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:

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

ARTICLE IV

PROTECTION OF PERSONAL INFORMATION

§ 401. Definitions of terms. The following definitions are applicable to this article, except where different meanings are expressly specified:

1. "Personal information subject" means any natural person who has his or her personal information collected or maintained by a personal information recipient.

2. "Personal information recipient" means any natural person, corporation, partnership, limited liability company, unincorporated association, government, or other entity, that, in the course of their personal, business, commercial, corporate, association or governmental operations, collects, receives, stores, maintains, processes, or otherwise has access to, personal information.

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

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

LBD09699-02-9

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

5. "Third party personal information holder" means any personal information recipient, that agrees to collect, receive, store, maintain, process, or otherwise have access to, personal information, and was provided with such personal information from a personal information collector, a personal information holder, or another third party personal information holder. "Third party personal information holder" shall not include any of the following: a credit union as defined by subdivision nine of section two of the banking law or a federally chartered credit union as defined by the federal credit union act located and authorized to do business in New York; a savings bank as defined by subdivision four of section two of the banking law or any federal savings bank; or any savings and loan association as defined by subdivision eight of section two of the banking law or any federal savings and loan association.

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

(1) A governmentally issued identification number, including:

(i) social security number;

(ii) driver's license number;

(iii) state issued identification card number;

(iv) military identification card number;

(v) student identification number; or

(vi) a United States passport number;

(2) Personal financial information, including:

(i) financial account information, including:

(A) bank account information;

(B) investment account information;

(C) retirement account information;

(D) deferred compensation account information;

(E) mortgage account information;

(F) car loan account information;

(G) credit line account information;

(H) personal loan account information; or

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

(I) the number of such financial account;

(II) any record of such financial account;

(III) a transaction history of such account;

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

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

(ii) credit or debit card information, including:

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

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

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

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

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

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

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

(iii) credit status information, including:

(A) credit score;

(B) credit history; or

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

(3) Physical characteristic information, including:

(i) the height of the personal information subject;

(ii) the weight of the personal information subject;

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

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

(v) any other distinguishing characteristics of the personal information subject;

(4) Biometric information, including:

(i) fingerprints of the personal information subject;

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

(iii) eye scans of the personal information subject;

(iv) blood samples of the personal information subject;

(v) deoxyribonucleic acid (DNA) based samples of the personal information subject;

(vi) skin samples of the personal information subject;

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

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

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

(b) shall not include:

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

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

7. "Breach of security" means the unauthorized access, viewing, acquisition, copying, duplication, removal or any other use of personal information, either in unencrypted form or in encrypted form together with the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information. A good faith unauthorized access, viewing or acquisition of personal information, for the lawful purposes of a personal information collector, shall

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

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

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

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

11. "Encryption" means the transformation of data into a form in which the meaning of such data cannot be accessed without the use of a confidential process or key.

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

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

§ 403. Breach of security. 1. Notification to the division of state police. In addition to any other requirements contained within any other provision of law, not later than three days after discovering a security breach involving personal information, any personal information recipient that has experienced a breach of security involving personal information, shall make a comprehensive report to the division of state police, in the form and manner required by such division, notifying the division of state police of such security breach.

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

3. Notification of personal information subjects. In addition to any other requirements pursuant to any other provision of law, upon the receipt of the comprehensive report required by subdivision two of this section, the chief information officer of the office shall require, in a specified timeframe, and in a specified form and manner, that the personal information recipient, or third party personal information recipient, which sustained the breach of security of the personal information, notify all personal information subjects impacted by the security breach, of the fact that there has been a breach of security involving their personal information.

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

tion collector or a third party personal information collector unless brought in accordance with the provisions of subparagraph four of paragraph (c) of subdivision two of this section.

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

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

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

(c) Actions involving damages. Any action brought in accordance with this section, seeking damages for a breach of security involving a security breach of personal information from a personal information recipient, shall be brought as follows:

(1) personal information holders or third party personal information holders with annual revenues of ten million dollars or more. Any personal information holder, or third party personal information holder, that has annual revenues of ten million dollars or more, that experiences a breach of security involving such personal information, shall be strictly liable in a civil action brought in accordance with this section, for damages, if the personal information subject involved in the breach of security sustains any damages as a result of such breach. Such strict liability shall extend to damages in the amount of three times the amount of such damages sustained by the personal information subject, or an amount of up to ten thousand dollars, whichever is greater, together with costs, disbursements and attorneys fees of the action. Where the court finds that the personal information holder or a third party personal information holder, intentionally failed to establish a comprehensive personal information security program or intentionally failed to maintain safeguards, standards, protocols or best practices for the protection of personal information, then the court may also award punitive damages to the plaintiff of an action brought under this subdivision.

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

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

(3) personal information holders or third party personal information holders with annual revenues of less than one million dollars. Any personal information holder, or third party personal information holder, that has annual revenues of less than one million dollars, and that fails to maintain the safeguards, standards, protocols or best practices for the protection of personal information as established in its comprehensive personal information security program and that experiences a breach of security involving such personal information, shall be strictly liable in a civil action brought in accordance with this section, for damages, if the personal information subject involved in the breach of security sustains any damages as a result of such breach. Such strict liability shall extend to damages in the amount of three times the amount of such damages sustained by the personal information subject, or an amount of up to one thousand dollars, whichever is greater, together with costs, disbursements and attorneys fees of the action. Where the court finds that the personal information holder or a third party personal information holder, intentionally failed to establish a comprehensive personal information security program or intentionally failed to maintain safeguards, standards, protocols or best practices for the protection of personal information, then the court may also award punitive damages to the plaintiff of an action brought under this subdivision.

(4) personal information collectors. Any personal information collector that fails to maintain the safeguards, standards, protocols or best practices for the protection of personal information, or that fails to establish a comprehensive personal information security program and that experiences a breach of security involving such personal information, shall be strictly liable in a civil action for damages brought in accordance with this section, in the amount of such damages so sustained. Where the court finds that the personal information collector intentionally failed to establish a comprehensive personal information security program or intentionally failed to maintain safeguards, standards, protocols or best practices for the protection of personal information, then the court may also award punitive damages to the plaintiff of an action brought under this subdivision.

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

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

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

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

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

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

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

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

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