S T A T E O F N E W Y O R K

4887

2015-2016 Regular Sessions

I N S E N A T E

April 22, 2015

Introduced by Sen. VENDITTO -- (at request of the Attorney General) -- read twice and ordered printed, and when printed to be committed to the Committee on Consumer Protection

AN ACT to amend the general business law and the state technology law, in relation to the data security act

THE PEOPLE OF THE STATE OF NEW YORK, REPRESENTED IN SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:

Section 1. This act shall be known and may be cited as the "data security act".

S 2. The opening paragraph and paragraph (b) of subdivision 1 of section 899-aa of the general business law, as added by chapter 442 of the laws of 2005, are amended to read as follows:

As used in this section, AND SECTION EIGHT HUNDRED NINETY-NINE-BB OF THIS ARTICLE, the following terms shall have the following meanings:

(b) "Private information" shall mean EITHER: (I) personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired:

(1) social security number;

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

(3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; OR

(4) BIOMETRIC INFORMATION, MEANING DATA GENERATED BY AUTOMATIC MEASUREMENTS OF AN INDIVIDUAL'S PHYSICAL CHARACTERISTICS, WHICH ARE USED BY THE OWNER OR LICENSEE TO AUTHENTICATE THE INDIVIDUAL'S IDENTITY;

(II) A USER NAME OR EMAIL ADDRESS IN COMBINATION WITH A PASSWORD OR SECURITY QUESTION AND ANSWER THAT WOULD PERMIT ACCESS TO AN ONLINE ACCOUNT; OR

(III) ANY UNSECURED PROTECTED HEALTH INFORMATION AS DEFINED IN THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (45 C.F.R. PTS. 160, 162, 164), AS AMENDED FROM TIME TO TIME.

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

LBD08145-09-5

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

S 3. Subdivisions 4 and 5 of section 899-aa of the general business law, as added by chapter 442 of the laws of 2005, are amended to read as follows:

4. (A) The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

(B) THE PRODUCTION OF FORENSIC REPORTS TO LOCAL AND STATE LAW ENFORCEMENT AGENCIES FOR THE PURPOSES OF INVESTIGATING AND IDENTIFYING THOSE RESPONSIBLE FOR A BREACH OF THE SECURITY OF THE SYSTEM SHALL NOT CONSTITUTE A WAIVER OF ANY APPLICABLE PRIVILEGE OR PROTECTION PROVIDED BY LAW, INCLUDING TRADE SECRET PROTECTION, AND FORENSIC REPORTS SO PRODUCED SHALL NOT BE SUBJECT TO DISCLOSURE UNDER ARTICLE SIX OF THE PUBLIC OFFICERS LAW.

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

(a) written notice;

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

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

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

(1) e-mail notice when such business has an e-mail address for the subject persons;

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

(3) notification to major statewide media.

(E) IN THE CASE OF A BREACH OF THE SECURITY OF THE SYSTEM INVOLVING A USER NAME, AND PASSWORD OR SECURITY QUESTION AND ANSWER WHICH WOULD PERMIT ACCESS TO AN ONLINE ACCOUNT, AS PROVIDED IN SUBPARAGRAPH (II) OF PARAGRAPH (B) OF SUBDIVISION ONE OF THIS SECTION, AND NO OTHER PRIVATE INFORMATION DEFINED IN SUCH PARAGRAPH (B), THE PERSON OR BUSINESS MAY COMPLY WITH THIS SECTION BY PROVIDING NOTIFICATION IN ELECTRONIC OR OTHER FORM THAT DIRECTS THE PERSON WHOSE PRIVATE INFORMATION HAS BEEN BREACHED PROMPTLY TO CHANGE HIS OR HER PASSWORD AND SECURITY QUESTION OR ANSWER, AS APPLICABLE, OR TO TAKE OTHER STEPS APPROPRIATE TO PROTECT THE ONLINE ACCOUNT WITH THE PERSON OR BUSINESS AND ALL OTHER ONLINE ACCOUNTS FOR WHICH THE PERSON WHOSE PRIVATE INFORMATION HAS BEEN BREACHED USES THE SAME INFORMATION.

(F) IN THE CASE OF A BREACH OF THE SECURITY OF THE SYSTEM INVOLVING THE LOGIN CREDENTIALS OF AN EMAIL ACCOUNT FURNISHED BY THE PERSON OR

BUSINESS AS PROVIDED IN SUBPARAGRAPH (II) OF PARAGRAPH (B) OF SUBDIVISION ONE OF THIS SECTION, THE PERSON OR BUSINESS SHALL NOT COMPLY WITH THIS SECTION BY PROVIDING THE SECURITY BREACH NOTIFICATION TO THAT EMAIL ADDRESS, BUT SHALL, INSTEAD, COMPLY WITH THIS SECTION BY PROVIDING NOTICE BY ANOTHER METHOD DESCRIBED IN THIS SUBDIVISION OR BY CLEAR AND CONSPICUOUS NOTICE DELIVERED TO THE RESIDENT ONLINE WHEN THE RESIDENT IS CONNECTED TO THE ONLINE ACCOUNT FROM AN INTERNET PROTOCOL ADDRESS OR ONLINE LOCATION FROM WHICH THE PERSON OR BUSINESS KNOWS THE RESIDENT CUSTOMARILY ACCESSES THE ACCOUNT.

S 4. Paragraph (a) of subdivision 6 of section 899-aa of the general business law, as amended by chapter 491 of the laws of 2005, is amended to read as follows:

(a) whenever the attorney general shall believe from evidence satisfactory to him OR HER that there is a violation of this [article] SECTION 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. In such action the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this [article] SECTION, if notification was not provided to such person pursuant to this [article] SECTION, including consequential financial losses. Whenever the court shall determine in such action that a person or business violated this [article] SECTION knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to ten dollars per instance of failed notification, provided that the latter amount shall not exceed one [hundred fifty thousand] MILLION dollars.

S 5. Paragraph (a) of subdivision 1 of section 208 of the state technology law, as added by chapter 442 of the laws of 2005, is amended to read as follows:

(a) "Private information" shall mean EITHER: (I) personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number; or

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

(II) A USER NAME OR EMAIL ADDRESS IN COMBINATION WITH A PASSWORD OR SECURITY QUESTION AND ANSWER THAT WOULD PERMIT ACCESS TO AN ONLINE ACCOUNT; OR

(III) ANY UNSECURED PROTECTED HEALTH INFORMATION AS DEFINED IN THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (45 C.F.R. PTS. 160, 162, 164), AS AMENDED FROM TIME TO TIME.

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

S 6. The general business law is amended by adding a new section 899-bb to read as follows:

S 899-BB. DATA SECURITY REQUIREMENTS. 1. REASONABLE SAFEGUARDS. (A) ANY PERSON OR BUSINESS THAT CONDUCTS BUSINESS IN NEW YORK STATE, AND OWNS OR LICENSES COMPUTERIZED DATA WHICH INCLUDES PRIVATE INFORMATION OF A RESIDENT OF NEW YORK SHALL DEVELOP, IMPLEMENT AND MAINTAIN REASONABLE

SAFEGUARDS TO PROTECT THE SECURITY, CONFIDENTIALITY AND INTEGRITY OF THE PRIVATE INFORMATION, INCLUDING DISPOSAL OF DATA.

(B) THE FOLLOWING SHALL BE DEEMED TO BE IN COMPLIANCE WITH PARAGRAPH (A) OF THIS SUBDIVISION:

(I) A PERSON OR BUSINESS THAT COMPLIES WITH A STATE OR FEDERAL LAW PROVIDING GREATER PROTECTION TO PRIVATE INFORMATION THAN THAT PROVIDED BY THIS SECTION;

(II) A PERSON OR BUSINESS THAT IS SUBJECT TO AND COMPLIES WITH REGULATIONS PROMULGATED PURSUANT TO TITLE V OF THE GRAMM-LEACH-BLILEY ACT OF 1999 (15 U.S.C. 6801 TO 6809);

(III) A PERSON OR BUSINESS THAT COMPLIES WITH CURRENT INTERNATIONAL STANDARDS ORGANIZATION STANDARDS FOR INFORMATION SECURITY;

(IV) A PERSON OR BUSINESS THAT IS SUBJECT TO AND COMPLIES WITH REGULATIONS IMPLEMENTING THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (45 C.F.R. PARTS 160 AND 164) AND THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT, AS AMENDED FROM TIME TO TIME;

(V) A PERSON OR BUSINESS THAT COMPLIES WITH CURRENT NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY STANDARDS AS REFERENCED IN SUBDIVISION THREE OF THIS SECTION; OR

(VI) A PERSON OR BUSINESS THAT IMPLEMENTS AN INFORMATION SECURITY PROGRAM THAT INCLUDES THE FOLLOWING:

(A) ADMINISTRATIVE SAFEGUARDS SUCH AS THE FOLLOWING, IN WHICH THE PERSON OR BUSINESS:

(I) DESIGNATES ONE OR MORE EMPLOYEES TO COORDINATE THE SECURITY PROGRAM;

(II) IDENTIFIES REASONABLY FORESEEABLE INTERNAL AND EXTERNAL RISKS;

(III) ASSESSES THE SUFFICIENCY OF SAFEGUARDS IN PLACE TO CONTROL THE IDENTIFIED RISKS;

(IV) TRAINS AND MANAGES EMPLOYEES IN THE SECURITY PROGRAM PRACTICES AND PROCEDURES;

(V) SELECTS SERVICE PROVIDERS CAPABLE OF MAINTAINING APPROPRIATE SAFEGUARDS, AND REQUIRES THOSE SAFEGUARDS BY CONTRACT;

(VI) ADJUSTS THE SECURITY PROGRAM IN LIGHT OF BUSINESS CHANGES OR NEW CIRCUMSTANCES; AND

(B) TECHNICAL SAFEGUARDS SUCH AS THE FOLLOWING, IN WHICH THE PERSON OR BUSINESS:

(I) ASSESSES RISKS IN NETWORK AND SOFTWARE DESIGN;

(II) ASSESSES RISKS IN INFORMATION PROCESSING, TRANSMISSION AND STORAGE;

(III) DETECTS, PREVENTS AND RESPONDS TO ATTACKS OR SYSTEM FAILURES;

(IV) REGULARLY TESTS AND MONITORS THE EFFECTIVENESS OF KEY CONTROLS, SYSTEMS AND PROCEDURES; AND

(C) PHYSICAL SAFEGUARDS SUCH AS THE FOLLOWING, IN WHICH THE PERSON OR BUSINESS:

(I) ASSESSES RISKS OF INFORMATION STORAGE AND DISPOSAL;

(II) DETECTS, PREVENTS AND RESPONDS TO INTRUSIONS;

(III) PROTECTS AGAINST UNAUTHORIZED ACCESS TO OR USE OF PRIVATE INFORMATION DURING OR AFTER THE COLLECTION, TRANSPORTATION AND DESTRUCTION OR DISPOSAL OF THE INFORMATION; AND

(IV) DISPOSES OF PRIVATE INFORMATION AFTER IT IS NO LONGER NEEDED FOR BUSINESS PURPOSES BY ERASING ELECTRONIC MEDIA SO THAT THE INFORMATION CANNOT BE READ OR RECONSTRUCTED.

2. REBUTTABLE PRESUMPTION. A PERSON OR BUSINESS THAT OBTAINS AN INDEPENDENT, THIRD-PARTY AUDIT AND CERTIFICATION ANNUALLY UNDER THE DATA SECURITY STANDARD LISTED IN PARAGRAPH (B) OF SUBDIVISION ONE OF THIS

SECTION SHALL RECEIVE A REBUTTABLE PRESUMPTION THAT IT MAINTAINED REASONABLE SAFEGUARDS TO PROTECT THE SECURITY, CONFIDENTIALITY AND INTEGRITY OF THE PRIVATE INFORMATION.

3. CERTIFICATION AUTHORITY AND REGULATION. THE DEPARTMENT OF FINANCIAL SERVICES SHALL PROMULGATE REGULATIONS REGARDING INDEPENDENT, THIRD-PARTY LICENSED INSURERS RESPONSIBLE FOR CERTIFYING ENTITIES THAT MEET THE REASONABLE DATA SECURITY REQUIREMENTS SET FORTH IN SUBPARAGRAPH (VI) OF PARAGRAPH (B) OF SUBDIVISION ONE OF THIS SECTION.

4. SAFE HARBOR. ANY PERSON OR BUSINESS THAT COMPLIES WITH THE MOST UP TO DATE VERSION OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY SPECIAL PUBLICATION 800-53 SHALL BE IMMUNE FROM LIABILITY IN A CIVIL ACTION, INCLUDING BUT NOT LIMITED TO AN ACTION BROUGHT BY THE ATTORNEY GENERAL, RESULTING FROM UNAUTHORIZED ACCESS TO PRIVATE INFORMATION BY A THIRD-PARTY ABSENT EVIDENCE OF WILLFUL MISCONDUCT, BAD FAITH OR GROSS NEGLIGENCE. COMPLIANCE MUST BE CERTIFIED ANNUALLY BY AN INDEPENDENT, THIRD-PARTY LICENSED INSURER, AUTHORIZED BY THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.

5. ENFORCEMENT. (A) WHENEVER THE ATTORNEY GENERAL SHALL BELIEVE FROM EVIDENCE SATISFACTORY TO HIM OR HER THAT THERE IS A VIOLATION OF THIS SECTION 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. IN SUCH ACTION, THE COURT MAY AWARD DAMAGES FOR ACTUAL COSTS OR LOSSES INCURRED BY A PERSON AS A RESULT OF THE FAILURE BY A PERSON OR BUSINESS TO COMPLY WITH THE DATA SECURITY REQUIREMENTS SET FORTH IN THIS SECTION, INCLUDING CONSEQUENTIAL FINANCIAL LOSSES, AS WELL AS A CIVIL PENALTY OF UP TO TWO HUNDRED FIFTY DOLLARS, WHICH PENALTY MAY BE INCREASED BY A FACTOR LESS THAN OR EQUAL TO THE NUMBER OF PERSONS WHOSE PRIVATE INFORMATION WAS COMPROMISED; PROVIDED HOWEVER, THAT THE AGGREGATE AMOUNT OF ANY CIVIL PENALTIES SO IMPOSED SHALL NOT EXCEED TEN MILLION DOLLARS. WHENEVER THE COURT SHALL DETERMINE THAT A PERSON OR BUSINESS VIOLATED THIS SECTION KNOWINGLY OR RECKLESSLY, THE COURT MAY, IN LIEU OF IMPOSING A CIVIL PENALTY AS SET FORTH ABOVE, INSTEAD IMPOSE A CIVIL PENALTY OF UP TO ONE THOUSAND DOLLARS, WHICH PENALTY MAY BE INCREASED BY A FACTOR LESS THAN OR EQUAL TO THE NUMBER OF PERSONS WHOSE PRIVATE INFORMATION WAS COMPROMISED; PROVIDED HOWEVER, THAT THE AGGREGATE AMOUNT OF ANY CIVIL PENALTIES SO IMPOSED SHALL NOT EXCEED THE GREATER OF FIFTY MILLION DOLLARS OR THREE TIMES THE AGGREGATE AMOUNT OF ANY ACTUAL COSTS AND LOSSES AS DETERMINED BY THE COURT. A COURT MAY AWARD A CIVIL PENALTY PURSUANT TO THIS PARAGRAPH WITHOUT A SHOWING OF FINANCIAL LOSS.

(B) THE REMEDIES PROVIDED BY THIS SECTION SHALL BE IN ADDITION TO ANY OTHER LAWFUL REMEDY AVAILABLE.

(C) NO ACTION MAY BE BROUGHT UNDER THE PROVISIONS OF THIS SECTION UNLESS SUCH ACTION IS COMMENCED WITHIN THREE YEARS IMMEDIATELY AFTER THE DATE OF THE ACT OR OMISSION COMPLAINED OF OR THE DATE OF DISCOVERY OF SUCH ACT OR OMISSION.

S 7. Section 208 of the state technology law is amended by adding a new subdivision 9 to read as follows:

9. DATA SECURITY REQUIREMENTS. (A) ANY STATE ENTITY THAT OWNS, MAINTAINS, OR OTHERWISE POSSESSES PRIVATE INFORMATION SHALL DEVELOP, IMPLEMENT AND MAINTAIN REASONABLE SAFEGUARDS TO PROTECT THE SECURITY, CONFIDENTIALITY AND INTEGRITY OF THE PRIVATE INFORMATION, INCLUDING DISPOSAL OF DATA.

(B) THE FOLLOWING SHALL BE DEEMED TO BE IN COMPLIANCE WITH PARAGRAPH (A) OF THIS SUBDIVISION:
(I) A STATE ENTITY THAT COMPLIES WITH A STATE OR FEDERAL LAW PROVIDING GREATER PROTECTION TO PRIVATE INFORMATION THAN THAT PROVIDED BY THIS SECTION;
(II) A STATE ENTITY THAT IS SUBJECT TO AND COMPLIES WITH REGULATIONS PROMULGATED PURSUANT TO TITLE V OF THE GRAMM-LEACH-BLILEY ACT OF 1999 (15 U.S.C. 6801 TO 6809);
(III) A STATE ENTITY THAT COMPLIES WITH THE MOST CURRENT INTERNATIONAL STANDARDS ORGANIZATION STANDARDS FOR INFORMATION SECURITY;
(IV) A STATE ENTITY THAT IS SUBJECT TO AND COMPLIES WITH REGULATIONS IMPLEMENTING THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (45 C.F.R. PARTS 160 AND 164) AND THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT, AS AMENDED FROM TIME TO TIME;
(V) A STATE ENTITY THAT COMPLIES WITH CURRENT NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY STANDARDS; OR
(VI) A STATE ENTITY THAT IMPLEMENTS AN INFORMATION SECURITY PROGRAM THAT INCLUDES THE FOLLOWING:
(A) ADMINISTRATIVE SAFEGUARDS SUCH AS THE FOLLOWING, IN WHICH THE STATE ENTITY:
(I) DESIGNATES ONE OR MORE EMPLOYEES TO COORDINATE THE SECURITY PROGRAM;
(II) IDENTIFIES REASONABLY FORESEEABLE INTERNAL AND EXTERNAL RISKS;
(III) ASSESSES THE SUFFICIENCY OF SAFEGUARDS IN PLACE TO CONTROL THE IDENTIFIED RISKS;
(IV) TRAINS AND MANAGES EMPLOYEES IN THE SECURITY PROGRAM PRACTICES AND PROCEDURES;
(V) SELECTS SERVICE PROVIDERS CAPABLE OF MAINTAINING APPROPRIATE SAFE-GUARDS, AND REQUIRES THOSE SAFEGUARDS BY CONTRACT; AND
(VI) ADJUSTS THE SECURITY PROGRAM IN LIGHT OF BUSINESS CHANGES OR NEW CIRCUMSTANCES;
(B) TECHNICAL SAFEGUARDS SUCH AS THE FOLLOWING, IN WHICH THE STATE ENTITY:
(I) ASSESSES RISKS IN NETWORK AND SOFTWARE DESIGN;
(II) ASSESSES RISKS IN INFORMATION PROCESSING, TRANSMISSION AND STOR-AGE;
(III) DETECTS, PREVENTS AND RESPONDS TO ATTACKS OR SYSTEM FAILURES; AND
(IV) REGULARLY TESTS AND MONITORS THE EFFECTIVENESS OF KEY CONTROLS, SYSTEMS AND PROCEDURES; AND
(C) PHYSICAL SAFEGUARDS SUCH AS THE FOLLOWING, IN WHICH THE STATE ENTITY:
(I) ASSESSES RISKS OF INFORMATION STORAGE AND DISPOSAL;
(II) DETECTS, PREVENTS AND RESPONDS TO INTRUSIONS;
(III) PROTECTS AGAINST UNAUTHORIZED ACCESS TO OR USE OF PRIVATE INFOR-MATION DURING OR AFTER THE COLLECTION, TRANSPORTATION AND DESTRUCTION OR DISPOSAL OF THE INFORMATION; AND
(IV) DISPOSES OF PRIVATE INFORMATION AFTER IT IS NO LONGER NEEDED FOR BUSINESS PURPOSES OR AS REQUIRED BY LOCAL, STATE OR FEDERAL LAW BY ERAS-ING ELECTRONIC MEDIA SO THAT THE INFORMATION CANNOT BE READ OR RECON-STRUCTED.
S 8. This act shall take effect January 1, 2016.