

10190

I N A S S E M B L Y

September 24, 2014

Introduced by COMMITTEE ON RULES -- (at request of 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:

1 Section 1. Section 899-aa of the general business law, as added by
2 chapter 442 of the laws of 2005, paragraph (c) of subdivision 1, para-
3 graph (a) of subdivision 6 and subdivision 8 as amended by chapter 491
4 of the laws of 2005 and paragraph (a) of subdivision 8 as amended by
5 section 6 of part N of chapter 55 of the laws of 2013, is amended to
6 read as follows:
7 S 899-aa. SAFEGUARDING PERSONAL INFORMATION; [Notification;] NOTIFICA-
8 TION, person without valid authorization has acquired private informa-
9 tion. 1. As used in this section, the following terms shall have the
10 following meanings:
11 (a) "Personal information" shall mean any information concerning a
12 natural person which, because of name, number, personal mark, or other
13 identifier, can be used to identify such natural person;
14 (b) "Private information" shall mean personal information consisting
15 of any information in combination with any one or more of the following
16 data elements, when either the personal information or the data element
17 is not encrypted, or encrypted with an encryption key that has also been
18 acquired:
19 (1) social security number;
20 (2) driver's license number or non-driver identification card number;
21 or
22 (3) account number, credit or debit card number, in combination with
23 any required security code, access code, or password that would permit
24 access to an individual's financial account;

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

LBD15710-01-4

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

4 (c) "Breach of the security of the system" shall mean unauthorized
5 acquisition or acquisition without valid authorization of computerized
6 data that compromises the security, confidentiality, or integrity of
7 personal information maintained by a business. Good faith acquisition of
8 personal information by an employee or agent of the business for the
9 purposes of the business is not a breach of the security of the system,
10 provided that the private information is not used or subject to unau-
11 thorized disclosure.

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

16 (1) indications that the information is in the physical possession and
17 control of an unauthorized person, such as a lost or stolen computer or
18 other device containing information; or

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

20 (3) indications that the information was used by an unauthorized
21 person, such as fraudulent accounts opened or instances of identity
22 theft reported.

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

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

36 (A) DEVELOP, IMPLEMENT, AND MAINTAIN A COMPREHENSIVE INFORMATION SECU-
37 RITY PROGRAM WHICH MUST BE CONSISTENT WITH THE SAFEGUARDS FOR PROTECTION
38 OF PERSONAL INFORMATION AND INFORMATION OF A SIMILAR CHARACTER SET FORTH
39 IN ANY STATE OR FEDERAL LAWS OR REGULATIONS BY WHICH THE PERSON WHO OWNS
40 OR LICENSES SUCH INFORMATION MAY BE REGULATED, AND THAT IS WRITTEN IN
41 ONE OR MORE READILY ACCESSIBLE PARTS AND CONTAINS ADMINISTRATIVE, TECH-
42 NICAL, AND PHYSICAL SAFEGUARDS THAT ARE APPROPRIATE TO:

43 (I) THE SIZE, SCOPE, AND TYPE OF BUSINESS OF THE PERSON OBLIGATED TO
44 SAFEGUARD THE PERSONAL INFORMATION UNDER SUCH COMPREHENSIVE INFORMATION
45 SECURITY PROGRAM;

46 (II) THE AMOUNT OF RESOURCES AVAILABLE TO SUCH PERSON OR BUSINESS;

47 (III) THE AMOUNT OF STORED DATA; AND

48 (IV) THE NEED FOR SECURITY AND CONFIDENTIALITY OF INFORMATION OF
49 CUSTOMERS AND EMPLOYEES OF THE BUSINESS.

50 (B) disclose any breach of the security of the system following
51 discovery or notification of the breach in the security of the system to
52 any resident of New York state whose private information was, or is
53 reasonably believed to have been, acquired by a person without valid
54 authorization. The disclosure shall be made in the most expedient time
55 possible and without unreasonable delay, consistent with the legitimate
56 needs of law enforcement, as provided in subdivision four of this

1 section, or any measures necessary to determine the scope of the breach
2 and restore the reasonable integrity of the system.

3 3. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, EVERY COMPREHEN-
4 SIVE INFORMATION SECURITY PROGRAM PURSUANT TO PARAGRAPH (A) OF SUBDIVI-
5 SION TWO SHALL INCLUDE, BUT NOT BE LIMITED TO:

6 (A) DESIGNATING ONE OR MORE EMPLOYEES TO MAINTAIN THE COMPREHENSIVE
7 INFORMATION SECURITY PROGRAM;

8 (B) IDENTIFYING AND ASSESSING REASONABLY FORESEEABLE INTERNAL AND
9 EXTERNAL RISKS TO THE SECURITY, CONFIDENTIALITY, AND/OR INTEGRITY OF ANY
10 ELECTRONIC, PAPER, OR OTHER RECORDS CONTAINING PERSONAL INFORMATION, AND
11 EVALUATING AND IMPROVING, WHERE NECESSARY, THE CURRENT SAFEGUARDS FOR
12 LIMITING SUCH RISKS, INCLUDING, BUT NOT LIMITED TO:

13 (I) PROVIDING ONGOING EMPLOYEE TRAINING;

14 (II) MONITORING EMPLOYEE COMPLIANCE WITH POLICIES AND PROCEDURES; AND

15 (III) IDENTIFYING MEANS FOR DETECTING AND PREVENTING SECURITY SYSTEM
16 FAILURES.

17 (C) DEVELOPING SECURITY POLICIES FOR EMPLOYEES RELATING TO THE STOR-
18 AGE, ACCESS, AND TRANSPORTATION OF RECORDS CONTAINING PERSONAL INFORMA-
19 TION OUTSIDE OF BUSINESS PREMISES;

20 (D) IMPOSING DISCIPLINARY MEASURES FOR VIOLATIONS OF THE COMPREHENSIVE
21 INFORMATION SECURITY PROGRAM RULES;

22 (E) PREVENTING TERMINATED OR FORMER EMPLOYEES FROM ASSESSING RECORDS
23 CONTAINING PERSONAL INFORMATION;

24 (F) OVERSEEING THIRD-PARTY SERVICE PROVIDERS BY:

25 (I) TAKING REASONABLE STEPS TO SELECT AND RETAIN THIRD-PARTY SERVICE
26 PROVIDERS THAT ARE CAPABLE OF MAINTAINING APPROPRIATE SECURITY MEASURES
27 TO PROTECT SUCH PERSONAL INFORMATION CONSISTENT WITH THESE PROVISIONS
28 AND ANY APPLICABLE FEDERAL LAWS OR REGULATIONS; AND

29 (II) REQUIRING SUCH THIRD-PARTY SERVICE PROVIDERS BY CONTRACT TO
30 IMPLEMENT AND MAINTAIN SUCH APPROPRIATE SECURITY MEASURES FOR PERSONAL
31 INFORMATION; PROVIDED, HOWEVER, THAT UNTIL OCTOBER FIRST, TWO THOUSAND
32 SEVENTEEN, A CONTRACT A PERSON OR BUSINESS HAS ENTERED INTO WITH A
33 THIRD-PARTY SERVICE PROVIDER TO PERFORM SERVICES FOR OR FUNCTIONS ON
34 BEHALF OF SUCH PERSON OR BUSINESS SATISFIES THE PROVISIONS OF THIS
35 SUBPARAGRAPH EVEN IF THE CONTRACT A PERSON OR BUSINESS HAS ENTERED INTO
36 WITH A THIRD-PARTY SERVICE PROVIDER DOES NOT INCLUDE A REQUIREMENT THAT
37 THE THIRD-PARTY SERVICE PROVIDER MAINTAINS SUCH APPROPRIATE SAFEGUARDS,
38 AS LONG AS SAID PERSON OR BUSINESS ENTERED INTO THE CONTRACT NO LATER
39 THAN OCTOBER FIRST, TWO THOUSAND FIFTEEN.

40 (G) PLACING REASONABLE RESTRICTIONS UPON PHYSICAL ACCESS TO RECORDS
41 CONTAINING PERSONAL INFORMATION, AND STORAGE OF SUCH RECORDS AND DATA IN
42 LOCKED FACILITIES, STORAGE AREAS, OR CONTAINERS;

43 (H) ENSURING THAT THE COMPREHENSIVE INFORMATION SECURITY PROGRAM IS
44 SEPARATING IN A MANNER REASONABLY CALCULATED TO PREVENT UNAUTHORIZED
45 ACCESS TO OR UNAUTHORIZED USE OF PERSONAL INFORMATION, AND UPGRADING
46 INFORMATION SAFEGUARDS AS NECESSARY TO LIMIT RISKS;

47 (I) REVIEWING THE SCOPE OF THE SECURITY MEASURES AT LEAST ANNUALLY OR
48 WHENEVER THERE IS A MATERIAL CHANGE IN BUSINESS PRACTICES THAT MAY
49 REASONABLY JEOPARDIZE THE SECURITY OR INTEGRITY OF RECORDS CONTAINING
50 PERSONAL INFORMATION; AND

51 (J) DOCUMENTING RESPONSIVE ACTIONS TAKEN IN CONNECTION WITH ANY INCI-
52 DENT INVOLVING A BREACH OF SECURITY, AND MANDATORY POST-INCIDENT REVIEW
53 OF EVENTS AND ACTIONS TAKEN, IF ANY, TO MAKE CHANGES IN BUSINESS PRAC-
54 TICES RELATING TO PROTECTION OF PERSONAL INFORMATION.

1 [3.]4. Any person or business which maintains computerized data which
2 includes private information which such person or business does not own
3 shall:

4 (A) INCLUDE IN ITS WRITTEN, COMPREHENSIVE INFORMATION SECURITY PROGRAM
5 THE ESTABLISHMENT AND MAINTENANCE OF A SECURITY SYSTEM COVERING ITS
6 COMPUTERS, INCLUDING ANY WIRELESS SYSTEM, THAT, AT A MINIMUM, AND TO THE
7 EXTENT TECHNICALLY FEASIBLE, INCLUDE THE FOLLOWING ELEMENTS:

8 (I) SECURE USER AUTHENTICATION PROTOCOLS INCLUDING:

9 (1) CONTROL OF USER IDENTIFICATIONS AND OTHER IDENTIFIERS;

10 (2) A REASONABLY SECURE METHOD OF ASSIGNING AND SELECTING PASSWORDS,
11 OR USE OF UNIQUE IDENTIFIER TECHNOLOGIES, SUCH AS BIOMETRICS OR TOKEN
12 DEVICES;

13 (3) CONTROL OF DATA SECURITY PASSWORDS TO ENSURE THAT SUCH PASSWORDS
14 ARE KEPT IN A LOCATION AND/OR FORMAT THAT DOES NOT COMPROMISE THE SECU-
15 RITY OF THE DATA THEY PROTECT;

16 (4) RESTRICTING ACCESS TO ACTIVE USERS AND ACTIVE USER ACCOUNTS ONLY;
17 AND

18 (5) BLOCKING ACCESS TO USER IDENTIFICATION AFTER MULTIPLE UNSUCCESSFUL
19 ATTEMPTS TO GAIN ACCESS OR THE LIMITATION PLACED ON ACCESS FOR THE
20 PARTICULAR SYSTEM;

21 (II) SECURE ACCESS CONTROL MEASURES THAT:

22 (1) RESTRICT ACCESS TO RECORDS AND FILES CONTAINING PERSONAL INFORMA-
23 TION TO THOSE WHO NEED SUCH INFORMATION TO PERFORM THEIR JOB DUTIES; AND

24 (2) ASSIGN UNIQUE IDENTIFICATIONS PLUS PASSWORDS, WHICH ARE NOT
25 VENDOR-SUPPLIED DEFAULT PASSWORDS, TO EACH PERSON WITH COMPUTER ACCESS
26 THAT ARE REASONABLY DESIGNED TO MAINTAIN THE INTEGRITY OF THE SECURITY
27 OF THE ACCESS CONTROLS;

28 (III) ENCRYPTION OF ALL TRANSMITTED RECORDS AND FILES CONTAINING
29 PERSONAL INFORMATION THAT WILL TRAVEL ACROSS PUBLIC NETWORKS, AND
30 ENCRYPTION OF ALL DATA CONTAINING PERSONAL INFORMATION TO BE TRANSMITTED
31 WIRELESSLY;

32 (IV) REASONABLE MONITORING OF SYSTEMS FOR UNAUTHORIZED USE OF OR
33 ACCESS TO PERSONAL INFORMATION;

34 (V) ENCRYPTION OF ALL PERSONAL INFORMATION STORED ON LAPTOPS OR OTHER
35 PORTABLE DEVICES;

36 (VI) FOR FILES CONTAINING PERSONAL INFORMATION ON A SYSTEM THAT IS
37 CONNECTED TO THE INTERNET, FIREWALL PROTECTION AND OPERATING SYSTEM
38 SECURITY PATCHES REASONABLY DESIGNED TO MAINTAIN THE INTEGRITY OF THE
39 PERSONAL INFORMATION;

40 (VII) SYSTEM SECURITY AGENT SOFTWARE WHICH MUST INCLUDE MALWARE
41 PROTECTION AND VIRUS DEFINITIONS, OR A VERSION OF SUCH SOFTWARE THAT CAN
42 STILL BE SUPPORTED WITH UP-TO-DATE PATCHES AND VIRUS DEFINITIONS, AND IS
43 SET TO RECEIVE THE MOST CURRENT SECURITY UPDATES ON A REGULAR BASIS; AND

44 (VIII) EDUCATION AND TRAINING OF EMPLOYEES ON THE PROPER USE OF THE
45 COMPUTER SECURITY SYSTEM AND THE IMPORTANCE OF PERSONAL INFORMATION
46 SECURITY.

47 (B) notify the owner or licensee of the information of any breach of
48 the security of the system immediately following discovery, if the
49 private information was, or is reasonably believed to have been,
50 acquired by a person without valid authorization.

51 [4.] 5. The notification required by this section may be delayed if a
52 law enforcement agency determines that such notification impedes a crim-
53 inal investigation. The notification required by this section shall be
54 made after such law enforcement agency determines that such notification
55 does not compromise such investigation.

1 [5.] 6. The notice required by this section shall be directly provided
2 to the affected persons by one of the following methods:

3 (a) written notice;

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

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

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

19 (1) e-mail notice when such business has an e-mail address for the
20 subject persons;

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

23 (3) notification to major statewide media.

24 [6.] 7. (a) whenever the attorney general shall believe from evidence
25 satisfactory to him that there is a violation of this article he may
26 bring an action in the name and on behalf of the people of the state of
27 New York, in a court of justice having jurisdiction to issue an injunc-
28 tion, to enjoin and restrain the continuation of such violation. In
29 such action, preliminary relief may be granted under article sixty-three
30 of the civil practice law and rules. In such action the court may award
31 damages for actual costs or losses incurred by a person entitled to
32 notice pursuant to this article, if notification was not provided to
33 such person pursuant to this article, including consequential financial
34 losses. Whenever the court shall determine in such action that a person
35 or business violated this article knowingly or recklessly, the court may
36 impose a civil penalty of the greater of five thousand dollars or up to
37 ten dollars per instance of failed notification, provided that the
38 latter amount shall not exceed one hundred fifty thousand dollars.

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

41 (c) no action may be brought under the provisions of this section
42 unless such action is commenced within two years immediately after the
43 date of the act complained of or the date of discovery of such act.

44 [7.] 8. Regardless of the method by which notice is provided, such
45 notice shall include contact information for the person or business
46 making the notification and a description of the categories of informa-
47 tion that were, or are reasonably believed to have been, acquired by a
48 person without valid authorization, including specification of which of
49 the elements of personal information and private information were, or
50 are reasonably believed to have been, so acquired.

51 [8.] 9. (a) In the event that any New York residents are to be noti-
52 fied, the person or business shall notify the state attorney general,
53 the department of state and the division of state police as to the
54 timing, content and distribution of the notices and approximate number
55 of affected persons. Such notice shall be made without delaying notice
56 to affected New York residents.

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

6 [9.] 10. The provisions of this section shall be exclusive and shall
7 preempt any provisions of local law, ordinance or code, and no locality
8 shall impose requirements that are inconsistent with or more restrictive
9 than those set forth in this section.

10 S 2. This act shall take effect immediately; provided, however, that
11 the provisions of this act shall apply to any person or business who
12 owns or licenses personal information about a resident of New York with-
13 in eighteen months after such effective date, provided, further, that
14 any person or business may come into compliance before such effective
15 date.