

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 5. The Personal Information Protection Act is  
5 amended by changing Sections 5, 10, and 12 and by adding  
6 Section 40 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 "breach"  
16 means unauthorized acquisition of computerized data that  
17 compromises the security, confidentiality, or integrity of  
18 personal information maintained by the data collector. "Breach  
19 of the security of the system data" does not include good faith  
20 acquisition of personal information by an employee or agent of  
21 the data collector for a legitimate purpose of the data  
22 collector, provided that the personal information is not used  
23 for a purpose unrelated to the data collector's business or

1 subject to further unauthorized disclosure.

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

6 (1) Social Security number.

7 (2) Driver's license number or State identification  
8 card number.

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

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

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

17 (815 ILCS 530/10)

18 Sec. 10. Notice of Breach.

19 (a) Any data collector that owns or licenses personal  
20 information concerning an Illinois resident shall notify the  
21 resident at no charge that there has been a breach of the  
22 security of the system data following discovery or notification  
23 of the breach. The disclosure notification shall be made in the  
24 most expedient time possible and without unreasonable delay,  
25 consistent with any measures necessary to determine the scope

1 of the breach and restore the reasonable integrity, security,  
2 and confidentiality of the data system. The disclosure  
3 notification to an Illinois resident shall include, but need  
4 not be limited to, (i) the toll-free numbers and addresses for  
5 consumer reporting agencies, (ii) the toll-free number,  
6 address, and website address for the Federal Trade Commission,  
7 and (iii) a statement that the individual can obtain  
8 information from these sources about fraud alerts and security  
9 freezes. The notification shall not, however, include  
10 information concerning the number of Illinois residents  
11 affected by the breach.

12 (b) Any data collector that maintains or stores, but does  
13 not own or license, computerized data that includes personal  
14 information that the data collector does not own or license  
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. In  
19 addition to providing such notification to the owner or  
20 licensee, the data collector shall cooperate with the owner or  
21 licensee in matters relating to the breach. That cooperation  
22 shall include, but need not be limited to, (i) informing the  
23 owner or licensee of the breach, including giving notice of the  
24 date or approximate date of the breach and the nature of the  
25 breach, and (ii) informing the owner or licensee of any steps  
26 the data collector has taken or plans to take relating to the

1 breach. The data collector's cooperation shall not, however, be  
2 deemed to require either the disclosure of confidential  
3 business information or trade secrets or the notification of an  
4 Illinois resident who may have been affected by the breach.

5 (b-5) The notification to an Illinois resident required by  
6 subsection (a) of this Section may be delayed if an appropriate  
7 law enforcement agency determines that notification will  
8 interfere with a criminal investigation and provides the data  
9 collector with a written request for the delay. However, the  
10 data collector must notify the Illinois resident as soon as  
11 notification will no longer interfere with the investigation.

12 (c) For purposes of this Section, notice to consumers may  
13 be provided by one of the following methods:

14 (1) written notice;

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

20 (3) substitute notice, if the data collector  
21 demonstrates that the cost of providing notice would exceed  
22 \$250,000 or that the affected class of subject persons to  
23 be notified exceeds 500,000, or the data collector does not  
24 have sufficient contact information. Substitute notice  
25 shall consist of all of the following: (i) email notice if  
26 the data collector has an email address for the subject

1 persons; (ii) conspicuous posting of the notice on the data  
2 collector's web site page if the data collector maintains  
3 one; and (iii) notification to major statewide media.

4 (d) Notwithstanding any other subsection in this Section  
5 ~~(e)~~, a data collector that maintains its own notification  
6 procedures as part of an information security policy for the  
7 treatment of personal information and is otherwise consistent  
8 with the timing requirements of this Act, shall be deemed in  
9 compliance with the notification requirements of this Section  
10 if the data collector notifies subject persons in accordance  
11 with its policies in the event of a breach of the security of  
12 the system data.

13 (Source: P.A. 94-36, eff. 1-1-06; 94-947, eff. 6-27-06.)

14 (815 ILCS 530/12)

15 Sec. 12. Notice of breach; State agency.

16 (a) Any State agency that collects personal information  
17 concerning an Illinois resident shall notify the resident at no  
18 charge that there has been a breach of the security of the  
19 system data or written material following discovery or  
20 notification of the breach. The disclosure notification shall  
21 be made in the most expedient time possible and without  
22 unreasonable delay, consistent with any measures necessary to  
23 determine the scope of the breach and restore the reasonable  
24 integrity, security, and confidentiality of the data system.  
25 The disclosure notification to an Illinois resident shall

1 include, but need not be limited to, (i) the toll-free numbers  
2 and addresses for consumer reporting agencies, (ii) the  
3 toll-free number, address, and website address for the Federal  
4 Trade Commission, and (iii) a statement that the individual can  
5 obtain information from these sources about fraud alerts and  
6 security freezes. The notification shall not, however, include  
7 information concerning the number of Illinois residents  
8 affected by the breach.

9 (a-5) The notification to an Illinois resident required by  
10 subsection (a) of this Section may be delayed if an appropriate  
11 law enforcement agency determines that notification will  
12 interfere with a criminal investigation and provides the State  
13 agency with a written request for the delay. However, the State  
14 agency must notify the Illinois resident as soon as  
15 notification will no longer interfere with the investigation.

16 (b) For purposes of this Section, notice to residents may  
17 be provided by one of the following methods:

18 (1) written notice;

19 (2) electronic notice, if the notice provided is  
20 consistent with the provisions regarding electronic  
21 records and signatures for notices legally required to be  
22 in writing as set forth in Section 7001 of Title 15 of the  
23 United States Code; or

24 (3) substitute notice, if the State agency  
25 demonstrates that the cost of providing notice would exceed  
26 \$250,000 or that the affected class of subject persons to

1 be notified exceeds 500,000, or the State agency does not  
2 have sufficient contact information. Substitute notice  
3 shall consist of all of the following: (i) email notice if  
4 the State agency has an email address for the subject  
5 persons; (ii) conspicuous posting of the notice on the  
6 State agency's web site page if the State agency maintains  
7 one; and (iii) notification to major statewide media.

8 (c) Notwithstanding subsection (b), a State agency that  
9 maintains its own notification procedures as part of an  
10 information security policy for the treatment of personal  
11 information and is otherwise consistent with the timing  
12 requirements of this Act shall be deemed in compliance with the  
13 notification requirements of this Section if the State agency  
14 notifies subject persons in accordance with its policies in the  
15 event of a breach of the security of the system data or written  
16 material.

17 (d) If a State agency is required to notify more than 1,000  
18 persons of a breach of security pursuant to this Section, the  
19 State agency shall also notify, without unreasonable delay, all  
20 consumer reporting agencies that compile and maintain files on  
21 consumers on a nationwide basis, as defined by 15 U.S.C.  
22 Section 1681a(p), of the timing, distribution, and content of  
23 the notices. Nothing in this subsection (d) shall be construed  
24 to require the State agency to provide to the consumer  
25 reporting agency the names or other personal identifying  
26 information of breach notice recipients.

1 (Source: P.A. 94-947, eff. 6-27-06.)

2 (815 ILCS 530/40 new)

3 Sec. 40. Disposal of materials containing personal  
4 information; Attorney General.

5 (a) In this Section, "person" means: a natural person; a  
6 corporation, partnership, association, or other legal entity;  
7 a unit of local government or any agency, department, division,  
8 bureau, board, commission, or committee thereof; or the State  
9 of Illinois or any constitutional officer, agency, department,  
10 division, bureau, board, commission, or committee thereof.

11 (b) A person must dispose of the materials containing  
12 personal information in a manner that renders the personal  
13 information unreadable, unusable, and undecipherable. Proper  
14 disposal methods include, but are not limited to, the  
15 following:

16 (1) Paper documents containing personal information  
17 may be either redacted, burned, pulverized, or shredded so  
18 that personal information cannot practicably be read or  
19 reconstructed.

20 (2) Electronic media and other non-paper media  
21 containing personal information may be destroyed or erased  
22 so that personal information cannot practicably be read or  
23 reconstructed.

24 (c) Any person disposing of materials containing personal  
25 information may contract with a third party to dispose of such

1 materials in accordance with this Section. Any third party that  
2 contracts with a person to dispose of materials containing  
3 personal information must implement and monitor compliance  
4 with policies and procedures that prohibit unauthorized access  
5 to or acquisition of or use of personal information during the  
6 collection, transportation, and disposal of materials  
7 containing personal information.

8 (d) Any person, including but not limited to a third party  
9 referenced in subsection (c), who violates this Section is  
10 subject to a civil penalty of not more than \$100 for each  
11 individual with respect to whom personal information is  
12 disposed of in violation of this Section. A civil penalty may  
13 not, however, exceed \$50,000 for each instance of improper  
14 disposal of materials containing personal information. The  
15 Attorney General may impose a civil penalty after notice to the  
16 person accused of violating this Section and an opportunity for  
17 that person to be heard in the matter. The Attorney General may  
18 file a civil action in the circuit court to recover any penalty  
19 imposed under this Section.

20 (e) In addition to the authority to impose a civil penalty  
21 under subsection (d), the Attorney General may bring an action  
22 in the circuit court to remedy a violation of this Section,  
23 seeking any appropriate relief.