for the purpose of
35 furnishing consumer reports to third parties, and which uses any means
36 or facility of interstate commerce for the purpose of preparing or
37 furnishing consumer reports. A list of consumer reporting agencies shall
38 be compiled by the state attorney general and [furnished upon request to
39 any person or business required to make a notification under subdivision
40 two of this section] PUBLICLY POSTED ON ITS WEBSITE.

41 (E) "CREDIT CARD" SHALL MEAN ANY CARD OR OTHER CREDIT DEVICE ISSUED BY
42 A FINANCIAL INSTITUTION TO A CONSUMER FOR THE PURPOSE OF PROVIDING
43 MONEY, PROPERTY, LABOR OR SERVICES ON CREDIT.

44 (F) "DEBIT CARD" SHALL MEAN ANY CARD OR OTHER DEVICE ISSUED BY A
45 FINANCIAL INSTITUTION TO A CONSUMER FOR USE IN INITIATING AN ELECTRONIC
46 FUND TRANSFER FROM THE ACCOUNT OF THE CONSUMER AT SUCH FINANCIAL INSTI-
47 TUTION, FOR THE PURPOSE OF TRANSFERRING MONEY BETWEEN ACCOUNTS OR
48 OBTAINING MONEY, PROPERTY, LABOR, OR SERVICES.

49 2. Any person or business which conducts business in New York state,
50 and which owns or licenses computerized data which includes private
51 information shall disclose any breach of the security of the system
52 following discovery or notification of the breach in the security of the
53 system to any resident of New York state whose private information was,
54 or is reasonably believed to have been, acquired by a person without
55 valid authorization OR BY AN UNAUTHORIZED PERSON. The disclosure shall
56 be made in the most expedient time possible and without unreasonable

1 delay, consistent with the legitimate needs of law enforcement, as
2 provided in subdivision four of this section, or any measures necessary
3 to determine the scope of the breach and restore the [reasonable] integ-
4 rity of the system.

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

7 (a) written notice;

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

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

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

23 (1) e-mail notice when such business has an e-mail address for the
24 subject persons, PROVIDED THE BREACHED INFORMATION DOES NOT INCLUDE AN
25 E-MAIL ADDRESS IN COMBINATION WITH A PASSWORD OR SECURITY QUESTION AND
26 ANSWER THAT WOULD PERMIT ACCESS TO THE ONLINE ACCOUNT, IN WHICH CASE,
27 NOTICE SHOULD BE PROVIDED AS DESCRIBED IN PARAGRAPH (E) OF THIS SUBDIVI-
28 SION;

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

31 (3) notification to major statewide media.

32 (E) IN THE CASE OF A BREACH OF THE SECURITY OF THE SYSTEM INVOLVING AN
33 E-MAIL ADDRESS IN COMBINATION WITH A PASSWORD OR SECURITY QUESTION AND
34 ANSWER THAT WOULD PERMIT ACCESS TO THE ONLINE ACCOUNT AS OUTLINED IN
35 SUBPARAGRAPH (II) OF PARAGRAPH (B) OF SUBDIVISION ONE OF THIS SECTION,
36 AND NO OTHER PRIVATE INFORMATION DEFINED IN PARAGRAPH (B) OF SUBDIVISION
37 ONE OF THIS SECTION, THE PERSON OR BUSINESS SHALL NOT COMPLY WITH THIS
38 SECTION BY PROVIDING THE SECURITY BREACH NOTIFICATION TO THAT E-MAIL
39 ACCOUNT, BUT SHALL INSTEAD COMPLY WITH THIS SECTION BY PROVIDING NOTICE
40 BY ANOTHER METHOD DESCRIBED IN THIS SUBDIVISION OR BY CLEAR AND CONSPIC-
41 UOUS NOTICE DELIVERED TO THE CONSUMER ONLINE WHEN THE CONSUMER IS
42 CONNECTED TO THE ONLINE ACCOUNT FROM AN INTERNET PROTOCOL ADDRESS OR
43 FROM AN ONLINE LOCATION WHICH THE PERSON OR BUSINESS KNOWS THE CONSUMER
44 CUSTOMARILY ACCESSES THE ONLINE ACCOUNT.

45 (F) ANY CREDIT OR DEBIT CARD ISSUER THAT ISSUES A NEW CREDIT OR DEBIT
46 CARD AS A RESULT OF A BREACH OF THE SECURITY OF THE SYSTEM PURSUANT TO
47 PARAGRAPH (C) OF SUBDIVISION ONE OF THIS SECTION, SHALL PROVIDE NOTICE
48 PRIOR TO THE ISSUANCE OF ANY REPLACEMENT CREDIT OR DEBIT CARD ABSENT ANY
49 DOCUMENTED EVIDENCE OF UNAUTHORIZED USE OF SUCH CREDIT OR DEBIT CARD.

50 6. (a) whenever the attorney general shall believe from evidence
51 satisfactory to him that there is a violation of this article he may
52 bring an action in the name and on behalf of the people of the state of
53 New York, in a court of justice having jurisdiction to issue an injunc-
54 tion, to enjoin and restrain the continuation of such violation. In
55 such action, preliminary relief may be granted under article sixty-three
56 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 include contact information for the person or business making the
19 notification, THE TELEPHONE NUMBERS AND WEBSITES OF THE RELEVANT STATE
20 AND FEDERAL AGENCIES THAT PROVIDE INFORMATION REGARDING SECURITY BREACH
21 RESPONSE AND IDENTITY THEFT PREVENTION AND PROTECTION INFORMATION, and a
22 description of the categories of information that were, or are reason-
23 ably believed to have been, acquired by a person without valid authori-
24 zation OR BY AN UNAUTHORIZED PERSON, including specification of which of
25 the elements of personal information and private information were, or
26 are reasonably believed to have been, so acquired.

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

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

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

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

51 S 2. Paragraphs (a) and (d) of subdivision 1 and subdivisions 2, 6, 7
52 and 8 of section 208 of the state technology law, paragraphs (a) and (d)
53 of subdivision 1 and subdivision 8 as added by chapter 442 of the laws
54 of 2005, subdivision 2 and paragraph (a) of subdivision 7 as amended by
55 section 5 of part N of chapter 55 of the laws of 2013 and subdivisions 6

1 and 7 as amended by chapter 491 of the laws of 2005, are amended to read
2 as follows:

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

7 (1) social security number;

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

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

13 (4) BIOMETRIC INFORMATION, MEANING DATA GENERATED BY AUTOMATIC MEAS-
14 UREMENTS OF AN INDIVIDUAL'S PHYSICAL CHARACTERISTICS, WHICH ARE USED BY
15 THE OWNER OR LICENSEE TO AUTHENTICATE THE INDIVIDUAL'S IDENTITY;

16 (II) A USER NAME OR E-MAIL ADDRESS IN COMBINATION WITH A PASSWORD OR
17 SECURITY QUESTION AND ANSWER THAT WOULD PERMIT ACCESS TO AN ONLINE
18 ACCOUNT; OR

19 (III) ANY UNSECURED PROTECTED HEALTH INFORMATION AS DEFINED IN THE
20 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (45 C.F.R.
21 PTS. 160, 162, 164), AS AMENDED FROM TIME TO TIME.

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

25 (d) "Consumer reporting agency" shall mean any person which, for mone-
26 tary fees, dues, or on a cooperative nonprofit basis, regularly engages
27 in whole or in part in the practice of assembling or evaluating consumer
28 credit information or other information on consumers for the purpose of
29 furnishing consumer reports to third parties, and which uses any means
30 or facility of interstate commerce for the purpose of preparing or
31 furnishing consumer reports. A list of consumer reporting agencies shall
32 be compiled by the state attorney general and [furnished upon request to
33 state entities required to make a notification under subdivision two of
34 this section] PUBLICLY POSTED ON ITS WEBSITE.

35 2. Any state entity that owns or licenses computerized data that
36 includes private information shall disclose any breach of the security
37 of the system following discovery or notification of the breach in the
38 security of the system to any resident of New York state whose private
39 information was, or is reasonably believed to have been, acquired by a
40 person without valid authorization OR AN UNAUTHORIZED PERSON. The
41 disclosure shall be made in the most expedient time possible and without
42 unreasonable delay, consistent with the legitimate needs of law enforce-
43 ment, as provided in subdivision four of this section, or any measures
44 necessary to determine the scope of the breach and restore the [reason-
45 able] integrity of the data system. The state entity shall consult with
46 the state office of information technology services to determine the
47 scope of the breach and restoration measures. WITHIN NINETY DAYS OF THE
48 NOTICE OF THE BREACH, THE OFFICE OF INFORMATION TECHNOLOGY SERVICES
49 SHALL DELIVER A REPORT ON THE SCOPE OF THE BREACH AND RECOMMENDATIONS TO
50 RESTORE AND IMPROVE THE SECURITY OF THE SYSTEM TO THE STATE ENTITY.

51 6. Regardless of the method by which notice is provided, such notice
52 shall include contact information for the state entity making the
53 notification, THE TELEPHONE NUMBERS AND THE WEBSITES FOR THE RELEVANT
54 STATE AND FEDERAL AGENCIES THAT PROVIDE INFORMATION REGARDING SECURITY
55 BREACH RESPONSE AND IDENTITY THEFT PREVENTION AND PROTECTION INFORMATION
56 and a description of the categories of information that were, or are

1 reasonably believed to have been, acquired by a person without valid
2 authorization OR AN UNAUTHORIZED PERSON, including specification of
3 which of the elements of personal information and private information
4 were, or are reasonably believed to have been, so acquired.

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

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

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

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

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