



94TH GENERAL ASSEMBLY

State of Illinois

2005 and 2006

HB4253

Introduced 12/15/2005, by Rep. Thomas Holbrook

SYNOPSIS AS INTRODUCED:

815 ILCS 530/5
815 ILCS 530/10
815 ILCS 530/25 new

Amends the Personal Information Protection Act. Changes the definition of "breach of security of the system data" to "breach of the security of the system data or written material". Provides that the notice requirements of the Act apply to breaches of written material containing personal information. Provides that any State agency that collects personal data and has had a breach of security of the system data or written material shall submit an annual report to the General Assembly listing the breaches and outlining any corrective measures that have been taken to prevent future breaches of the security of the system data or written material. Effective immediately.

LRB094 15513 LCT 50712 b

FISCAL NOTE ACT
MAY APPLY

1 AN ACT concerning consumer fraud.

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

4 Section 5. The Personal Information Protection Act is
5 amended by changing Sections 5 and 10 and by adding Section 25
6 as follows:

7 (815 ILCS 530/5)

8 Sec. 5. Definitions. In this Act:

9 "Data Collector" may include, but is not limited to,
10 government agencies, public and private universities,
11 privately and publicly held corporations, financial
12 institutions, retail operators, and any other entity that, for
13 any purpose, handles, collects, disseminates, or otherwise
14 deals with nonpublic personal information.

15 "Breach of the security of the system data or written
16 material" means unauthorized acquisition of computerized data
17 or written material that compromises the security,
18 confidentiality, or integrity of personal information
19 maintained by the data collector. "Breach of the security of
20 the system data" does not include good faith acquisition of
21 personal information by an employee or agent of the data
22 collector for a legitimate purpose of the data collector,
23 provided that the personal information is not used for a
24 purpose unrelated to the data collector's business or subject
25 to further unauthorized disclosure.

26 "Personal information" means an individual's first name or
27 first initial and last name in combination with any one or more
28 of the following data elements, when either the name or the
29 data elements are not encrypted or redacted:

30 (1) Social Security number.

31 (2) Driver's license number or State identification
32 card number.

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

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

8 (Source: P.A. 94-36, eff. 1-1-06.)

9 (815 ILCS 530/10)

10 Sec. 10. Notice of Breach.

11 (a) Any data collector that owns or licenses personal
12 information concerning an Illinois resident shall notify the
13 resident that there has been a breach of the security of the
14 system data or written material following discovery or
15 notification of the breach. The disclosure notification shall
16 be made in the most expedient time possible and without
17 unreasonable delay, consistent with any measures necessary to
18 determine the scope of the breach and restore the reasonable
19 integrity, security, and confidentiality of the data system or
20 written material files.

21 (b) Any data collector that maintains computerized data
22 that includes personal information that the data collector does
23 not own or license shall notify the owner or licensee of the
24 information of any breach of the security of the data
25 immediately following discovery, if the personal information
26 was, or is reasonably believed to have been, acquired by an
27 unauthorized person.

28 (b-5) Any data collector that maintains material files that
29 include personal information that the data collector does not
30 own or license shall notify the owner or licensee of the
31 information of any breach of the security of the data or
32 material files immediately following discovery, if the
33 personal information was, or is reasonably believed to have
34 been, acquired by an unauthorized person.

35 (c) For purposes of this Section, notice to consumers may

1 be provided by one of the following methods:

2 (1) written notice;

3 (2) electronic notice, if the notice provided is
4 consistent with the provisions regarding electronic
5 records and signatures for notices legally required to be
6 in writing as set forth in Section 7001 of Title 15 of the
7 United States Code; or

8 (3) substitute notice, if the data collector
9 demonstrates that the cost of providing notice would exceed
10 \$250,000 or that the affected class of subject persons to
11 be notified exceeds 500,000, or the data collector does not
12 have sufficient contact information. Substitute notice
13 shall consist of all of the following: (i) email notice if
14 the data collector has an email address for the subject
15 persons; (ii) conspicuous posting of the notice on the data
16 collector's web site page if the data collector maintains
17 one; and (iii) notification to major statewide media.

18 (d) Notwithstanding subsection (c), a data collector that
19 maintains its own notification procedures as part of an
20 information security policy for the treatment of personal
21 information and is otherwise consistent with the timing
22 requirements of this Act, shall be deemed in compliance with
23 the notification requirements of this Section if the data
24 collector notifies subject persons in accordance with its
25 policies in the event of a breach of the security of the system
26 data or written material.

27 (Source: P.A. 94-36, eff. 1-1-06.)

28 (815 ILCS 530/25 new)

29 Sec. 25. Annual reporting. Any State agency that collects
30 personal data and has had a breach of security of the system
31 data or written material shall submit an annual report to the
32 General Assembly listing the breaches and outlining any
33 corrective measures that have been taken to prevent future
34 breaches of the security of the system data or written
35 material.

1 Section 99. Effective date. This Act takes effect upon
2 becoming law.