

2005 N.Y. S.N. 5827


Enacted, August 9, 2005

Reporter

2005 N.Y. ALS 491; 2005 N.Y. LAWS 491; 2005 N.Y. S.N. 5827

NEW YORK ADVANCE LEGISLATIVE SERVICE > NEW YORK 228TH ANNUAL LEGISLATIVE SESSION 2005-2006 Regular Sessions > CHAPTER 491 > SENATE BILL 5827

Notice

 [A> UPPERCASE TEXT WITHIN THESE SYMBOLS IS ADDED <A]
[D> Text within these symbols is deleted <D]

Synopsis

AN ACT to amend a chapter of the laws of 2005 amending the state technology law and the general business law relating to enacting the "information security breach and notification act" in relation to the legislative intent of such act and to amend the state technology law and the general business law, in relation to the "information security breach and notification act"

Text

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

Section 1. Section 2 of a chapter of the laws of 2005 amending the state technology law and the general business law relating to enacting the "information security breach and notification act", as proposed in legislative bills numbers S.3492-A and A.4254-A, is amended to read as follows:

Section 2. Legislative Intent. The legislature finds that identity theft and security breaches have affected thousands statewide and millions of people nationwide. The legislature also finds that affected persons are hindered by a lack of information regarding breaches, and that the impact of exposing information that should be held private can be farreaching. In addition, the Legislature finds that state residents deserve a right to know when they have been exposed to identity theft. The legislature further finds that affected state residents deserve an advocate who can speak and take action on their behalf because recovering from identity theft can, and sometimes does, take many years.

Therefore, the legislature enacts the information security breach and notification act which will guarantee state residents the right to know what information was exposed during a breach, so that they can take the necessary steps to both prevent and repair any damage [D> they may incur because of a public or private sector entity's failure to make proper notification <D] [A> THAT HAS OR MAY OCCUR AS A RESULT OF THE BREACH <A] .

Section 2. Paragraph (b) of subdivision 1 and subdivision 2 of section 208 of the state technology law, as added by a chapter of the laws of 2005 amending the state technology law and the general business law relating to enacting

the "information security breach and notification act", as proposed in legislative bills numbers S.3492-A and A.4254-A, are amended to read as follows:

(b) "Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by a state entity. Good faith acquisition of personal 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.

[A> IN DETERMINING WHETHER 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: <A]

[A> (1) INDICATIONS THAT THE INFORMATION IS IN THE PHYSICAL POSSESSION AND CONTROL OF AN UNAUTHORIZED PERSON, SUCH AS A LOST OR STOLEN COMPUTER OR OTHER DEVICE CONTAINING INFORMATION; OR <A]

[A> (2) INDICATIONS THAT THE INFORMATION HAS BEEN DOWNLOADED OR COPIED; OR <A]

[A> (3) INDICATIONS THAT THE INFORMATION WAS USED BY AN UNAUTHORIZED PERSON, SUCH AS FRAUDULENT ACCOUNTS OPENED OR INSTANCES OF IDENTITY THEFT REPORTED. <A]

2. Any state entity that owns or licenses computerized data that includes private information shall 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. 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. [A> 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. <A]

Section 3. Paragraph (c) of subdivision 5 of section 208 of the state technology law, as added by a chapter of the laws of 2005 amending the state technology law and the general business law relating to enacting the "information security breach and notification act", as proposed in legislative bills numbers S.3492-A and A.4254-A, is relettered paragraph (d) and a new paragraph (c) is added to read as follows:

[A> (C) TELEPHONE NOTIFICATION PROVIDED THAT A LOG OF EACH SUCH NOTIFICATION IS KEPT BY THE STATE ENTITY WHO NOTIFIES AFFECTED PERSONS; OR <A]

Section 4. Subdivisions 6 and 7 of section 208 of the state technology law, as added by a chapter of the laws of 2005 amending the state technology law and the general business law relating to enacting the "information security breach and notification act", as proposed in legislative bills numbers S.3492-A and A.4254-A, are amended to read as follows:

6. Regardless of the method by which notice is provided, such notice shall include contact information for the [D> person or business <D] [A> STATE ENTITY <A] making the notification 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.

7. (a) In the event that any New York residents are to be notified [D> at one time <D] , the [D> person or business <D] [A> STATE ENTITY <A] 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 approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

[A> (B) <A] In the event that more than five thousand New York residents are to be notified at one time, the [D> person or business <D] [A> STATE ENTITY <A] 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.

Section 5. Paragraph (c) of subdivision 1 of [section 899-aa of the general business law](#), as added by a chapter of the laws of 2005 amending the state technology law and the general business law relating to enacting the "information security breach and notification act", as proposed in legislative bills numbers S.3492-A and A.4254-A, is amended to read as follows:

(c) "Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. Good faith acquisition of personal 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.

[A> IN DETERMINING WHETHER 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: <A]

[A> (1) INDICATIONS THAT THE INFORMATION IS IN THE PHYSICAL POSSESSION AND CONTROL OF AN UNAUTHORIZED PERSON, SUCH AS A LOST OR STOLEN COMPUTER OR OTHER DEVICE CONTAINING INFORMATION; OR <A]

[A> (2) INDICATIONS THAT THE INFORMATION HAS BEEN DOWNLOADED OR COPIED; OR <A]

[A> (3) INDICATIONS THAT THE INFORMATION WAS USED BY AN UNAUTHORIZED PERSON, SUCH AS FRAUDULENT ACCOUNTS OPENED OR INSTANCES OF IDENTITY THEFT REPORTED. <A]

Section 6. Paragraph (a) of subdivision 6 of [section 899-aa of the general business law](#), as added by a chapter of the laws of 2005 amending the state technology law and the general business law relating to enacting the "information security breach and notification act", as proposed in legislative bills numbers S.3492-A and A.4254-A, is amended to read as follows:

(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, [A> IF NOTIFICATION WAS NOT PROVIDED TO SUCH PERSON PURSUANT TO THIS ARTICLE, <A] 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.

Section 7. Subdivision 8 of [section 899-aa of the general business law](#), as added by a chapter of the laws of 2005 amending the state technology law and the general business law relating to enacting the "information security

breach and notification act", as proposed in legislative bills numbers S.3492-A and A.4254-A, is amended to read as follows:

8. (a) In the event that any New York residents are to be notified **[D>** at one time **<D]** , 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 approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

(b) In the event that more than five 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.

Section 8. This act shall take effect on the same date and in the same manner as a chapter of the laws of 2005 amending the state technology law and the general business law relating to enacting the "information security breach and notification act" as proposed in legislative bills numbers S.3492-A and A.4254-A, takes effect.

History

Enacted August 9, 2005

Sponsor

Introduced by Sens. FUSCHILLO, SPANO, GOLDEN, LEIBELL, NOZZOLIO -- read twice and ordered printed, and when printed to be committed to the Committee on Rules Introduced by COMMITTEE ON RULES -- (at request of M. of A. Brennan) -- read once and referred to the Committee on Governmental Operations

NEW YORK ADVANCE LEGISLATIVE SERVICE
Copyright © 2022 LexisNexis. All rights reserved.