

STATE OF NEW YORK

6933--B

2017-2018 Regular Sessions

IN SENATE

November 1, 2017

Introduced by Sens. CARLUCCI, KAMINSKY -- 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 -- reported favorably from said committee and committed to the Committee on Finance -- 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. This act shall be known and may be cited as the "Stop Hacks
2 and Improve Electronic Data Security Act (SHIELD 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 to read as follows:

14 1. As used in this section, the following terms shall have the follow-
15 ing meanings:

16 (a) "Personal information" shall mean any information concerning a
17 natural person which, because of name, number, personal mark, or other
18 identifier, can be used to identify such natural person;

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

LBD13619-10-8

1 (b) "Private information" shall mean either: (i) personal information
2 consisting of any information in combination with any one or more of the
3 following data elements, when either the data element or the combination
4 of personal information [~~or~~] plus the data element is not encrypted, or
5 is encrypted with an encryption key that has also been accessed or
6 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 or other informa-
12 tion that would permit access to an individual's financial account;

13 (4) account number, credit or debit card number, if circumstances
14 exist wherein such number could be used to access an individual's finan-
15 cial account without additional identifying information, security code,
16 access code, or password; or

17 (5) biometric information, meaning data generated by electronic meas-
18 urements of an individual's unique physical characteristics, such as a
19 fingerprint, voice print, retina or iris image, or other unique physical
20 representation or digital representation of biometric data which are
21 used to authenticate or ascertain the individual's identity;

22 (ii) a user name or e-mail address in combination with a password or
23 security question and answer that would permit access to an online
24 account; or

25 (iii) any unsecured protected health information held by a "covered
26 entity" as defined in the health insurance portability and accountabil-
27 ity act of 1996 (45 C.F.R. pts. 160, 162, 164), as amended from time to
28 time.

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

32 (c) "Breach of the security of the system" shall mean unauthorized
33 access to or acquisition of, or access to or acquisition without valid
34 authorization, of computerized data that compromises the security,
35 confidentiality, or integrity of [~~personal~~] private information main-
36 tained by a business. Good faith access to, or acquisition of
37 [~~personal~~], private information by an employee or agent of the business
38 for the purposes of the business is not a breach of the security of the
39 system, provided that the private information is not used or subject to
40 unauthorized disclosure.

41 In determining whether information has been accessed, or is reasonably
42 believed to have been accessed, by an unauthorized person or a person
43 without valid authorization, such business may consider, among other
44 factors, indications that the information was viewed, communicated with,
45 used, or altered by a person without valid authorization or by an unau-
46 thorized person.

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

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

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

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

4 (d) "Consumer reporting agency" shall mean any person which, for mone-
5 tary fees, dues, or on a cooperative nonprofit basis, regularly engages
6 in whole or in part in the practice of assembling or evaluating consumer
7 credit information or other information on consumers for the purpose of
8 furnishing consumer reports to third parties, and which uses any means
9 or facility of interstate commerce for the purpose of preparing or
10 furnishing consumer reports. A list of consumer reporting agencies shall
11 be compiled by the state attorney general and furnished upon request to
12 any person or business required to make a notification under subdivision
13 two of this section.

14 2. Any person or business which [~~conducts business in New York state,~~
15 ~~and which~~] owns or licenses computerized data which includes private
16 information shall disclose any breach of the security of the system
17 following discovery or notification of the breach in the security of the
18 system to any resident of New York state whose private information was,
19 or is reasonably believed to have been, accessed or acquired by a person
20 without valid authorization. The disclosure shall be made in the most
21 expedient time possible and without unreasonable delay, consistent with
22 the legitimate needs of law enforcement, as provided in subdivision four
23 of this section, or any measures necessary to determine the scope of the
24 breach and restore the [~~reasonable~~] integrity of the system.

25 (a) Notice to affected persons under this section is not required if
26 the exposure of private information was an inadvertent disclosure by
27 persons authorized to access private information, and the person or
28 business reasonably determines such exposure will not likely result in
29 misuse of such information, or financial or emotional harm to the
30 affected persons. Such a determination must be documented in writing and
31 maintained for at least five years. The person or business shall provide
32 the written determination to the state attorney general within ten days
33 after the determination.

34 (b) If notice of the breach of the security of the system is made to
35 affected persons pursuant to the breach notification requirements under
36 any of the following laws, nothing in this section shall require any
37 additional notice to those affected persons, but notice still shall be
38 provided to the state attorney general, the department of state and the
39 office of information technology services pursuant to paragraph (a) of
40 subdivision eight of this section and to consumer reporting agencies
41 pursuant to paragraph (b) of subdivision eight of this section:

42 (i) regulations promulgated pursuant to Title V of the federal Gramm-
43 Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

44 (ii) regulations implementing the Health Insurance Portability and
45 Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended
46 from time to time, and the Health Information Technology for Economic
47 and Clinical Health Act, as amended from time to time;

48 (iii) part five hundred of title twenty-three of the official compila-
49 tion of codes, rules and regulations of the state of New York, as
50 amended from time to time; or

51 (iv) any other data security rules and regulations of, and the stat-
52 utes administered by, any official department, division, commission or
53 agency of the federal or New York state government as such rules, regu-
54 lations or statutes are interpreted by such department, division,
55 commission or agency or by the federal or New York state courts.

1 3. Any person or business which maintains computerized data which
2 includes private information which such person or business does not own
3 shall notify the owner or licensee of the information of any breach of
4 the security of the system immediately following discovery, if the
5 private information was, or is reasonably believed to have been,
6 acquired by a person without valid authorization.

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

9 (a) written notice;

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

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

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

25 (1) e-mail notice when such business has an e-mail address for the
26 subject persons, except if the breached information includes an e-mail
27 address in combination with a password or security question and answer
28 that would permit access to the online account, in which case the person
29 or business shall instead provide clear and conspicuous notice delivered
30 to the consumer online when the consumer is connected to the online
31 account from an internet protocol address or from an online location
32 which the person or business knows the consumer customarily uses to
33 access the online account;

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

36 (3) notification to major statewide media.

37 6. (a) whenever the attorney general shall believe from evidence
38 satisfactory to him or her that there is a violation of this article he
39 or she may bring an action in the name and on behalf of the people of
40 the state of New York, in a court of justice having jurisdiction to
41 issue an injunction, to enjoin and restrain the continuation of such
42 violation. In such action, preliminary relief may be granted under
43 article sixty-three of the civil practice law and rules. In such action
44 the court may award damages for actual costs or losses incurred by a
45 person entitled to notice pursuant to this article, if notification was
46 not provided to such person pursuant to this article, including conse-
47 quential financial losses. Whenever the court shall determine in such
48 action that a person or business violated this article knowingly or
49 recklessly, the court may impose a civil penalty of the greater of five
50 thousand dollars or up to [~~ten~~] twenty dollars per instance of failed
51 notification, provided that the latter amount shall not exceed [~~one~~] two
52 hundred fifty thousand dollars.

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

55 (c) no action may be brought under the provisions of this section
56 unless such action is commenced within [~~two~~] three years [~~immediately~~]

1 after either the date [~~of the act complained of or the date of discovery~~
2 ~~of such act~~] on which the attorney general became aware of the
3 violation, or the date of notice sent pursuant to paragraph (a) of
4 subdivision eight of this section, whichever occurs first.

5 7. Regardless of the method by which notice is provided, such notice
6 shall include contact information for the person or business making the
7 notification, the telephone numbers and websites of the relevant state
8 and federal agencies that provide information regarding security breach
9 response and identity theft prevention and protection information, and a
10 description of the categories of information that were, or are reason-
11 ably believed to have been, accessed or acquired by a person without
12 valid authorization, including specification of which of the elements of
13 personal information and private information were, or are reasonably
14 believed to have been, so accessed or acquired.

15 8. (a) In the event that any New York residents are to be notified,
16 the person or business shall notify the state attorney general, the
17 department of state and the [~~division of state police~~] office of infor-
18 mation technology services as to the timing, content and distribution of
19 the notices and approximate number of affected persons and shall provide
20 a copy of the template of the notice sent to affected persons. Such
21 notice shall be made without delaying notice to affected New York resi-
22 dents.

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

28 § 4. The general business law is amended by adding a new section 899-
29 bb to read as follows:

30 § 899-bb. Data security protections. 1. Definitions. (a) "Compliant
31 regulated entity" shall mean any person or business that is subject to,
32 and in compliance with, any of the following data security requirements:

33 (i) regulations promulgated pursuant to Title V of the federal Gramm-
34 Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

35 (ii) regulations implementing the Health Insurance Portability and
36 Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended
37 from time to time, and the Health Information Technology for Economic
38 and Clinical Health Act, as amended from time to time;

39 (iii) part five hundred of title twenty-three of the official compila-
40 tion of codes, rules and regulations of the state of New York, as
41 amended from time to time; or

42 (iv) any other data security rules and regulations of, and the stat-
43 utes administered by, any official department, division, commission or
44 agency of the federal or New York state government as such rules, regu-
45 lations or statutes are interpreted by such department, division,
46 commission or agency or by the federal or New York state courts.

47 (b) "Private information" shall have the same meaning as defined in
48 section eight hundred ninety-nine-aa of this article.

49 (c) "Small business" shall mean any person or business with (i) fewer
50 than fifty employees; (ii) less than three million dollars in gross
51 annual revenue in each of the last three fiscal years; or (iii) less
52 than five million dollars in year-end total assets, calculated in
53 accordance with generally accepted accounting principles.

54 2. Reasonable security requirement. (a) Any person or business that
55 owns or licenses computerized data which includes private information of
56 a resident of New York shall develop, implement and maintain reasonable

1 safeguards to protect the security, confidentiality and integrity of the
2 private information including, but not limited to, disposal of data.

3 (b) A person or business shall be deemed to be in compliance with
4 paragraph (a) of this subdivision if it either:

5 (i) is a compliant regulated entity as defined in subdivision one of
6 this section; or

7 (ii) implements a data security program that includes the following:

8 (A) reasonable administrative safeguards such as the following, in
9 which the person or business:

10 (1) designates one or more employees to coordinate the security
11 program;

12 (2) identifies reasonably foreseeable internal and external risks;

13 (3) assesses the sufficiency of safeguards in place to control the
14 identified risks;

15 (4) trains and manages employees in the security program practices and
16 procedures;

17 (5) selects service providers capable of maintaining appropriate safe-
18 guards, and requires those safeguards by contract; and

19 (6) adjusts the security program in light of business changes or new
20 circumstances; and

21 (B) reasonable technical safeguards such as the following, in which
22 the person or business:

23 (1) assesses risks in network and software design;

24 (2) assesses risks in information processing, transmission and stor-
25 age;

26 (3) detects, prevents and responds to attacks or system failures; and

27 (4) regularly tests and monitors the effectiveness of key controls,
28 systems and procedures; and

29 (C) reasonable physical safeguards such as the following, in which the
30 person or business:

31 (1) assesses risks of information storage and disposal;

32 (2) detects, prevents and responds to intrusions;

33 (3) protects against unauthorized access to or use of private informa-
34 tion during or after the collection, transportation and destruction or
35 disposal of the information; and

36 (4) disposes of private information within a reasonable amount of time
37 after it is no longer needed for business purposes by erasing electronic
38 media so that the information cannot be read or reconstructed.

39 (c) A small business as defined in paragraph (c) of subdivision one of
40 this section complies with subparagraph (ii) of paragraph (b) of subdi-
41 vision two of this section if the small business's security program
42 contains reasonable administrative, technical and physical safeguards
43 that are appropriate for the size and complexity of the small business,
44 the nature and scope of the small business's activities, and the sensi-
45 tivity of the personal information the small business collects from or
46 about consumers.

47 (d) Any person or business that fails to comply with this subdivision
48 shall be deemed to have violated section three hundred forty-nine of
49 this chapter, and the attorney general may bring an action in the name
50 and on behalf of the people of the state of New York to enjoin such
51 violations and to obtain civil penalties under section three hundred
52 fifty-d of this chapter.

53 (e) Nothing in this section shall create a private right of action.

54 § 5. Paragraph (a) of subdivision 1 and subdivisions 2, 3, 6, 7 and 8
55 of section 208 of the state technology law, paragraph (a) of subdivision
56 1 and subdivisions 3 and 8 as added by chapter 442 of the laws of 2005,

1 subdivision 2 and paragraph (a) of subdivision 7 as amended by section 5
2 of part N of chapter 55 of the laws of 2013 and subdivisions 6 and 7 as
3 amended by chapter 491 of the laws of 2005, are amended to read as
4 follows:

5 (a) "Private information" shall mean either: (i) personal information
6 consisting of any information in combination with any one or more of the
7 following data elements, when either the data element or the combination
8 of personal information [~~or~~] plus the data element is not encrypted or
9 encrypted with an encryption key that has also been accessed or
10 acquired:

11 (1) social security number;

12 (2) driver's license number or non-driver identification card number;
13 [~~or~~]

14 (3) account number, or credit or debit card number, in combination
15 with any required identifying information, security code, access code,
16 or password which would permit access to an individual's financial
17 account;

18 (4) account number, or credit or debit card number, if circumstances
19 exist wherein such number could be used to access to an individual's
20 financial account without additional identifying information, security
21 code, access code, or password; or

22 (5) biometric information, meaning data generated by electronic meas-
23 urements of an individual's unique physical characteristics, such as
24 fingerprint, voice print, or retina or iris image, or other unique phys-
25 ical representation or digital representation which are used to authen-
26 ticate or ascertain 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. The disclosure shall
43 be made in the most expedient time possible and without unreasonable
44 delay, consistent with the legitimate needs of law enforcement, as
45 provided in subdivision four of this section, or any measures necessary
46 to determine the scope of the breach and restore the [~~reasonable~~] integ-
47 rity of the data system. The state entity shall consult with the state
48 office of information technology services to determine the scope of the
49 breach and restoration measures. Within ninety days of the notice of the
50 breach, the office of information technology services shall deliver a
51 report on the scope of the breach and recommendations to restore and
52 improve the security of the system to the state entity.

53 (a) Notice to affected persons under this section is not required if
54 the exposure of private information was an inadvertent disclosure by
55 persons authorized to access private information, and the state entity
56 reasonably determines such exposure will not likely result in misuse of

1 such information, or financial or emotional harm to the affected
2 persons. Such a determination must be documented in writing and main-
3 tained for at least five years. The state entity shall provide the writ-
4 ten determination to the state attorney general within ten days after
5 the determination.

6 (b) If notice of the breach of the security of the system is made to
7 affected persons pursuant to the breach notification requirements under
8 any of the following laws, nothing in this section shall require any
9 additional notice to those affected persons, but notice still shall be
10 provided to the state attorney general, the department of state and the
11 office of information technology services pursuant to paragraph (a) of
12 subdivision seven of this section and to consumer reporting agencies
13 pursuant to paragraph (b) of subdivision seven of this section:

14 (i) regulations promulgated pursuant to Title V of the federal Gramm-
15 Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

16 (ii) regulations implementing the Health Insurance Portability and
17 Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended
18 from time to time, and the Health Information Technology for Economic
19 and Clinical Health Act, as amended from time to time;

20 (iii) part five hundred of title twenty-three of the official compila-
21 tion of codes, rules and regulations of the state of New York, as
22 amended from time to time; or

23 (iv) any other data security rules and regulations of, and the stat-
24 utes administered by, any official department, division, commission or
25 agency of the federal or New York state government as such rules, regu-
26 lations or statutes are interpreted by such department, division,
27 commission or agency or by the federal or New York state courts.

28 3. Any state entity that maintains computerized data that includes
29 private information which such agency does not own shall notify the
30 owner or licensee of the information of any breach of the security of
31 the system immediately following discovery, if the private information
32 was, or is reasonably believed to have been, acquired by a person with-
33 out valid authorization.

34 6. Regardless of the method by which notice is provided, such notice
35 shall include contact information for the state entity making the
36 notification, the telephone numbers and websites of the relevant state
37 and federal agencies that provide information regarding security breach
38 response and identity theft prevention and protection information and a
39 description of the categories of information that were, or are reason-
40 ably believed to have been, accessed or acquired by a person without
41 valid authorization, including specification of which of the elements of
42 personal information and private information were, or are reasonably
43 believed to have been, so accessed or acquired.

44 7. (a) In the event that any New York residents are to be notified,
45 the state entity shall notify the state attorney general, the department
46 of state and the state office of information technology services as to
47 the timing, content and distribution of the notices and approximate
48 number of affected persons and provide a copy of the template of the
49 notice sent to affected persons. Such notice shall be made without
50 delaying notice to affected New York residents.

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

1 8. The state office of information technology services shall develop,
2 update and provide regular training to all state entities relating to
3 best practices for the prevention of a breach of the security of the
4 system.

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

11 § 6. This act shall take effect on the ninetieth day after it shall
12 have become a law; provided, however, that section four of this act
13 shall take effect on the two hundred fortieth day after it shall have
14 become a law.