STATE OF NEW YORK

_____

Cal. No. 1094

5575--B

2019-2020 Regular Sessions

IN SENATE

May 7, 2019
_____

Introduced by Sens. THOMAS, CARLUCCI, BIAGGI -- (at request of the
  Attorney General) -- read twice and ordered printed, and when printed
  to be committed to the Committee on Internet and Technology -- commit-
  tee discharged and said bill committed to the Committee on Consumer
  Protection -- committee discharged, bill amended, ordered reprinted as
  amended and recommitted to said committee -- reported favorably from
  said committee, ordered to first and second report, ordered to a third
  reading, passed by Senate and delivered to the Assembly, recalled,
  vote reconsidered, restored to third reading, amended and ordered
  reprinted, retaining its place in the order of third reading

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 "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, subdivisions 1, 2, 3, 5, 6 and 7 as added by chap-
10 ter 442 of the laws of 2005, paragraph (c) of subdivision 1, paragraph
11 (a) of subdivision 6 and subdivision 8 as amended by chapter 491 of the
12 laws of 2005 and paragraph (a) of subdivision 8 as amended by section 6
13 of part N of chapter 55 of the laws of 2013, are amended, subdivision 9
14 is renumbered subdivision 10 and a new subdivision 9 is added to read as
15 follows:
16   1. As used in this section, the following terms shall have the follow-
17 ing meanings:

                                                              LBD05343-07-9

 1   (a) "Personal information" shall mean any information concerning a
 2 natural person which, because of name, number, personal mark, or other
 3 identifier, can be used to identify such natural person;
 4   (b) "Private information" shall mean **either: (i)** personal information
 5 consisting of any information in combination with any one or more of the
 6 following data elements, when either the **data element or the combination**
 7 **of** personal information [~~or~~] **plus** the data element is not encrypted, or
 8 **is** encrypted with an encryption key that has also been **accessed or**
 9 acquired:
10   (1) social security number;
11   (2) driver's license number or non-driver identification card number;
12 [~~or~~]
13   (3) account number, credit or debit card number, in combination with
14 any required security code, access code, [~~or~~] password **or other informa-**
15 **tion** that would permit access to an individual's financial account;
16   **(4) account number, credit or debit card number, if circumstances**
17 **exist wherein such number could be used to access an individual's finan-**
18 **cial account without additional identifying information, security code,**
19 **access code, or password; or**
20   **(5) biometric information, meaning data generated by electronic meas-**
21 **urements of an individual's unique physical characteristics, such as a**
22 **fingerprint, voice print, retina or iris image, or other unique physical**
23 **representation or digital representation of biometric data which are**
24 **used to authenticate or ascertain the individual's identity; or**
25   **(ii) a user name or e-mail address in combination with a password or**
26 **security question and answer that would permit access to an online**
27 **account.**
28   "Private information" does not include publicly available information
29 which is lawfully made available to the general public from federal,
30 state, or local government records.
31   (c) "Breach of the security of the system" shall mean unauthorized
32 **access to or** acquisition **of,** or **access to or** acquisition without valid
33 authorization**,** of computerized data that compromises the security,
34 confidentiality, or integrity of [~~personal~~] **private** information main-
35 tained by a business. Good faith **access to, or** acquisition of
36 [~~personal~~]**, private** information by an employee or agent of the business
37 for the purposes of the business is not a breach of the security of the
38 system, provided that the private information is not used or subject to
39 unauthorized disclosure.
40   **In determining whether information has been accessed, or is reasonably**
41 **believed to have been accessed, by an unauthorized person or a person**
42 **without valid authorization, such business may consider, among other**
43 **factors, indications that the information was viewed, communicated with,**
44 **used, or altered by a person without valid authorization or by an unau-**
45 **thorized person.**
46   In determining whether information has been acquired, or is reasonably
47 believed to have been acquired, by an unauthorized person or a person
48 without valid authorization, such business may consider the following
49 factors, among others:
50   (1) indications that the information is in the physical possession and
51 control of an unauthorized person, such as a lost or stolen computer or
52 other device containing information; or
53   (2) indications that the information has been downloaded or copied; or
54   (3) indications that the information was used by an unauthorized
55 person, such as fraudulent accounts opened or instances of identity
56 theft reported.

 1   (d) "Consumer reporting agency" shall mean any person which, for mone-
 2 tary fees, dues, or on a cooperative nonprofit basis, regularly engages
 3 in whole or in part in the practice of assembling or evaluating consumer
 4 credit information or other information on consumers for the purpose of
 5 furnishing consumer reports to third parties, and which uses any means
 6 or facility of interstate commerce for the purpose of preparing or
 7 furnishing consumer reports. A list of consumer reporting agencies shall
 8 be compiled by the state attorney general and furnished upon request to
 9 any person or business required to make a notification under subdivision
10 two of this section.
11   2. Any person or business which [~~conducts business in New York state,~~
12 ~~and which~~] owns or licenses computerized data which includes private
13 information shall disclose any breach of the security of the system
14 following discovery or notification of the breach in the security of the
15 system to any resident of New York state whose private information was,
16 or is reasonably believed to have been, **accessed or** acquired by a person
17 without valid authorization. The disclosure shall be made in the most
18 expedient time possible and without unreasonable delay, consistent with
19 the legitimate needs of law enforcement, as provided in subdivision four
20 of this section, or any measures necessary to determine the scope of the
21 breach and restore the [~~reasonable~~] integrity of the system.
22   **(a) Notice to affected persons under this section is not required if**
23 **the exposure of private information was an inadvertent disclosure by**
24 **persons authorized to access private information, and the person or**
25 **business reasonably determines such exposure will not likely result in**
26 **misuse of such information, or financial harm to the affected persons or**
27 **emotional harm in the case of unknown disclosure of online credentials**
28 **as found in subparagraph (ii) of paragraph (b) of subdivision one of**
29 **this section. Such a determination must be documented in writing and**
30 **maintained for at least five years. If the incident affects over five**
31 **hundred residents of New York, the person or business shall provide the**
32 **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 **division of state police pursuant to paragraph (a) of subdivision eight**
40 **of this section and to consumer reporting agencies pursuant to paragraph**
41 **(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 **accessed or** 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. In no event**
5 **shall an action be brought after six years from the date of discovery of**
6 **the breach of private information by the company unless the company took**
7 **steps to hide the breach**.
8   7. Regardless of the method by which notice is provided, such notice
9 shall include contact information for the person or business making the
10 notification**, the telephone numbers and websites of the relevant state**
11 **and federal agencies that provide information regarding security breach**
12 **response and identity theft prevention and protection information,** and a
13 description of the categories of information that were, or are reason-
14 ably believed to have been, **accessed or** acquired by a person without
15 valid authorization, including specification of which of the elements of
16 personal information and private information were, or are reasonably
17 believed to have been, so **accessed or** acquired.
18   8. (a) In the event that any New York residents are to be notified,
19 the person or business shall notify the state attorney general, the
20 department of state and the division of state police as to the timing,
21 content and distribution of the notices and approximate number of
22 affected persons **and shall provide a copy of the template of the notice**
23 **sent to affected persons**. Such notice shall be made without delaying
24 notice to affected New York residents.
25   (b) In the event that more than five thousand New York residents are
26 to be notified at one time, the person or business shall also notify
27 consumer reporting agencies as to the timing, content and distribution
28 of the notices and approximate number of affected persons. Such notice
29 shall be made without delaying notice to affected New York residents.
30   **9. Any covered entity required to provide notification of a breach,**
31 **including breach of information that is not "private information" as**
32 **defined in paragraph (b) of subdivision one of this section, to the**
33 **secretary of health and human services pursuant to the Health Insurance**
34 **Portability and Accountability Act of 1996 or the Health Information**
35 **Technology for Economic and Clinical Health Act, as amended from time to**
36 **time, shall provide such notification to the state attorney general**
37 **within five business days of notifying the secretary.**
38   § 4. The general business law is amended by adding a new section 899-
39 bb to read as follows:
40   **§ 899-bb. Data security protections. 1. Definitions. (a) "Compliant**
41 **regulated entity" shall mean any person or business that is subject to,**
42 **and in compliance with, any of the following data security requirements:**
43   **(i) regulations promulgated pursuant to Title V of the federal Gramm-**
44 **Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;**
45   **(ii) regulations implementing the Health Insurance Portability and**
46 **Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended**
47 **from time to time, and the Health Information Technology for Economic**
48 **and Clinical Health Act, as amended from time to time;**
49   **(iii) part five hundred of title twenty-three of the official compila-**
50 **tion of codes, rules and regulations of the state of New York, as**
51 **amended from time to time; or**
52   **(iv) any other data security rules and regulations of, and the stat-**
53 **utes administered by, any official department, division, commission or**
54 **agency of the federal or New York state government as such rules, regu-**
55 **lations or statutes are interpreted by such department, division,**
56 **commission or agency or by the federal or New York state courts.**

1 (b) "Private information" shall have the same meaning as defined in
2 section eight hundred ninety-nine-aa of this article.
3 (c) "Small business" shall mean any person or business with (i) fewer
4 than fifty employees; (ii) less than three million dollars in gross
5 annual revenue in each of the last three fiscal years; or (iii) less
6 than five million dollars in year-end total assets, calculated in
7 accordance with generally accepted accounting principles.
8 2. Reasonable security requirement. (a) Any person or business that
9 owns or licenses computerized data which includes private information of
10 a resident of New York shall develop, implement and maintain reasonable
11 safeguards to protect the security, confidentiality and integrity of the
12 private information including, but not limited to, disposal of data.
13 (b) A person or business shall be deemed to be in compliance with
14 paragraph (a) of this subdivision if it either:
15 (i) is a compliant regulated entity as defined in subdivision one of
16 this section; or
17 (ii) implements a data security program that includes the following:
18 (A) reasonable administrative safeguards such as the following, in
19 which the person or business:
20 (1) designates one or more employees to coordinate the security
21 program;
22 (2) identifies reasonably foreseeable internal and external risks;
23 (3) assesses the sufficiency of safeguards in place to control the
24 identified risks;
25 (4) trains and manages employees in the security program practices and
26 procedures;
27 (5) selects service providers capable of maintaining appropriate safe-
28 guards, and requires those safeguards by contract; and
29 (6) adjusts the security program in light of business changes or new
30 circumstances; and
31 (B) reasonable technical safeguards such as the following, in which
32 the person or business:
33 (1) assesses risks in network and software design;
34 (2) assesses risks in information processing, transmission and stor-
35 age;
36 (3) detects, prevents and responds to attacks or system failures; and
37 (4) regularly tests and monitors the effectiveness of key controls,
38 systems and procedures; and
39 (C) reasonable physical safeguards such as the following, in which the
40 person or business:
41 (1) assesses risks of information storage and disposal;
42 (2) detects, prevents and responds to intrusions;
43 (3) protects against unauthorized access to or use of private informa-
44 tion during or after the collection, transportation and destruction or
45 disposal of the information; and
46 (4) disposes of private information within a reasonable amount of time
47 after it is no longer needed for business purposes by erasing electronic
48 media so that the information cannot be read or reconstructed.
49 (c) A small business as defined in paragraph (c) of subdivision one of
50 this section complies with subparagraph (ii) of paragraph (b) of subdi-
51 vision two of this section if the small business's security program
52 contains reasonable administrative, technical and physical safeguards
53 that are appropriate for the size and complexity of the small business,
54 the nature and scope of the small business's activities, and the sensi-
55 tivity of the personal information the small business collects from or
56 about consumers.

 1   **(d) Any person or business that fails to comply with this subdivision**
 2 **shall be deemed to have violated section three hundred forty-nine of**
 3 **this chapter, and the attorney general may bring an action in the name**
 4 **and on behalf of the people of the state of New York to enjoin such**
 5 **violations and to obtain civil penalties under section three hundred**
 6 **fifty-d of this chapter.**
 7   **(e) Nothing in this section shall create a private right of action.**
 8   § 5. Paragraph (a) of subdivision 1 and subdivisions 2, 3, 6, 7 and 8
 9 of section 208 of the state technology law, paragraph (a) of subdivision
10 1 and subdivisions 3 and 8 as added by chapter 442 of the laws of 2005,
11 subdivision 2 and paragraph (a) of subdivision 7 as amended by section 5
12 of part N of chapter 55 of the laws of 2013 and subdivisions 6 and 7 as
13 amended by chapter 491 of the laws of 2005, are amended and a new subdi-
14 vision 9 is added to read as follows:
15   (a) "Private information" shall mean **either: (i)** personal information
16 **consisting of any information** in combination with any one or more of the
17 following data elements, when either the **data element or the combination**
18 **of** personal information [~~or~~] **plus** the data element is not encrypted or
19 encrypted with an encryption key that has also been **accessed or**
20 acquired:
21   (1) social security number;
22   (2) driver's license number or non-driver identification card number;
23 [~~or~~]
24   (3) account number, credit or debit card number, in combination with
25 any required security code, access code, [~~or~~] password **or other informa-**
26 **tion** which would permit access to an individual's financial account**;**
27   **(4) account number, or credit or debit card number, if circumstances**
28 **exist wherein such number could be used to access to an individual's**
29 **financial account without additional identifying information, security**
30 **code, access code, or password; or**
31   **(5) biometric information, meaning data generated by electronic meas-**
32 **urements of an individual's unique physical characteristics, such as**
33 **fingerprint, voice print, or retina or iris image, or other unique phys-**
34 **ical representation or digital representation which are used to authen-**
35 **ticate or ascertain the individual's identity; or**
36   **(ii) a user name or e-mail address in combination with a password or**
37 **security question and answer that would permit access to an online**
38 **account.**
39   "Private information" does not include publicly available information
40 that is lawfully made available to the general public from federal,
41 state, or local government records.
42   2. Any state entity that owns or licenses computerized data that
43 includes private information shall disclose any breach of the security
44 of the system following discovery or notification of the breach in the
45 security of the system to any resident of New York state whose private
46 information was, or is reasonably believed to have been, **accessed or**
47 acquired by a person without valid authorization. The disclosure shall
48 be made in the most expedient time possible and without unreasonable
49 delay, consistent with the legitimate needs of law enforcement, as
50 provided in subdivision four of this section, or any measures necessary
51 to determine the scope of the breach and restore the [~~reasonable~~] integ-
52 rity of the data system. The state entity shall consult with the state
53 office of information technology services to determine the scope of the
54 breach and restoration measures. **Within ninety days of the notice of the**
55 **breach, the office of information technology services shall deliver a**

1 **report on the scope of the breach and recommendations to restore and**
2 **improve the security of the system to the state entity.**
3 **(a) Notice to affected persons under this section is not required if**
4 **the exposure of private information was an inadvertent disclosure by**
5 **persons authorized to access private information, and the state entity**
6 **reasonably determines such exposure will not likely result in misuse of**
7 **such information, or financial or emotional harm to the affected**
8 **persons. Such a determination must be documented in writing and main-**
9 **tained for at least five years. If the incident affected over five**
10 **hundred residents of New York, the state entity shall provide the writ-**
11 **ten determination to the state attorney general within ten days after**
12 **the determination.**
13 **(b) If notice of the breach of the security of the system is made to**
14 **affected persons pursuant to the breach notification requirements under**
15 **any of the following laws, nothing in this section shall require any**
16 **additional notice to those affected persons, but notice still shall be**
17 **provided to the state attorney general, the department of state and the**
18 **office of information technology services pursuant to paragraph (a) of**
19 **subdivision seven of this section and to consumer reporting agencies**
20 **pursuant to paragraph (b) of subdivision seven of this section:**
21 **(i) regulations promulgated pursuant to Title V of the federal Gramm-**
22 **Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;**
23 **(ii) regulations implementing the Health Insurance Portability and**
24 **Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended**
25 **from time to time, and the Health Information Technology for Economic**
26 **and Clinical Health Act, as amended from time to time;**
27 **(iii) part five hundred of title twenty-three of the official compila-**
28 **tion of codes, rules and regulations of the state of New York, as**
29 **amended from time to time; or**
30 **(iv) any other data security rules and regulations of, and the stat-**
31 **utes administered by, any official department, division, commission or**
32 **agency of the federal or New York state government as such rules, regu-**
33 **lations or statutes are interpreted by such department, division,**
34 **commission or agency or by the federal or New York state courts.**
35 3. Any state entity that maintains computerized data that includes
36 private information which such agency does not own shall notify the
37 owner or licensee of the information of any breach of the security of
38 the system immediately following discovery, if the private information
39 was, or is reasonably believed to have been, **accessed or** acquired by a
40 person without valid authorization.
41 6. Regardless of the method by which notice is provided, such notice
42 shall include contact information for the state entity making the
43 notification**, the telephone numbers and websites of the relevant state**
44 **and federal agencies that provide information regarding security breach**
45 **response and identity theft prevention and protection information** and a
46 description of the categories of information that were, or are reason-
47 ably believed to have been, **accessed or** acquired by a person without
48 valid authorization, including specification of which of the elements of
49 personal information and private information were, or are reasonably
50 believed to have been, so **accessed or** acquired.
51 7. (a) In the event that any New York residents are to be notified,
52 the state entity shall notify the state attorney general, the department
53 of state and the state office of information technology services as to
54 the timing, content and distribution of the notices and approximate
55 number of affected persons **and provide a copy of the template of the**

1 **notice sent to affected persons**. Such notice shall be made without
2 delaying notice to affected New York residents.
3   (b) In the event that more than five thousand New York residents are
4 to be notified at one time, the state entity shall also notify consumer
5 reporting agencies as to the timing, content and distribution of the
6 notices and approximate number of affected persons. Such notice shall be
7 made without delaying notice to affected New York residents.
8   8. **The state office of information technology services shall develop,**
9 **update and provide regular training to all state entities relating to**
10 **best practices for the prevention of a breach of the security of the**
11 **system.**
12   **9. Any covered entity required to provide notification of a breach,**
13 **including breach of information that is not "private information" as**
14 **defined in paragraph (a) of subdivision one of this section, to the**
15 **secretary of health and human services pursuant to the Health Insurance**
16 **Portability and Accountability Act of 1996 or the Health Information**
17 **Technology for Economic and Clinical Health Act, as amended from time to**
18 **time, shall provide such notification to the state attorney general**
19 **within five business days of notifying the secretary.**
20   **10.** Any entity listed in subparagraph two of paragraph (c) of subdi-
21 vision one of this section shall adopt a notification policy no more
22 than one hundred twenty days after the effective date of this section.
23 Such entity may develop a notification policy which is consistent with
24 this section or alternatively shall adopt a local law which is consist-
25 ent with this section.
26   § 6. This act shall take effect on the ninetieth day after it shall
27 have become a law; provided, however, that section four of this act
28 shall take effect on the two hundred fortieth day after it shall have
29 become a law.