



**94TH GENERAL ASSEMBLY**  
**State of Illinois**  
**2005 and 2006**  
**SB1899**

Introduced 2/25/2005, by Sen. Dan Cronin

**SYNOPSIS AS INTRODUCED:**

New Act

Creates the Identity Theft Notification Act. Requires any agency, person, or business that conducts business in Illinois and owns or licenses data that includes personal information concerning an Illinois resident to notify the resident that there has been a breach of the security of that data following discovery or notification of the breach. Requires any agency, person, or business that maintains data that includes personal information concerning an Illinois resident and that the agency, person, or business does not own to notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been acquired by an unauthorized person. Provides that notice may be provided in one of the following ways: (1) written notice; (2) electronic notice; or (3) substitute notice if the agency, person, or business demonstrates that the cost of providing notice would exceed \$250,000, or the affected class of persons to be notified exceeds 500,000, or the agency, person, or business does not have sufficient contact information.

LRB094 11231 RXD 41958 b

1 AN ACT concerning business.

2 **Be it enacted by the People of the State of Illinois,**  
3 **represented in the General Assembly:**

4 Section 1. Short title. This Act may be cited as the  
5 Identity Theft Notification Act.

6 Section 5. Definitions. In this Act:

7 "Breach of the security of the data" means unauthorized  
8 acquisition of data that compromises the security and  
9 confidentiality of personal information maintained by an  
10 agency, person, or business.

11 "Breach of the security of the data" does not include good  
12 faith acquisition of personal information by an employee or  
13 agent of the agency, person, or business, provided that the  
14 personal information is not used for a purpose unrelated to the  
15 business of the agency, person, or business or subjected to  
16 further unauthorized disclosure.

17 "Personal information" means an individual's first name or  
18 first initial and last name in combination with any one or more  
19 of the following data elements, when the data elements are not  
20 encrypted or redacted:

21 (1) Social security number.

22 (2) Driver's license number or Illinois State  
23 Identification Card number.

24 (3) Account number or credit or debit card number, in  
25 combination with any required security code, access code,  
26 or password that would permit access to an individual's  
27 financial account.

28 "Personal information" does not include publicly available  
29 information that is lawfully made available to the general  
30 public from federal, State, or local government records.

31 Section 10. Security breach; notification.

1 (a) Any agency, person, or business that conducts business  
2 in Illinois and that owns or licenses data that includes  
3 personal information concerning an Illinois resident shall  
4 notify the resident that there has been a breach of the  
5 security of that data following discovery or notification of  
6 the breach. The notification shall be made in the most  
7 expedient time possible and without unreasonable delay,  
8 consistent with the legitimate needs of the law enforcement  
9 agency, as provided in subsection (d), or any measures  
10 necessary to determine the scope of the breach and restore the  
11 reasonable security and confidentiality of the data.

12 (b) Any agency, person, or business that maintains data  
13 that includes personal information concerning an Illinois  
14 resident and that the agency, person, or business does not own  
15 shall notify the owner or licensee of the information of any  
16 breach of the security of the data immediately following  
17 discovery, if the personal information was, or is reasonably  
18 believed to have been acquired by an unauthorized person.

19 (c) Notice may be provided by one of the following methods:

20 (1) written notice;

21 (2) electronic notice, if the notice provided is  
22 consistent with the provisions regarding electronic  
23 records and signatures set forth in Section 7001 of Title  
24 15 of the United States Code; or

25 (3) substitute notice, if the agency, person, or  
26 business demonstrates that the cost of providing notice  
27 would exceed \$250,000, or the affected class of persons to  
28 be notified exceeds 500,000, or the agency, person, or  
29 business does not have sufficient contact information.

30 Substitute notice shall consist of all of the following:

31 (i) email notification if the agency, person, or business  
32 has an email address for the person to be notified; (ii)  
33 conspicuous posting of the notice on the web site page of  
34 the agency, person, or business, if the agency, person, or  
35 business maintains a web site page; and (iii) notification  
36 to major statewide media outlets.

1           (d) The notification required under this Section may be  
2 delayed if a law enforcement agency determines that the  
3 notification will impede a criminal investigation.  
4 Notification shall be made after the law enforcement agency  
5 determines that it will not compromise its investigation.  
6 Notification shall not be required if, as a result of an  
7 investigation, the law enforcement agency concludes that  
8 personal information was not acquired by an unauthorized  
9 person.

10           (e) Notwithstanding subsection (c) of this Section, any  
11 agency, person, or business that maintains its own notification  
12 procedures as part of an information security policy for the  
13 treatment of personal information and is otherwise consistent  
14 with the timing requirements of this Section shall be deemed to  
15 be in compliance with the notification requirements of this  
16 Section if the agency, person, or business notifies the subject  
17 persons in accordance with its policies in the event of a  
18 breach of security of the data.