

STATE OF NEW YORK

8169

2019-2020 Regular Sessions

IN ASSEMBLY

June 4, 2019

Introduced by M. of A. LiPETRI -- read once and referred to the Committee on Governmental Operations

AN ACT to amend the state technology law, in relation to protecting personal information

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

1 Section 1. The state technology law is amended by adding a new article
2 4 to read as follows:

ARTICLE IV

PROTECTION OF PERSONAL INFORMATION

Section 401. Definitions of terms.

402. Duty to protect personal information.

403. Breach of security.

404. Causes of action.

9 § 401. Definitions of terms. The following definitions are applicable
10 to this article, except where different meanings are expressly speci-
11 fied:

12 1. "Personal information subject" means any natural person who has his
13 or her personal information collected or maintained by a personal infor-
14 mation recipient.

15 2. "Personal information recipient" means any natural person, corpo-
16 ration, partnership, limited liability company, unincorporated associ-
17 ation, government, or other entity, that, in the course of their
18 personal, business, commercial, corporate, association or governmental
19 operations, collects, receives, stores, maintains, processes, or other-
20 wise has access to, personal information.

21 3. "Personal information collector" means any personal information
22 recipient, that does not maintain or store such personal information, or
23 maintain access to such personal information, for more than five
24 minutes, and was provided with the personal information by the personal
25 information subject.

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

LBD09699-02-9

1 4. "Personal information holder" means any personal information recip-
2 ient, that maintains or stores such personal information, or maintains
3 access to such personal information, for more than five minutes, and was
4 provided with the personal information by the personal information
5 subject. "Personal information holder" shall not include any of the
6 following: a credit union as defined by subdivision nine of section two
7 of the banking law or a federally chartered credit union as defined by
8 the federal credit union act located and authorized to do business in
9 New York; a savings bank as defined by subdivision four of section two
10 of the banking law or any federal savings bank; or any savings and loan
11 association as defined by subdivision eight of section two of the baking
12 law or any federal savings and loan association.

13 5. "Third party personal information holder" means any personal infor-
14 mation recipient, that agrees to collect, receive, store, maintain,
15 process, or otherwise have access to, personal information, and was
16 provided with such personal information from a personal information
17 collector, a personal information holder, or another third party
18 personal information holder. "Third party personal information holder"
19 shall not include any of the following: a credit union as defined by
20 subdivision nine of section two of the banking law or a federally char-
21 tered credit union as defined by the federal credit union act located
22 and authorized to do business in New York; a savings bank as defined by
23 subdivision four of section two of the banking law or any federal
24 savings bank; or any savings and loan association as defined by subdivi-
25 sion eight of section two of the banking law or any federal savings and
26 loan association.

27 6. "Personal information" (a) means any information, including paper-
28 based information or electronic information, that contains a New York
29 state resident's first name and last name, or a New York state resi-
30 dent's first initial and last name, in combination with any one or more
31 of the following other informational elements that relate to such resi-
32 dent:

33 (1) A governmentally issued identification number, including:

34 (i) social security number;

35 (ii) driver's license number;

36 (iii) state issued identification card number;

37 (iv) military identification card number;

38 (v) student identification number; or

39 (vi) a United States passport number;

40 (2) Personal financial information, including:

41 (i) financial account information, including:

42 (A) bank account information;

43 (B) investment account information;

44 (C) retirement account information;

45 (D) deferred compensation account information;

46 (E) mortgage account information;

47 (F) car loan account information;

48 (G) credit line account information;

49 (H) personal loan account information; or

50 (I) any other monetary fund or loan account information; including:

51 (I) the number of such financial account;

52 (II) any record of such financial account;

53 (III) a transaction history of such account;

54 (IV) a balance of such account; and/or

1 (V) any security code, access code, personal identification number or
2 password, that would permit access to, or use of, such financial
3 account;

4 (ii) credit or debit card information, including:

5 (A) the number of such credit card or debit card;

6 (B) the expiration date of such credit or debit card;

7 (C) the card verification value code number of such credit or debit
8 card;

9 (D) any record of such credit or debit card account;

10 (E) any transaction history of such credit or debit card;

11 (F) any balance of such credit or debit card; and/or

12 (G) any required security code, access code, personal identification
13 number or password, that would permit access to, or use of, such credit
14 or debit card; or

15 (iii) credit status information, including:

16 (A) credit score;

17 (B) credit history; or

18 (C) any information describing credit transactions of the personal
19 information subject;

20 (3) Physical characteristic information, including:

21 (i) the height of the personal information subject;

22 (ii) the weight of the personal information subject;

23 (iii) the hair color of the personal information subject;

24 (iv) the eye color of the personal information subject; and/or

25 (v) any other distinguishing characteristics of the personal informa-
26 tion subject;

27 (4) Biometric information, including:

28 (i) fingerprints of the personal information subject;

29 (ii) voice-prints of the personal information subject;

30 (iii) eye scans of the personal information subject;

31 (iv) blood samples of the personal information subject;

32 (v) deoxyribonucleic acid (DNA) based samples of the personal informa-
33 tion subject;

34 (vi) skin samples of the personal information subject;

35 (vii) hair samples of the personal information subject; and/or

36 (viii) any other biometric information which is intended or collected
37 for the purpose of identification of the personal information subject;
38 or

39 (5) Medical information, including but not limited to, any information
40 collected or maintained about a personal information subject pursuant to
41 examination, testing or treatment for physical or mental illness or
42 wellness, or any other information collected or maintained on a personal
43 information subject by a health care provider or health care insurer;

44 (b) shall not include:

45 (1) personal information that is lawfully obtained from publicly
46 available information, or from federal, state or local government
47 records lawfully made available to the general public; or

48 (2) paper-based information that has been intentionally discarded or
49 abandoned by the personal information subject.

50 7. "Breach of security" means the unauthorized access, viewing, acqui-
51 sition, copying, duplication, removal or any other use of personal
52 information, either in unencrypted form or in encrypted form together
53 with the confidential process or key that is capable of compromising the
54 security, confidentiality, or integrity of personal information. A good
55 faith unauthorized access, viewing or acquisition of personal informa-
56 tion, for the lawful purposes of a personal information collector, shall

1 not be deemed to be a breach of security unless the personal information
2 is thereafter used in an unauthorized manner or is subject to further
3 unauthorized disclosure, as a result of such good faith unauthorized
4 access or acquisition.

5 8. "Record" means any information upon which written, drawn, spoken,
6 visual, or electromagnetic data or images are recorded or preserved,
7 either as paper-based information or electronic information.

8 9. "Paper-based information" means personal information collected or
9 maintained via paper, writing or other drawing medium, or any other
10 physical based, tangible, recording medium.

11 10. "Electronic information" means personal information collected or
12 maintained via computer, telephone, internet, computer network or other
13 electrical, digital, magnetic, wireless, optical, electromagnetic or
14 similar device.

15 11. "Encryption" means the transformation of data into a form in which
16 the meaning of such data cannot be accessed without the use of a confi-
17 dential process or key.

18 12. "Office" means the office of information technology services.

19 § 402. Duty to protect personal information. Every personal informa-
20 tion recipient shall have a legal duty to protect the security and
21 integrity of all personal information in their custody from unauthorized
22 access or unauthorized use.

23 § 403. Breach of security. 1. Notification to the division of state
24 police. In addition to any other requirements contained within any other
25 provision of law, not later than three days after discovering a security
26 breach involving personal information, any personal information recipi-
27 ent that has experienced a breach of security involving personal infor-
28 mation, shall make a comprehensive report to the division of state
29 police, in the form and manner required by such division, notifying the
30 division of state police of such security breach.

31 2. Notification of the chief information officer. Not more than two
32 days after receiving the notification required pursuant to subdivision
33 one of this section, the division of state police shall provide the
34 comprehensive report provided to such division to the chief information
35 officer of the office.

36 3. Notification of personal information subjects. In addition to any
37 other requirements pursuant to any other provision of law, upon the
38 receipt of the comprehensive report required by subdivision two of this
39 section, the chief information officer of the office shall require, in a
40 specified timeframe, and in a specified form and manner, that the
41 personal information recipient, or third party personal information
42 recipient, which sustained the breach of security of the personal infor-
43 mation, notify all personal information subjects impacted by the securi-
44 ty breach, of the fact that there has been a breach of security involv-
45 ing their personal information.

46 § 404. Causes of action. 1. Civil actions. Any personal information
47 subject may bring a civil action, against a personal information holder
48 in the supreme court of any county in which the personal information
49 recipient resides or conducts business operations, for damages or equi-
50 table relief, arising from a breach of security, and in accordance with
51 the provisions of this section. A civil action for damages or equitable
52 relief, shall not, however, be brought by a personal information
53 subject, in any other state court of competent jurisdiction, other than
54 in accordance with the provisions of this section, if such civil action
55 arises out of a breach of security by a personal information holder. No
56 action shall be brought under this section against a personal informa-

1 tion collector or a third party personal information collector unless
2 brought in accordance with the provisions of subparagraph four of para-
3 graph (c) of subdivision two of this section.

4 2. Civil actions that may be brought by a personal information subject
5 against a personal information recipient.

6 (a) Timeliness of actions. A civil action may be brought in accordance
7 with this section if such civil action is brought within six years of
8 the date of the reporting of the breach of security as required by
9 section four hundred three of this article, or in the event no such
10 report was ever made, within any time after the date of the discovery of
11 the breach of security by the personal information subject.

12 (b) Equitable action. Any action brought in accordance with this
13 section, may seek damages and/or equitable relief. If a personal infor-
14 mation subject seeks equitable relief for a breach of security involving
15 a security breach of personal information from a personal information
16 recipient, and the court determines that such equitable relief is just
17 and proper and should be awarded, then in addition to such equitable
18 relief, the court may also award the personal information subject costs,
19 disbursements and attorneys fees of the action. No action brought under
20 this section for equitable relief shall prohibit a personal information
21 subject from also bringing any additional cause of action for damages,
22 when such additional cause of action is allowed under this article.

23 (c) Actions involving damages. Any action brought in accordance with
24 this section, seeking damages for a breach of security involving a secu-
25 rity breach of personal information from a personal information recipi-
26 ent, shall be brought as follows:

27 (1) personal information holders or third party personal information
28 holders with annual revenues of ten million dollars or more. Any
29 personal information holder, or third party personal information holder,
30 that has annual revenues of ten million dollars or more, that experi-
31 ences a breach of security involving such personal information, shall be
32 strictly liable in a civil action brought in accordance with this
33 section, for damages, if the personal information subject involved in
34 the breach of security sustains any damages as a result of such breach.
35 Such strict liability shall extend to damages in the amount of three
36 times the amount of such damages sustained by the personal information
37 subject, or an amount of up to ten thousand dollars, whichever is great-
38 er, together with costs, disbursements and attorneys fees of the action.
39 Where the court finds that the personal information holder or a third
40 party personal information holder, intentionally failed to establish a
41 comprehensive personal information security program or intentionally
42 failed to maintain safeguards, standards, protocols or best practices
43 for the protection of personal information, then the court may also
44 award punitive damages to the plaintiff of an action brought under this
45 subdivision.

46 (2) personal information holders or third party personal information
47 holders with annual revenues of between one million dollars and ten
48 million dollars. Any personal information holder, or third party
49 personal information holder, that has annual revenues of between one
50 million dollars and ten million dollars that experiences a breach of
51 security involving such personal information, shall be strictly liable
52 in a civil action brought in accordance with this section, for damages,
53 if the personal information subject involved in the breach of security
54 sustains any damages as a result of such breach. Such strict liability
55 shall extend to damages in the amount of three times the amount of such
56 damages sustained by the personal information subject, or an amount of

1 up to five thousand dollars, whichever is greater, together with costs,
2 disbursements and attorneys fees of the action. Where the court finds
3 that the personal information holder or a third party personal informa-
4 tion holder, intentionally failed to establish a comprehensive personal
5 information security program or intentionally failed to maintain safe-
6 guards, standards, protocols or best practices for the protection of
7 personal information, then the court may also award punitive damages to
8 the plaintiff of an action brought under this subdivision.

9 (3) personal information holders or third party personal information
10 holders with annual revenues of less than one million dollars. Any
11 personal information holder, or third party personal information holder,
12 that has annual revenues of less than one million dollars, and that
13 fails to maintain the safeguards, standards, protocols or best practices
14 for the protection of personal information as established in its compre-
15 hensive personal information security program and that experiences a
16 breach of security involving such personal information, shall be strict-
17 ly liable in a civil action brought in accordance with this section, for
18 damages, if the personal information subject involved in the breach of
19 security sustains any damages as a result of such breach. Such strict
20 liability shall extend to damages in the amount of three times the
21 amount of such damages sustained by the personal information subject, or
22 an amount of up to one thousand dollars, whichever is greater, together
23 with costs, disbursements and attorneys fees of the action. Where the
24 court finds that the personal information holder or a third party
25 personal information holder, intentionally failed to establish a compre-
26 hensive personal information security program or intentionally failed to
27 maintain safeguards, standards, protocols or best practices for the
28 protection of personal information, then the court may also award puni-
29 tive damages to the plaintiff of an action brought under this subdivi-
30 sion.

31 (4) personal information collectors. Any personal information collec-
32 tor that fails to maintain the safeguards, standards, protocols or best
33 practices for the protection of personal information, or that fails to
34 establish a comprehensive personal information security program and that
35 experiences a breach of security involving such personal information,
36 shall be strictly liable in a civil action for damages brought in
37 accordance with this section, in the amount of such damages so
38 sustained. Where the court finds that the personal information collector
39 intentionally failed to establish a comprehensive personal information
40 security program or intentionally failed to maintain safeguards, stand-
41 ards, protocols or best practices for the protection of personal infor-
42 mation, then the court may also award punitive damages to the plaintiff
43 of an action brought under this subdivision.

44 (5) no action brought under this section for damages shall prohibit a
45 personal information subject from also bringing any additional cause of
46 action for equitable relief, when such additional cause of action is
47 also allowed under this article.

48 3. Civil actions that may be brought by the attorney general against a
49 personal information recipient.

50 (a) Whenever the attorney general believes from evidence satisfactory
51 to him or her that there is a violation of this article by a personal
52 information holder or third party personal information holder with annu-
53 al revenues of ten million dollars or more, he or she may bring an
54 action in the name and on behalf of the people of the state of New York,
55 in a court of justice having jurisdiction to issue an injunction, to
56 enjoin and restrain the continuation of such violation. In such action,

1 preliminary relief may be granted under article sixty-three of the civil
2 practice law and rules.

3 (b) In such action the court may award damages for actual costs or
4 losses incurred by a personal information subject suffering damages
5 pursuant to this article, if the breach occurred pursuant to this arti-
6 cle, including consequential financial losses. Whenever the court shall
7 determine in such action that a personal information holder or third
8 party personal information holder with annual revenues of ten million
9 dollars or more violated this article, the personal information holder
10 or third party personal information holder shall be held strictly liable
11 and responsible for damages for actual costs or losses incurred by a
12 personal information subject suffering damages.

13 (c) Whenever the court shall determine in such action that a personal
14 information holder or third party personal information holder with annu-
15 al revenues of ten million dollars or more violated this article, the
16 court may impose a civil penalty of two hundred fifty thousand dollars
17 per instance of breach, provided that the total amounts shall not exceed
18 one hundred million dollars.

19 (d) The remedies provided by this section shall be in addition to any
20 other lawful remedy available.

21 (e) No action may be brought under the provisions of this section
22 unless such action is commenced within six years immediately after
23 either the date of the act complained of or the date of discovery of
24 such act on which the attorney general became aware of the violation, or
25 the date of notice sent pursuant to section four hundred three of this
26 article.

27 § 2. This act shall take effect on the one hundred eightieth day after
28 it shall have become a law.