STATE OF NEW YORK

_____

6933--A

2017-2018 Regular Sessions

IN SENATE

November 1, 2017
_____

Introduced by Sen. CARLUCCI -- read twice and ordered printed, and when
printed to be committed to the Committee on Rules -- recommitted to
the Committee on Consumer Protection in accordance with Senate Rule 6,
sec. 8 -- 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 Assem-
bly, do enact as follows:**

1   Section 1. This act shall be known and may be cited as the "New York
2 Data Security Act".
3   § 2. The article heading of article 39-F of the general business law,
4 as added by chapter 442 of the laws of 2005, is amended to read as
5 follows:
6   NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE
7   INFORMATION**; DATA SECURITY PROTECTIONS**
8   § 3. Subdivisions 1, 2, 3, 5, 6, 7 and 8 of section 899-aa of the
9 general business law, as added by chapter 442 of the laws of 2005, para-
10 graph (c) of subdivision 1, paragraph (a) of subdivision 6 and subdivi-
11 sion 8 as amended by chapter 491 of the laws of 2005 and paragraph (a)
12 of subdivision 8 as amended by section 6 of part N of chapter 55 of the
13 laws of 2013, are amended and a new subdivision 5-a is added to read as
14 follows:
15   1. As used in this section, the following terms shall have the follow-
16 ing meanings:
17   (a) "Personal information" shall mean any information concerning a
18 natural person which, because of name, number, personal mark, or other
19 identifier, can be used to identify such natural person;
20   (b) "Private information" shall mean **either: (i)** personal information
21 consisting of any information in combination with any one or more of the
22 following data elements, when either the personal information or the

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

 1 data element is not encrypted, or encrypted with an encryption key that
 2 has also been **accessed or** acquired:
 3   (1) social security number;
 4   (2) driver's license number or non-driver identification card number;
 5 [~~or~~]
 6   (3) account number, credit or debit card number, in combination with
 7 any required security code, access code, [~~or~~] password **or other informa-**
 8 **tion** that would permit access to an individual's financial account;
 9   **(4) account number, credit or debit card number, if circumstances**
10 **exist wherein such number could be used to access an individual's finan-**
11 **cial account without additional identifying information, security code,**
12 **access code, or password; or**
13   **(5) biometric information, meaning data generated by automatic meas-**
14 **urements of an individual's physical characteristics, which are used to**
15 **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 held by a "covered**
20 **entity" as defined in the health insurance portability and accountabil-**
21 **ity act of 1996 (45 C.F.R. pts. 160, 162, 164), as amended from time to**
22 **time.**
23   "Private information" does not include publicly available information
24 which is lawfully made available to the general public from federal,
25 state, or local government records.
26   (c) "Breach of the security of the system" shall mean unauthorized
27 **access to or** acquisition **of,** or **access to or** acquisition without valid
28 authorization**,** of computerized data that compromises the security,
29 confidentiality, or integrity of [~~personal~~] **private** information main-
30 tained by a business. Good faith **access to, or** acquisition of
31 [~~personal~~]**, private** information by an employee or agent of the business
32 for the purposes of the business is not a breach of the security of the
33 system, provided that the private information is not used or subject to
34 unauthorized disclosure.
35   **In determining whether information has been accessed, or is reasonably**
36 **believed to have been accessed, by an unauthorized person or a person**
37 **without valid authorization, such business may consider, among other**
38 **factors, indications that the information was viewed, communicated with,**
39 **used, or altered by a person without valid authorization or by an unau-**
40 **thorized person.**
41   In determining whether information has been acquired, or is reasonably
42 believed to have been acquired, by an unauthorized person or a person
43 without valid authorization, such business may consider the following
44 factors, among others:
45   (1) indications that the information is in the physical possession and
46 control of **a person without valid authorization or by** an unauthorized
47 person, such as a lost or stolen computer or other device containing
48 information; or
49   (2) indications that the information has been downloaded or copied; or
50   (3) indications that the information was used by **a person without**
51 **valid authorization or** an unauthorized person, such as fraudulent
52 accounts opened or instances of identity theft reported.
53   (d) "Consumer reporting agency" shall mean any person which, for mone-
54 tary fees, dues, or on a cooperative nonprofit basis, regularly engages
55 in whole or in part in the practice of assembling or evaluating consumer
56 credit information or other information on consumers for the purpose of

 1 furnishing consumer reports to third parties, and which uses any means
 2 or facility of interstate commerce for the purpose of preparing or
 3 furnishing consumer reports. A list of consumer reporting agencies shall
 4 be compiled by the state attorney general and furnished upon request to
 5 any person or business required to make a notification under subdivision
 6 two of this section.
 7 **(e) "Credit card" shall mean any card or other credit device issued by**
 8 **a financial institution to a consumer for the purpose of providing**
 9 **money, property, labor or services on credit.**
10 **(f) "Debit card" shall mean any card or other device issued by a**
11 **financial institution to a consumer for use in initiating an electronic**
12 **fund transfer from the account of the consumer at such financial insti-**
13 **tution, for the purpose of transferring money between accounts or**
14 **obtaining money, property, labor or services.**
15   2. Any person or business which [~~conducts business in New York state,~~
16 ~~and which~~] owns or licenses computerized data which includes private
17 information shall disclose any breach of the security of the system
18 following discovery or notification of the breach in the security of the
19 system to any resident of New York state whose private information was,
20 or is reasonably believed to have been, **accessed or** acquired by a person
21 without valid authorization **or by an unauthorized person**. The disclo-
22 sure shall be made in the most expedient time possible and without
23 unreasonable delay, consistent with the legitimate needs of law enforce-
24 ment, as provided in subdivision four of this section, or any measures
25 necessary to determine the scope of the breach and restore the [~~reason-~~
26 ~~able~~] integrity of the system.
27   3. Any person or business which maintains computerized data which
28 includes private information which such person or business does not own
29 shall notify the owner or licensee of the information of any breach of
30 the security of the system immediately following discovery, if the
31 private information was, or is reasonably believed to have been,
32 acquired by a person without valid authorization **or by an unauthorized**
33 **person**.
34   5. The notice required by this section shall be directly provided to
35 the affected persons by one of the following methods:
36   (a) written notice;
37   (b) electronic notice, provided that the person to whom notice is
38 required has expressly consented to receiving said notice in electronic
39 form and a log of each such notification is kept by the person or busi-
40 ness who notifies affected persons in such form; provided further,
41 however, that in no case shall any person or business require a person
42 to consent to accepting said notice in said form as a condition of
43 establishing any business relationship or engaging in any transaction.
44   (c) telephone notification provided that a log of each such notifica-
45 tion is kept by the person or business who notifies affected persons; or
46   (d) substitute notice, if a business demonstrates to the state attor-
47 ney general that the cost of providing notice would exceed two hundred
48 fifty thousand dollars, or that the affected class of subject persons to
49 be notified exceeds five hundred thousand, or such business does not
50 have sufficient contact information. Substitute notice shall consist of
51 all of the following:
52   (1) e-mail notice when such business has an e-mail address for the
53 subject persons**, except if the breached information includes an e-mail**
54 **address in combination with a password or security question and answer**
55 **that would permit access to the online account, in which case the person**
56 **or business shall instead provide clear and conspicuous notice delivered**

 1 **to the consumer online when the consumer is connected to the online**
 2 **account from an internet protocol address or from an online location**
 3 **which the person or business knows the consumer customarily uses to**
 4 **access the online account**;
 5 (2) conspicuous posting of the notice on such business's web site
 6 page, if such business maintains one; and
 7 (3) notification to major statewide media.
 8 **5-a. Any credit or debit card issuer that issues a new credit or debit**
 9 **card as a result of a breach of the security of the system pursuant to**
10 **paragraph (c) of subdivision one of this section, shall provide the**
11 **consumer notice that the issuance of the replacement credit or debit**
12 **card is due to a potential compromise of the prior card absent any**
13 **evidence of actual or potential unauthorized use of such credit or debit**
14 **card or other circumstances precipitating the issuance of a replacement**
15 **card.**
16 6. (a) whenever the attorney general shall believe from evidence
17 satisfactory to him that there is a violation of this article he may
18 bring an action in the name and on behalf of the people of the state of
19 New York, in a court of justice having jurisdiction to issue an injunc-
20 tion, to enjoin and restrain the continuation of such violation. In
21 such action, preliminary relief may be granted under article sixty-three
22 of the civil practice law and rules. In such action the court may award
23 damages for actual costs or losses incurred by a person entitled to
24 notice pursuant to this article, if notification was not provided to
25 such person pursuant to this article, including consequential financial
26 losses. Whenever the court shall determine in such action that a person
27 or business violated this article knowingly or recklessly, the court may
28 impose a civil penalty of the greater of five thousand dollars or up to
29 [~~ten~~] **twenty** dollars per instance of failed notification, provided that
30 the latter amount shall not exceed [~~one~~] **two** hundred fifty thousand
31 dollars.
32 (b) the remedies provided by this section shall be in addition to any
33 other lawful remedy available.
34 (c) no action may be brought under the provisions of this section
35 unless such action is commenced within [~~two~~] **three** years [~~immediately~~]
36 after **either** the date [~~of the act complained of or the date of discovery~~
37 ~~of such act~~] **on which the attorney general became aware of the**
38 **violation, or the date of notice sent pursuant to paragraph (a) of**
39 **subdivision eight of this section, whichever occurs first**.
40 7. Regardless of the method by which notice is provided, such notice
41 shall include contact information for the person or business making the
42 notification**, the telephone numbers and websites of the relevant state**
43 **and federal agencies that provide information regarding security breach**
44 **response and identity theft prevention and protection information,** and a
45 description of the categories of information that were, or are reason-
46 ably believed to have been, **accessed or** acquired by a person without
47 valid authorization **or by an unauthorized person**, including specifica-
48 tion of which of the elements of personal information and private infor-
49 mation were, or are reasonably believed to have been, so **accessed or**
50 acquired.
51 8. (a) In the event that any New York residents are to be notified,
52 the person or business shall notify the state attorney general, the
53 department of state and the [~~division of state police~~] **office of infor-**
54 **mation technology services** as to the timing, content and distribution of
55 the notices and approximate number of affected persons **and shall provide**
56 **a copy of the template of the notice sent to affected persons**.   Such

1 notice shall be made without delaying notice to affected New York resi-
2 dents.
3   (b) In the event that more than five thousand New York residents are
4 to be notified at one time, the person or business shall also notify
5 consumer reporting agencies as to the timing, content and distribution
6 of the notices and approximate number of affected persons. Such notice
7 shall be made without delaying notice to affected New York residents.
8   § 4. The general business law is amended by adding a new section 899-
9 bb to read as follows:
10   § 899-bb. Data security protections. 1. Definitions. (a) "Compliant
11 regulated entity" shall mean any person or business that is subject to,
12 and in compliance with, any of the following data security requirements:
13   (i) regulations promulgated pursuant to Title V of the federal Gramm-
14 Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;
15   (ii) regulations implementing the Health Insurance Portability and
16 Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended
17 from time to time, and the Health Information Technology for Economic
18 and Clinical Health Act, as amended from time to time;
19   (iii) part five hundred of title twenty-three of the official compila-
20 tion of codes, rules and regulations of the state of New York, as
21 amended from time to time; or
22   (iv) any other data security rules and regulations of, and the stat-
23 utes administered by, any official department, division, commission or
24 agency of the federal or New York State government as such rules, regu-
25 lations or statutes are interpreted by such department, division,
26 commission or agency or by the federal or New York State courts.
27   (b) "Certified compliant entity" shall mean any person or business
28 that:
29   (i) is compliant with any of the data security requirements in para-
30 graph (a) of this subdivision or with the most up to date version of the
31 International Standards Organization Standard 27002 or with the most up
32 to date version of National Institute of Standards and Technology
33 Special Publication 800-53, as it relates to the protection of electron-
34 ic private information; and
35   (ii) has such compliance certified annually by an independent, third-
36 party assessment organization that is authorized to provide such certif-
37 ications by the official department, division, commissioner or agency or
38 standards body that promulgates the data security regulations or stand-
39 ards being certified.
40   (c) "Private information" shall have the same meaning as defined in
41 section eight hundred ninety-nine-aa of this article.
42   (d) "Small business" shall mean any person or business with (i) fewer
43 than fifty employees, including any independent contractors, of the
44 business; (ii) less than three million dollars in gross annual revenue
45 in each of the last three fiscal years; or (iii) less than five million
46 dollars in year-end total assets, calculated in accordance with general-
47 ly accepted accounting principles.
48   2. Reasonable security. (a) Any person or business that owns or
49 licenses computerized data which includes private information of a resi-
50 dent of New York shall develop, implement and maintain reasonable safe-
51 guards to protect the security, confidentiality and integrity of the
52 private information including, but not limited to, disposal of data.
53   (b) Small businesses subject to the requirements of paragraph (a) of
54 this subdivision shall be deemed to be in compliance with such require-
55 ment if they implement and maintain reasonable safeguards that are
56 appropriate to the size and complexity of the small business to protect

1 the security, confidentiality and integrity of the private information
2 including, but not limited to, disposal of data.
3   (c) A person or business shall be deemed to be in compliance with
4 paragraphs (a) and (b) of this subdivision if it either:
5   (i) is a compliant regulated entity as defined in subdivision one of
6 this section;
7   (ii) is a certified compliant entity as defined in subdivision one of
8 this section; or
9   (iii) implements a data security program that includes the following:
10   (A) administrative safeguards such as the following, in which the
11 person or business:
12   (1) designates one or more employees to coordinate the security
13 program;
14   (2) identifies reasonably foreseeable internal and external risks;
15   (3) assesses the sufficiency of safeguards in place to control the
16 identified risks;
17   (4) trains and manages employees in the security program practices and
18 procedures;
19   (5) selects service providers capable of maintaining appropriate safe-
20 guards, and requires those safeguards by contract; and
21   (6) adjusts the security program in light of business changes or new
22 circumstances; and
23   (B) technical safeguards such as the following, in which the person or
24 business:
25   (1) assesses risks in network and software design;
26   (2) assesses risks in information processing, transmission and stor-
27 age;
28   (3) detects, prevents and responds to attacks or system failures; and
29   (4) regularly tests and monitors the effectiveness of key controls,
30 systems and procedures; and
31   (C) physical safeguards such as the following, in which the person or
32 business:
33   (1) assesses risks of information storage and disposal;
34   (2) detects, prevents and responds to intrusions;
35   (3) protects against unauthorized access to or use of private informa-
36 tion during or after the collection, transportation and destruction or
37 disposal of the information; and
38   (4) disposes of private information within a reasonable amount of time
39 after it is no longer needed for business purposes by erasing electronic
40 media so that the information cannot be read or reconstructed.
41   (d) Any person or business required to comply with paragraph (a) or
42 (b) of this subdivision that fails to comply with such subdivisions
43 shall be deemed to have violated section three hundred forty-nine of
44 this chapter, and the attorney general may bring an action in the name
45 and on behalf of the people of the state of New York to enjoin such
46 violations and to obtain civil penalties under section three hundred
47 fifty-d of this chapter.
48   (e) Nothing in this section shall create a private right of action.
49   3. Safe harbor for certified compliant entities. A certified compli-
50 ant entity shall not be subject to an enforcement action by the attorney
51 general pursuant to subdivision two of this section if:
52   (a) it provides copies of its certifications of compliance to the
53 attorney general; and
54   (b) there is no evidence of willful misconduct, bad faith or gross
55 negligence.

 1   § 5. Paragraph (a) of subdivision 1 and subdivisions 2, 3, 6, 7 and 8
 2 of section 208 of the state technology law, paragraph (a) of subdivision
 3 1 and subdivisions 3 and 8 as added by chapter 442 of the laws of 2005,
 4 subdivision 2 and paragraph (a) of subdivision 7 as amended by section 5
 5 of part N of chapter 55 of the laws of 2013 and subdivisions 6 and 7 as
 6 amended by chapter 491 of the laws of 2005, are amended to read as
 7 follows:
 8   (a) "Private information" shall mean **either: (i)** personal information
 9 **consisting of any information** in combination with any one or more of the
10 following data elements, when either the personal information or the
11 data element is not encrypted or encrypted with an encryption key that
12 has also been **accessed or** acquired:
13   (1) social security number;
14   (2) driver's license number or non-driver identification card number;
15 [~~or~~]
16   (3) account number, **or** credit or debit card number, in combination
17 with any required **identifying information,** security code, access code,
18 or password which would permit access to an individual's financial
19 account**;**
20   **(4) account number, or credit or debit card number, if circumstances**
21 **exist wherein such number could be used to access to an individual's**
22 **financial account without additional identifying information, security**
23 **code, access code, or password; or**
24   **(5) biometric information, meaning data generated by automatic meas-**
25 **urements of an individual's physical characteristics, which are used to**
26 **authenticate the individual's identity;**
27   **(ii) a user name or e-mail address in combination with a password or**
28 **security question and answer that would permit access to an online**
29 **account; or**
30   **(iii) any unsecured protected health information held by a "covered**
31 **entity" as defined in the health insurance portability and accountabil-**
32 **ity act of 1996 (45 C.F.R. pts. 160, 162, 164), as amended from time to**
33 **time**.
34   "Private information" does not include publicly available information
35 that is lawfully made available to the general public from federal,
36 state, or local government records.
37   2. Any state entity that owns or licenses computerized data that
38 includes private information shall disclose any breach of the security
39 of the system following discovery or notification of the breach in the
40 security of the system to any resident of New York state whose private
41 information was, or is reasonably believed to have been, **accessed or**
42 acquired by a person without valid authorization **or an unauthorized**
43 **person**.   The disclosure shall be made in the most expedient time possi-
44 ble and without unreasonable delay, consistent with the legitimate needs
45 of law enforcement, as provided in subdivision four of this section, or
46 any measures necessary to determine the scope of the breach and restore
47 the [~~reasonable~~] integrity of the data system. The state entity shall
48 consult with the state office of information technology services to
49 determine the scope of the breach and restoration measures. **Within nine-**
50 **ty days of the notice of the breach, the office of information technolo-**
51 **gy services shall deliver a report on the scope of the breach and recom-**
52 **mendations to restore and improve the security of the system to the**
53 **state entity.**
54   3. Any state entity that maintains computerized data that includes
55 private information which such agency does not own shall notify the
56 owner or licensee of the information of any breach of the security of

1 the system immediately following discovery, if the private information
2 was, or is reasonably believed to have been, acquired by a person with-
3 out valid authorization **or an unauthorized person**.
4   6. Regardless of the method by which notice is provided, such notice
5 shall include contact information for the state entity making the
6 notification**, the telephone numbers and websites of the relevant state**
7 **and federal agencies that provide information regarding security breach**
8 **response and identity theft prevention and protection information** and a
9 description of the categories of information that were, or are reason-
10 ably believed to have been, **accessed or** acquired by a person without
11 valid authorization **or an unauthorized person**, including specification
12 of which of the elements of personal information and private information
13 were, or are reasonably believed to have been, so **accessed or** acquired.
14   7. (a) In the event that any New York residents are to be notified,
15 the state entity shall notify the state attorney general, the department
16 of state and the state office of information technology services as to
17 the timing, content and distribution of the notices and approximate
18 number of affected persons **and provide a copy of the template of the**
19 **notice sent to affected persons**. Such notice shall be made without
20 delaying notice to affected New York residents.
21   (b) In the event that more than five thousand New York residents are
22 to be notified at one time, the state entity shall also notify consumer
23 reporting agencies as to the timing, content and distribution of the
24 notices and approximate number of affected persons. Such notice shall be
25 made without delaying notice to affected New York residents.
26   8. **The state office of information technology services shall develop,**
27 **update and provide regular training to all state entities relating to**
28 **best practices for the prevention of a breach of the security of the**
29 **system.**
30   **9.** Any entity listed in subparagraph two of paragraph (c) of subdivi-
31 sion one of this section shall adopt a notification policy no more than
32 one hundred twenty days after the effective date of this section. Such
33 entity may develop a notification policy which is consistent with this
34 section or alternatively shall adopt a local law which is consistent
35 with this section.
36   § 6. This act shall take effect on the first of January next succeed-
37 ing the date on which it shall have become a law.