



Rep. Daniel J. Burke

**Filed: 3/8/2011**

09700HB3025ham001

LRB097 06857 AEK 51982 a

1 AMENDMENT TO HOUSE BILL 3025

2 AMENDMENT NO. \_\_\_\_\_. Amend House Bill 3025 by replacing  
3 everything after the enacting clause with the following:

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 or use of computerized data that

1 compromises the security, confidentiality, or integrity of  
2 personal information maintained by the data collector. "Breach  
3 of the security of the system data" does not include good faith  
4 acquisition of personal information by an employee or agent of  
5 the data collector for a legitimate purpose of the data  
6 collector, provided that the personal information is not used  
7 for a purpose unrelated to the data collector's business or  
8 subject to further unauthorized disclosure.

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

13 (1) Social Security number.

14 (2) Driver's license number or State identification  
15 card number.

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

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

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

24 (815 ILCS 530/10)

25 Sec. 10. Notice of Breach.

1 (a) Any data collector that owns or licenses personal  
2 information concerning an Illinois resident shall notify the  
3 resident at no charge that there has been a breach of the  
4 security of the system data following discovery or notification  
5 of the breach. The disclosure notification shall be made in the  
6 most expedient time possible and without unreasonable delay,  
7 consistent with any measures necessary to determine the scope  
8 of the breach and restore the reasonable integrity, security,  
9 and confidentiality of the data system. The disclosure  
10 notification to an Illinois resident shall include, but need  
11 not be limited to, information concerning (i) how the resident  
12 may request a security freeze pursuant to Section 2MM of the  
13 Consumer Fraud and Deceptive Business Practices Act and the  
14 necessary information that must be provided when requesting the  
15 security freeze, and (ii) any fees that must be paid to a  
16 consumer reporting agency in connection with a request for a  
17 security freeze. The notification shall not, however, include  
18 information concerning the number of Illinois residents  
19 affected by the breach.

20 In addition, a data collector that owns or licenses such  
21 personal information shall notify the Attorney General of the  
22 breach. The notification to the Attorney General shall include,  
23 but need not be limited to, information concerning (i) the  
24 nature of the breach, (ii) the number of Illinois residents  
25 affected by the breach at the time of notification, and (iii)  
26 any steps the data collector has taken or plans to take

1 relating to the breach.

2 (b) Any data collector that maintains or stores, but does  
3 not own or license, computerized data that includes personal  
4 information that the data collector does not own or license  
5 shall notify the owner or licensee of the information of any  
6 breach of the security of the data immediately following  
7 discovery, if the personal information was, or is reasonably  
8 believed to have been, acquired by an unauthorized person. In  
9 addition to providing such notification to the owner or  
10 licensee, the data collector shall cooperate with the owner or  
11 licensee in matters relating to the breach. That cooperation  
12 shall include, but need not be limited to, (i) informing the  
13 owner or licensee of the breach, including giving notice of the  
14 date or approximate date of the breach and the nature of the  
15 breach, and (ii) informing the owner or licensee of any steps  
16 the data collector has taken or plans to take relating to the  
17 breach. The data collector's cooperation shall not, however, be  
18 deemed to require either the disclosure of confidential  
19 business information or trade secrets or the notification of an  
20 Illinois resident who may have been affected by the breach.

21 (b-5) The notification to an Illinois resident required by  
22 subsection (a) of this Section may be delayed if an appropriate  
23 law enforcement agency determines that notification will  
24 interfere with a criminal investigation and provides the data  
25 collector with a written request for the delay. However, the  
26 data collector must notify the Illinois resident as soon as

1 notification will no longer interfere with the investigation.

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

4 (1) written notice;

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

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

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

1 policies in the event of a breach of the security of the system  
2 data.

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

4 (815 ILCS 530/12)

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

6 (a) Any State agency that collects personal information  
7 concerning an Illinois resident shall notify the resident at no  
8 charge that there has been a breach of the security of the  
9 system data or written material following discovery or  
10 notification of the breach. The disclosure notification shall  
11 be made in the most expedient time possible and without  
12 unreasonable delay, consistent with any measures necessary to  
13 determine the scope of the breach and restore the reasonable  
14 integrity, security, and confidentiality of the data system.  
15 The disclosure notification to an Illinois resident shall  
16 include, but need not be limited to, information concerning (i)  
17 how the resident may request a security freeze pursuant to  
18 Section 2MM of the Consumer Fraud and Deceptive Business  
19 Practices Act and the necessary information that must be  
20 provided when requesting the security freeze, and (ii) any fees  
21 that must be paid to a consumer reporting agency in connection  
22 with a request for a security freeze. The notification to an  
23 Illinois resident shall not, however, include information  
24 concerning the number of Illinois residents affected by the  
25 breach.

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

3 (1) written notice;

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

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

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

1 material.

2 (d) If a State agency is required to notify more than 1,000  
3 persons of a breach of security pursuant to this Section, the  
4 State agency shall also notify, without unreasonable delay, all  
5 consumer reporting agencies that compile and maintain files on  
6 consumers on a nationwide basis, as defined by 15 U.S.C.  
7 Section 1681a(p), of the timing, distribution, and content of  
8 the notices. Nothing in this subsection (d) shall be construed  
9 to require the State agency to provide to the consumer  
10 reporting agency the names or other personal identifying  
11 information of breach notice recipients.

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

13 (815 ILCS 530/40 new)

14 Sec. 40. Disposal of materials containing personal  
15 information; Attorney General.

16 (a) In this Section, "person" means: a natural person; a  
17 corporation, partnership, association, or other legal entity;  
18 a unit of local government or any agency, department, division,  
19 bureau, board, commission, or committee thereof; or the State  
20 of Illinois or any constitutional officer, agency, department,  
21 division, bureau, board, commission, or committee thereof.

22 (b) When disposing of materials containing personal  
23 information, a person must meet the following minimum standards  
24 for proper disposal of such materials:

25 (1) Paper documents containing personal information

1       must be either redacted, burned, pulverized, or shredded so  
2       that personal information cannot practicably be read or  
3       reconstructed.

4       (2) Electronic media and other non-paper media  
5       containing personal information must be destroyed or  
6       erased so that personal information cannot practicably be  
7       read or reconstructed.

8       (c) Any person disposing of materials containing personal  
9       information may contract with a third party to dispose of such  
10       materials in accordance with this Section. Any third party that  
11       contracts with a person to dispose of materials containing  
12       personal information must implement and monitor compliance  
13       with policies and procedures that prohibit unauthorized access  
14       to or acquisition of or use of personal information during the  
15       collection, transportation, and disposal of materials  
16       containing personal information.

17       (d) Any person who violates this Section is subject to a  
18       civil penalty of not more than \$100 for each individual with  
19       respect to whom personal information is disposed of in  
20       violation of this Section. A civil penalty may not, however,  
21       exceed \$50,000 for each instance of improper disposal of  
22       materials containing personal information. The Attorney  
23       General may impose a civil penalty after notice to the person  
24       accused of violating this Section and an opportunity for that  
25       person to be heard in the matter. The Attorney General may file  
26       a civil action in the circuit court to recover any penalty

1 imposed under this Section.

2 (e) In addition to the authority to impose a civil penalty  
3 under subsection (d), the Attorney General may bring an action  
4 in the circuit court to remedy a violation of this Section,  
5 seeking any appropriate relief."