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

3760

2009-2010 Regular Sessions

I N S E N A T E

March 31, 2009

Introduced by Sen. ADAMS -- 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 information security breach and notification act

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

Section 1. Section 899-aa of the general business law, as added by chapter 442 of the laws of 2005, paragraph (c) of subdivision 1, paragraph (a) of subdivision 6 and subdivision 8 as amended by chapter 491 of the laws of 2005, is amended to read as follows:

S 899-aa. Notification; [person without valid authorization has acquired] UNAUTHORIZED ACQUISITION OF private information. 1. As used in this section, the following terms shall have the following meanings:

(a) "ENCRYPTED" SHALL MEAN THE PROTECTION OF PRIVATE INFORMATION IN ELECTRONIC FORM IN STORAGE OR IN TRANSIT USING AN ENCRYPTION TECHNOLOGY THAT HAS BEEN ADOPTED BY A STANDARDS SETTING BODY GENERALLY RECOGNIZED IN THE INFORMATION TECHNOLOGY INDUSTRY, INCLUDING, BUT NOT LIMITED TO, THE FEDERAL DEPARTMENT OF COMMERCE'S NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, THE INTERNATIONAL STANDARDS ORGANIZATION, AND THE PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL.

(B) "Personal information" shall mean any information concerning a natural person which, because of name, number, [personal] SYMBOL, mark[,] or other identifier, can be used to identify [such] THAT natural person;

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

(1) social security number;

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

LBD08460-03-9

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

(3) FINANCIAL 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;].

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

PRIVATE INFORMATION SHALL NOT BE CONSIDERED TO BE ENCRYPTED FOR PURPOSES OF THIS SECTION IF IT IS ACQUIRED IN COMBINATION WITH ANY KEY REQUIRED TO ENABLE DECRYPTION OF THAT PRIVATE INFORMATION.

[(c)] (D) "Breach of the security of the system" shall mean: (1) unauthorized acquisition [or acquisition without valid authorization] of computerized data that compromises the security, confidentiality, or integrity of [personal] PRIVATE information maintained by a business; OR (2) WHEN IT IS REASONABLY BELIEVED THAT SUCH UNAUTHORIZED ACQUISITION HAS OCCURRED. Good faith OR INADVERTENT acquisition of [personal] PRIVATE information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system[, provided that the private information is not used or subject to unauthorized disclosure].

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

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

[(2)] (II) indications that the PRIVATE information has been downloaded or copied; or

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

[(d)] (E) "Consumer reporting agency" shall mean any [person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports] CONSUMER REPORTING AGENCY THAT COMPILES AND MAINTAINS FILES ON CONSUMERS ON A NATIONWIDE BASIS, AS DEFINED BY 15 U.S.C. S 1681A(P). A list of consumer reporting agencies shall be compiled by the state attorney general. SUCH LIST SHALL BE UPDATED BY THE ATTORNEY GENERAL ANNUALLY and SHALL BE furnished upon request IN A FORMAT OR FORMATS PRESCRIBED BY THE ATTORNEY GENERAL to any person or business required to make a notification under subdivision two of this section.

2. Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall: (A) IMPLEMENT AND MAINTAIN REASONABLE SECURITY SAFEGUARDS, APPROPRIATE TO THE NATURE OF THE INFORMATION, TO PREVENT UNAUTHORIZED ACCESS TO OR UNAUTHORIZED DESTRUCTION, USE, MODIFICATION, OR DISCLOSURE OF THE PRIVATE INFORMATION; AND (B) disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was[, or is reasonably believed to have been,

acquired by a person without valid authorization] SUBJECT TO THE BREACH OF THE SECURITY OF THE SYSTEM. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

3. Any person or business which maintains computerized data which includes private information which such person or business does not own shall: (A) IMPLEMENT AND MAINTAIN REASONABLE SECURITY SAFEGUARDS, APPROPRIATE TO THE NATURE OF THE INFORMATION, TO PREVENT UNAUTHORIZED ACCESS TO OR UNAUTHORIZED DESTRUCTION, USE, MODIFICATION, OR DISCLOSURE OF THE PRIVATE INFORMATION; AND (B) notify the owner or licensee of the information of any breach of the security of the system immediately following discovery[, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization] OF THE BREACH OF THE SECURITY OF THE SYSTEM AND SHALL COOPERATE WITH THE OWNER OR LICENSEE TO DETERMINE THE SCOPE OF THE BREACH AND RESTORE THE REASONABLE INTEGRITY OF THE SYSTEM. UNLESS THE PERSON OR BUSINESS WHO MAINTAINS COMPUTERIZED DATA WHICH IT DOES NOT OWN AND THE OWNER OR LICENSEE OF THAT DATA HAVE AGREED OTHERWISE IN WRITING, THE PERSON OR BUSINESS WHO MAINTAINS COMPUTERIZED DATA WHICH IT DOES NOT OWN SHALL BE LIABLE FOR THE COSTS ASSOCIATED WITH PROVIDING THE NOTIFICATIONS REQUIRED BY SUBDIVISIONS FIVE AND EIGHT OF THIS SECTION IF THE BREACH WAS CAUSED BY NEGLIGENT OR WILLFUL ACTS OR OMISSIONS OF THE PERSON OR BUSINESS, OR THE NEGLIGENT OR WILLFUL ACTS OR OMISSIONS OF AGENTS, OFFICERS, EMPLOYEES OR SUBCONTRACTORS OF THE PERSON OR BUSINESS.

4. The [notification] NOTIFICATIONS required by SUBDIVISIONS FIVE AND EIGHT OF this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation, PROVIDED THAT SUCH DETERMINATION IS MADE IN WRITING OR THE PERSON OR BUSINESS DOCUMENTS THE DETERMINATION CONTEMPORANEOUSLY IN WRITING, INCLUDING THE NAME OF THE LAW ENFORCEMENT OFFICER MAKING THE DETERMINATION AND THE LAW ENFORCEMENT AGENCY ENGAGED IN THE INVESTIGATION. The [notification] NOTIFICATIONS required by SUBDIVISIONS FIVE AND EIGHT OF this section shall be made IN THE MOST EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY after such law enforcement agency determines that such notification [does not] WOULD NO LONGER compromise such investigation. WRITTEN DOCUMENTATION OF THE FOREGOING DETERMINATIONS BY A LAW ENFORCEMENT AGENCY SHALL ACCOMPANY THE NOTIFICATION REQUIRED BY SUBDIVISION EIGHT OF THIS SECTION.

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

(a) written notice, WHICH SHALL BE IN AT LEAST TWELVE POINT TYPE;

(b) electronic notice, [provided that the] FOR THOSE AFFECTED PERSONS FOR WHOM THE PERSON OR BUSINESS HAS A VALID E-MAIL ADDRESS ONLY IF: (1) THE PERSON OR BUSINESS DOES NOT HAVE THE AFFECTED PERSON'S ADDRESS OR TELEPHONE CONTACT INFORMATION AND THE PERSON'S OR BUSINESS'S PRIMARY METHOD OF COMMUNICATION WITH THE AFFECTED PERSON IS BY ELECTRONIC MEANS; OR (2) THE AFFECTED person [to whom notice is required] has expressly consented to receiving said notice in electronic form [and]. ELECTRONIC NOTICES AUTHORIZED UNDER THIS PARAGRAPH SHALL NOT REQUEST OR CONTAIN A HYPERTEXT LINK TO A REQUEST THAT THE AFFECTED PERSON PROVIDE PRIVATE INFORMATION AND SHALL INCLUDE A CONSPICUOUS WARNING THAT THE AFFECTED PERSON SHOULD NOT PROVIDE PRIVATE INFORMATION IN RESPONSE TO ELECTRONIC COMMUNICATIONS REGARDING SECURITY BREACHES. THE PERSON OR BUSINESS SHALL KEEP 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]. IN no case shall any person or business require a person to consent to accepting said notice in [said] ELECTRONIC 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 PERSON OR 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 PERSON OR business does not have sufficient contact information. Substitute notice shall consist of all of the following:

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

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

(3) notification to [major statewide] APPROPRIATE media IN THE AREAS IN WHICH THE PERSON OR BUSINESS REASONABLY DETERMINES THAT THE NEW YORK RESIDENTS TO BE NOTIFIED RESIDE.

6. (a) whenever the attorney general shall believe from evidence satisfactory to him that there is a violation of this article he 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, if notification was not provided to such person pursuant to this article, including consequential financial losses. Whenever the court shall determine in such action that a person or business violated this article 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 dollars.

(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 two years immediately after the date of the act complained of or the date of discovery of such act.

7. Regardless of the method by which notice is provided, such notice shall include, AT A MINIMUM: (A) contact information for the person or business making the notification [and], INCLUDING: (1) A TELEPHONE NUMBER OR A TOLL-FREE TELEPHONE NUMBER, IF ONE IS MAINTAINED BY THE PERSON OR BUSINESS; (2) A MAILING ADDRESS; AND (3) AN E-MAIL ADDRESS, IF ONE IS MAINTAINED BY THE PERSON OR BUSINESS;

(B) a description of the categories of information [that were, or are reasonably believed to have been, acquired by a person without valid authorization], including specification of [which of] the elements of personal information and private information, THAT were[, or are reasonably believed to have been, so acquired] SUBJECT TO THE BREACH OF THE SECURITY OF THE SYSTEM;

(C) A WARNING TO AFFECTED PERSONS NOT TO PROVIDE PRIVATE INFORMATION IN RESPONSE TO ELECTRONIC COMMUNICATIONS REGARDING SECURITY BREACHES;

(D) INFORMATION RELATING TO OBTAINING AND REVIEWING FREE CREDIT REPORTS AND PLACING FREE SECURITY FREEZES AND FRAUD ALERTS ON CREDIT

REPORTS, INCLUDING TOLL-FREE TELEPHONE NUMBERS, E-MAIL ADDRESSES, WEBSITE ADDRESSES, AND MAILING ADDRESSES FOR THE CONSUMER REPORTING AGENCIES;

(E) A RECOMMENDATION THAT INCIDENTS OF IDENTITY THEFT BE REPORTED PROMPTLY TO LAW ENFORCEMENT AGENCIES, THE CONSUMER PROTECTION BOARD, THE FEDERAL TRADE COMMISSION, AND THE CONSUMER REPORTING AGENCIES; AND

(F) THE TOLL-FREE TELEPHONE NUMBER, E-MAIL ADDRESS, WEBSITE ADDRESS, AND MAILING ADDRESS OF THE CONSUMER PROTECTION BOARD.

8. (a) In the event that any New York residents are to be notified, the person or business shall notify the state attorney general, the consumer protection board, and the state office of cyber security and critical infrastructure coordination as to the timing, content and distribution of the notices [and], THE approximate number of affected persons, AND THE APPROXIMATE NUMBER OF AFFECTED NEW YORK RESIDENTS. Such notice shall be made without delaying notice to affected New York residents.

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

(C) IN THE EVENT THAT THE AFFECTED CLASS OF SUBJECT PERSONS TO BE NOTIFIED EXCEEDS FIVE HUNDRED THOUSAND, THE PERSON OR BUSINESS SHALL, WITHIN ONE HUNDRED TWENTY DAYS OF THE NOTIFICATION REQUIRED BY SUBDIVISION FIVE OF THIS SECTION, FILE A REPORT WITH THE ATTORNEY GENERAL, THE CONSUMER PROTECTION BOARD, AND THE STATE OFFICE OF CYBER SECURITY AND CRITICAL INFRASTRUCTURE COORDINATION DESCRIBING THE STEPS TAKEN TO MITIGATE THE EFFECTS OF THE BREACH IN THE SECURITY OF THE SYSTEM, INCLUDING, BUT NOT LIMITED TO, IMPLEMENTATION OF PROCEDURES FOR DETECTING, REPORTING, AND RESPONDING TO SUCH BREACHES, PROVIDED, HOWEVER, THAT THE PERSON OR BUSINESS SHALL NOT BE REQUIRED TO INCLUDE INFORMATION IN THE REPORT THAT IS SPECIFICALLY EXEMPTED FROM DISCLOSURE BY STATE OR FEDERAL LAW OR THAT WOULD, IF DISCLOSED, JEOPARDIZE THE PERSON'S OR BUSINESS'S CAPACITY TO GUARANTEE THE SECURITY OF INFORMATION TECHNOLOGY ASSETS, SUCH ASSETS ENCOMPASSING BOTH ELECTRONIC INFORMATION SYSTEMS AND INFRASTRUCTURES.

9. The provisions of this section shall be exclusive and shall preempt any provisions of local law, ordinance or code, and no locality shall impose requirements that are inconsistent with or more restrictive than those set forth in this section.

S 2. Section 208 of the state technology law, as added by chapter 442 of the laws of 2005, paragraph (b) of subdivision 1 and subdivisions 2, 6 and 7 as amended, paragraph (c) of subdivision 5 as added and paragraph (d) of subdivision 5 as relettered by chapter 491 of the laws of 2005, is amended to read as follows:

S 208. Notification; [person without valid authorization has acquired] UNAUTHORIZED ACQUISITION OF private information. 1. As used in this section, the following terms shall have the following meanings:

(a) "ENCRYPTED" SHALL MEAN THE PROTECTION OF PRIVATE INFORMATION IN ELECTRONIC FORM IN STORAGE OR IN TRANSIT USING AN ENCRYPTION TECHNOLOGY THAT HAS BEEN ADOPTED BY A STANDARDS SETTING BODY GENERALLY RECOGNIZED IN THE INFORMATION TECHNOLOGY INDUSTRY, INCLUDING, BUT NOT LIMITED TO, THE FEDERAL DEPARTMENT OF COMMERCE'S NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, THE INTERNATIONAL STANDARDS ORGANIZATION, AND THE PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL.

(B) "PERSONAL INFORMATION" SHALL MEAN PERSONAL INFORMATION AS DEFINED BY SUBDIVISION FIVE OF SECTION TWO HUNDRED TWO OF THIS ARTICLE.

(C) "Private information" shall mean personal information in combination with any one or more of the following data elements, when [either] BOTH the personal information [or] AND the data element [is] ARE 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) FINANCIAL 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].

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

PRIVATE INFORMATION SHALL NOT BE CONSIDERED TO BE ENCRYPTED FOR PURPOSES OF THIS SECTION IF IT IS ACQUIRED IN COMBINATION WITH ANY KEY REQUIRED TO ENABLE DECRYPTION OF THAT PRIVATE INFORMATION.

[(b)] (D) "Breach of the security of the system" shall mean: (1) unauthorized acquisition [or acquisition without valid authorization] of computerized data which compromises the security, confidentiality, or integrity of [personal] PRIVATE information maintained by a state entity; OR (2) WHEN IT IS REASONABLY BELIEVED THAT SUCH UNAUTHORIZED ACQUISITION HAS OCCURRED. Good faith OR INADVERTENT acquisition of [personal] PRIVATE information by an employee or agent of a state entity for the purposes of the agency is not a breach of the security of the system[, provided that the private information is not used or subject to unauthorized disclosure].

In determining whether PRIVATE information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person [or a person without valid authorization], such state entity may consider the following factors, among others:

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

[(2)] (II) indications that the PRIVATE information has been downloaded or copied; or

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

[(c)] (E) "State entity" shall mean any state board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the state of New York, except:

(1) the judiciary; and

(2) [all cities, counties, municipalities, villages, towns, and other local agencies] COUNTIES, CITIES, TOWNS, VILLAGES, SCHOOL DISTRICTS, BOARDS OF COOPERATIVE EDUCATIONAL SERVICES, LOCAL PUBLIC BENEFIT CORPORATIONS AND OTHER MUNICIPAL CORPORATIONS OR POLITICAL SUBDIVISIONS OF THE STATE.

[(d)] (F) "Consumer reporting agency" shall mean any [person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports] CONSUMER REPORTING AGENCY THAT

COMPILES AND MAINTAINS FILES ON CONSUMERS ON A NATIONWIDE BASIS, AS DEFINED BY 15 U.S.C. S 1681A(P). A list of consumer reporting agencies shall be compiled by the state attorney general. SUCH LIST SHALL BE UPDATED BY THE ATTORNEY GENERAL ANNUALLY and SHALL BE furnished upon request IN A FORMAT OR FORMATS PRESCRIBED BY THE ATTORNEY GENERAL to ANY state [entities] ENTITY required to make a notification under subdivision two of this section.

2. Any state entity that owns or licenses computerized data that includes private information shall: (A) CONSISTENT WITH ITS OBLIGATIONS UNDER THE PERSONAL PRIVACY PROTECTION LAW, IMPLEMENT AND MAINTAIN REASONABLE SECURITY SAFEGUARDS, APPROPRIATE TO THE NATURE OF THE INFORMATION, TO PREVENT UNAUTHORIZED ACCESS TO OR UNAUTHORIZED DESTRUCTION, USE, MODIFICATION, OR DISCLOSURE OF THE PRIVATE INFORMATION; AND (B) disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was[, or is reasonably believed to have been, acquired by a person without valid authorization] SUBJECT TO THE BREACH OF THE SECURITY OF THE SYSTEM. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The state entity shall consult with the state office of cyber security and critical infrastructure coordination to determine the scope of the breach and restoration measures.

3. Any state entity that maintains computerized data that includes private information which such agency does not own shall: (A) CONSISTENT WITH ITS OBLIGATIONS UNDER THE PERSONAL PRIVACY PROTECTION LAW, IMPLEMENT AND MAINTAIN REASONABLE SECURITY SAFEGUARDS, APPROPRIATE TO THE NATURE OF THE INFORMATION, TO PREVENT UNAUTHORIZED ACCESS TO OR UNAUTHORIZED DESTRUCTION, USE, MODIFICATION, OR DISCLOSURE OF THE PRIVATE INFORMATION; AND (B) notify the owner or licensee of the information of any breach of the security of the system immediately following discovery[, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization] OF THE BREACH OF THE SECURITY OF THE SYSTEM AND SHALL COOPERATE WITH THE CONSULTATION DESCRIBED IN SUBDIVISION TWO OF THIS SECTION.

4. The [notification] NOTIFICATIONS required by SUBDIVISIONS FIVE AND SEVEN OF this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation PROVIDED THAT SUCH DETERMINATION IS MADE IN WRITING OR THE STATE ENTITY DOCUMENTS THE DETERMINATION CONTEMPORANEOUSLY IN WRITING, INCLUDING THE NAME OF THE LAW ENFORCEMENT OFFICER MAKING THE DETERMINATION AND THE LAW ENFORCEMENT AGENCY ENGAGED IN THE INVESTIGATION. The [notification] NOTIFICATIONS required by SUBDIVISIONS FIVE AND SEVEN OF this section shall be made IN THE MOST EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY after such law enforcement agency determines that such notification [does not] WOULD NO LONGER compromise such investigation. WRITTEN DOCUMENTATION OF THE FOREGOING DETERMINATIONS BY A LAW ENFORCEMENT AGENCY SHALL ACCOMPANY THE NOTIFICATION REQUIRED BY SUBDIVISION SEVEN OF THIS SECTION.

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

(a) written notice, WHICH SHALL BE IN AT LEAST TWELVE POINT TYPE;

(b) electronic notice, [provided that] FOR THOSE AFFECTED PERSONS FOR WHOM THE STATE ENTITY HAS A VALID E-MAIL ADDRESS ONLY IF: (1) THE STATE

ENTITY DOES NOT HAVE THE AFFECTED PERSON'S ADDRESS OR TELEPHONE CONTACT INFORMATION AND THE STATE ENTITY'S PRIMARY METHOD OF COMMUNICATION WITH THE AFFECTED PERSON IS BY ELECTRONIC MEANS; OR (2) the AFFECTED person [to whom notice is required] has expressly consented to receiving said notice in electronic form [and]. ELECTRONIC NOTICES AUTHORIZED UNDER THIS PARAGRAPH SHALL NOT REQUEST OR CONTAIN A HYPERTEXT LINK TO A REQUEST THAT THE AFFECTED PERSON PROVIDE PRIVATE INFORMATION AND SHALL INCLUDE A CONSPICUOUS WARNING THAT THE AFFECTED PERSON SHOULD NOT PROVIDE PRIVATE INFORMATION IN RESPONSE TO ELECTRONIC COMMUNICATIONS REGARDING SECURITY BREACHES. THE STATE ENTITY SHALL KEEP a log of each such notification [is kept by the state entity who notifies affected persons in such form; provided further, however, that in]. IN no case shall any [person or business] STATE ENTITY require a person to consent to accepting said notice in [said] ELECTRONIC 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 state entity who notifies affected persons; or

(d) Substitute notice, if a state entity 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 agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

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

(2) conspicuous posting of the notice on such state entity's web site page, if such [agency] STATE ENTITY maintains one; and

(3) notification to [major statewide] APPROPRIATE media IN THE AREAS IN WHICH THE STATE ENTITY REASONABLY DETERMINES THAT THE NEW YORK RESIDENTS TO BE NOTIFIED RESIDE.

6. Regardless of the method by which notice is provided, such notice shall include, AT A MINIMUM: (A) contact information for the state entity making the notification, INCLUDING: (1) A TELEPHONE NUMBER OR A TOLL-FREE TELEPHONE NUMBER, IF ONE IS MAINTAINED BY THE STATE ENTITY; (2) A MAILING ADDRESS; AND (3) AN E-MAIL ADDRESS, IF ONE IS MAINTAINED BY THE STATE ENTITY; (B) and a description of the categories of information [that were, or are reasonably believed to have been, acquired by a person without valid authorization], including specification of [which of] the elements of personal information and private information, were[, or are reasonably believed to have been, so acquired] SUBJECT TO THE BREACH OF THE SECURITY OF THE SYSTEM; (C) A WARNING TO AFFECTED PERSONS NOT TO PROVIDE PRIVATE INFORMATION IN RESPONSE TO ELECTRONIC COMMUNICATIONS REGARDING SECURITY BREACHES; (D) INFORMATION RELATING TO OBTAINING AND REVIEWING FREE CREDIT REPORTS AND PLACING FREE SECURITY FREEZES AND FREE FRAUD ALERTS ON CREDIT REPORTS, INCLUDING TOLL-FREE TELEPHONE NUMBERS, E-MAIL ADDRESSES, WEBSITE ADDRESSES, AND MAILING ADDRESSES FOR THE CONSUMER REPORTING AGENCIES; (E) A RECOMMENDATION THAT INCIDENTS OF IDENTITY THEFT BE REPORTED PROMPTLY TO LAW ENFORCEMENT AGENCIES, THE CONSUMER PROTECTION BOARD, THE FEDERAL TRADE COMMISSION, AND THE CONSUMER REPORTING AGENCIES; AND (F) THE TOLL-FREE TELEPHONE NUMBER, E-MAIL ADDRESS, WEBSITE ADDRESS, AND MAILING ADDRESS OF THE CONSUMER PROTECTION BOARD.

7. (a) In the event that any New York residents are to be notified, the state entity shall notify the state attorney general, the consumer protection board, and the state office of cyber security and critical infrastructure coordination as to the timing, content and distribution

of the notices [and], THE approximate number of affected persons, AND THE APPROXIMATE NUMBER OF AFFECTED NEW YORK RESIDENTS. Such notice shall be made without delaying notice to affected New York residents.

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

(C) IN THE EVENT THAT THE AFFECTED CLASS OF SUBJECT PERSONS TO BE NOTIFIED EXCEEDS FIVE HUNDRED THOUSAND, THE STATE ENTITY SHALL, WITHIN ONE HUNDRED TWENTY DAYS OF THE NOTICE REQUIRED BY SUBDIVISION FIVE OF THIS SECTION, FILE A REPORT WITH THE STATE ATTORNEY GENERAL, THE CONSUMER PROTECTION BOARD, AND THE STATE OFFICE OF CYBER SECURITY AND CRITICAL INFRASTRUCTURE COORDINATION DESCRIBING THE STEPS TAKEN TO MITIGATE THE EFFECTS OF THE BREACH IN THE SECURITY OF THE SYSTEM, INCLUDING, BUT NOT LIMITED TO, IMPLEMENTATION OF PROCEDURES FOR DETECTING, REPORTING, AND RESPONDING TO SUCH BREACHES, PROVIDED, HOWEVER, THAT THE STATE ENTITY SHALL NOT BE REQUIRED TO INCLUDE INFORMATION IN THE REPORT THAT IS SPECIFICALLY EXEMPTED FROM DISCLOSURE BY STATE OR FEDERAL LAW OR THAT WOULD, IF DISCLOSED, JEOPARDIZE THE STATE ENTITY'S CAPACITY TO GUARANTEE THE SECURITY OF ITS INFORMATION TECHNOLOGY ASSETS, SUCH ASSETS ENCOMPASSING BOTH ELECTRONIC INFORMATION SYSTEMS AND INFRASTRUCTURES.

8. Any entity listed in subparagraph two of paragraph [(c)] (E) of subdivision one of this section shall adopt a notification policy [no more than one hundred twenty days after the effective date of this section. Such entity may develop a notification policy] which is consistent with this section or alternatively shall adopt a local law which is consistent with this section. SUCH ENTITY SHALL FILE A COPY OF ITS POLICY OR LOCAL LAW WITH THE CONSUMER PROTECTION BOARD WITHIN NINETY DAYS OF ITS ADOPTION.

S 3. This act shall take effect on the one hundred eightieth day after it shall have become a law.