



99TH GENERAL ASSEMBLY

State of Illinois

2015 and 2016

HB3652

by Rep. Carol Ammons

SYNOPSIS AS INTRODUCED:

815 ILCS 530/5
815 ILCS 530/10
815 ILCS 530/12
815 ILCS 530/40
815 ILCS 530/50 new

Amends the Personal Information Protection Act. Expands the scope of the Act to cover private contact information (home address, home or personal phone number, personal e-mail address). Limits the transfer of private contact information.

LRB099 09353 JLS 29558 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 5. The Personal Information Protection Act is
5 amended by changing Section 5, 10, 12, and 40 and adding
6 Section 50 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 or private contact
15 information.

16 "Breach of the security of the system data" or "breach"
17 means ~~unauthorized~~ acquisition, unauthorized by an individual,
18 of computerized data that compromises the security,
19 confidentiality, or integrity of the individual's personal
20 information or private contact information maintained by the
21 data collector. "Breach of the security of the system data"
22 does not include good faith acquisition of personal information
23 or private contact information by an employee or agent of the

1 data collector for a legitimate purpose of the data collector,
2 provided that the personal information or private contact
3 information is not used for a purpose unrelated to the data
4 collector's business or subject to further unauthorized
5 disclosure.

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

10 (1) Social Security number.

11 (2) Driver's license number or State identification
12 card number.

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

17 (4) Personal financial information.

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

21 "Private contact information" means an individual's home
22 or personal telephone number, home address, or personal e-mail
23 address.

24 (Source: P.A. 97-483, eff. 1-1-12.)

25 (815 ILCS 530/10)

1 Sec. 10. Notice of Breach.

2 (a) Any data collector that owns or licenses personal
3 information or private contact information concerning an
4 Illinois resident shall notify the resident at no charge that
5 there has been a breach of the security of the system data
6 following discovery or notification of the breach. The
7 disclosure notification shall be made in the most expedient
8 time possible and without unreasonable delay, consistent with
9 any measures necessary to determine the scope of the breach and
10 restore the reasonable integrity, security, and
11 confidentiality of the data system. The disclosure
12 notification to an Illinois resident shall include, but need
13 not be limited to, (i) the toll-free numbers and addresses for
14 consumer reporting agencies, (ii) the toll-free number,
15 address, and website address for the Federal Trade Commission,
16 and (iii) a statement that the individual can obtain
17 information from these sources about fraud alerts and security
18 freezes. The notification shall not, however, include
19 information concerning the number of Illinois residents
20 affected by the breach.

21 (b) Any data collector that maintains or stores, but does
22 not own or license, computerized data that includes personal
23 information or private contact information that the data
24 collector does not own or license shall notify the owner or
25 licensee of the information of any breach of the security of
26 the data immediately following discovery, if the personal

1 information or private contact information was, or is
2 reasonably believed to have been, acquired by an unauthorized
3 person. In addition to providing such notification to the owner
4 or licensee, the data collector shall cooperate with the owner
5 or licensee in matters relating to the breach. That cooperation
6 shall include, but need not be limited to, (i) informing the
7 owner or licensee of the breach, including giving notice of the
8 date or approximate date of the breach and the nature of the
9 breach, and (ii) informing the owner or licensee of any steps
10 the data collector has taken or plans to take relating to the
11 breach. The data collector's cooperation shall not, however, be
12 deemed to require either the disclosure of confidential
13 business information or trade secrets or the notification of an
14 Illinois resident who may have been affected by the breach.

15 (b-5) The notification to an Illinois resident required by
16 subsection (a) of this Section may be delayed if an appropriate
17 law enforcement agency determines that notification will
18 interfere with a criminal investigation and provides the data
19 collector with a written request for the delay. However, the
20 data collector must notify the Illinois resident as soon as
21 notification will no longer interfere with the investigation.

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

24 (1) written notice;

25 (2) electronic notice, if the notice provided is
26 consistent with the provisions regarding electronic

1 records and signatures for notices legally required to be
2 in writing as set forth in Section 7001 of Title 15 of the
3 United States Code; or

4 (3) substitute notice, if the data collector
5 demonstrates that the cost of providing notice would exceed
6 \$250,000 or that the affected class of subject persons to
7 be notified exceeds 500,000, or the data collector does not
8 have sufficient contact information. Substitute notice
9 shall consist of all of the following: (i) email notice if
10 the data collector has an email address for the subject
11 persons; (ii) conspicuous posting of the notice on the data
12 collector's web site page if the data collector maintains
13 one; and (iii) notification to major statewide media.

14 (d) Notwithstanding any other subsection in this Section, a
15 data collector that maintains its own notification procedures
16 as part of an information security policy for the treatment of
17 personal information or private contact information and is
18 otherwise consistent with the timing requirements of this Act,
19 shall be deemed in compliance with the notification
20 requirements of this Section if the data collector notifies
21 subject persons in accordance with its policies in the event of
22 a breach of the security of the system data.

23 (Source: P.A. 97-483, eff. 1-1-12.)

24 (815 ILCS 530/12)

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

1 (a) Any State agency that collects personal information or
2 private contact information concerning an Illinois resident
3 shall notify the resident at no charge that there has been a
4 breach of the security of the system data or written material
5 following discovery or notification of the breach. The
6 disclosure notification shall be made in the most expedient
7 time possible and without unreasonable delay, consistent with
8 any measures necessary to determine the scope of the breach and
9 restore the reasonable integrity, security, and
10 confidentiality of the data system. The disclosure
11 notification to an Illinois resident shall include, but need
12 not be limited to, (i) the toll-free numbers and addresses for
13 consumer reporting agencies, (ii) the toll-free number,
14 address, and website address for the Federal Trade Commission,
15 and (iii) a statement that the individual can obtain
16 information from these sources about fraud alerts and security
17 freezes. The notification shall not, however, include
18 information concerning the number of Illinois residents
19 affected by the breach.

20 (a-5) The notification to an Illinois resident required by
21 subsection (a) of this Section may be delayed if an appropriate
22 law enforcement agency determines that notification will
23 interfere with a criminal investigation and provides the State
24 agency with a written request for the delay. However, the State
25 agency must notify the Illinois resident as soon as
26 notification will no longer interfere with the investigation.

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 or private contact information and is otherwise
23 consistent with the timing requirements of this Act shall be
24 deemed in compliance with the notification requirements of this
25 Section if the State agency notifies subject persons in
26 accordance with its policies in the event of a breach of the

1 security of the system data or written 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. 97-483, eff. 1-1-12.)

13 (815 ILCS 530/40)

14 Sec. 40. Disposal of materials containing personal
15 information or private contact 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) A person must dispose of the materials containing
23 personal information or private contact information in a manner
24 that renders the personal information or private contact
25 information unreadable, unusable, and undecipherable. Proper

1 disposal methods include, but are not limited to, the
2 following:

3 (1) Paper documents containing personal information or
4 private contact information may be either redacted,
5 burned, pulverized, or shredded so that personal
6 information or private contact information cannot
7 practicably be read or reconstructed.

8 (2) Electronic media and other non-paper media
9 containing personal information or private contact
10 information may be destroyed or erased so that personal
11 information or private contact information cannot
12 practicably be read or reconstructed.

13 (c) Any person disposing of materials containing personal
14 information or private contact information may contract with a
15 third party to dispose of such materials in accordance with
16 this Section. Any third party that contracts with a person to
17 dispose of materials containing personal information or
18 private contact information must implement and monitor
19 compliance with policies and procedures that prohibit
20 unauthorized access to or acquisition of or use of personal
21 information or private contact information during the
22 collection, transportation, and disposal of materials
23 containing personal information or private contact
24 information.

25 (d) Any person, including but not limited to a third party
26 referenced in subsection (c), who violates this Section is

1 subject to a civil penalty of not more than \$100 for each
2 individual with respect to whom personal information or private
3 contact information is disposed of in violation of this
4 Section. A civil penalty may not, however, exceed \$50,000 for
5 each instance of improper disposal of materials containing
6 personal information or private contact information. The
7 Attorney General may impose a civil penalty after notice to the
8 person accused of violating this Section and an opportunity for
9 that person to be heard in the matter. The Attorney General may
10 file a civil action in the circuit court to recover any penalty
11 imposed under this Section.

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

16 (f) A financial institution under 15 U.S.C. 6801 et seq.
17 or any person subject to 15 U.S.C. 1681w is exempt from this
18 Section.

19 (g) Nothing in this Act prohibits a person from retaining
20 private contact information possessed by the person and used
21 for a legitimate business purpose of the person's business. A
22 legitimate business purpose includes, but is not limited to,
23 storing billing information, storing shipping information,
24 advertising by the person, marketing by the person, or any
25 other use related to the person's business.
26

1 (Source: P.A. 97-483, eff. 1-1-12.)

2 (815 ILCS 530/50 new)

3 Sec. 50. Prohibitions on the transfer of private contact
4 information. A person or data collector shall not sell private
5 contact information. A person or data collector may transfer or
6 share private contact information only to the extent the
7 transfer or sharing of private contact information is necessary
8 for a legitimate purpose of the data collector or person and
9 provided that the private contact information is not used for a
10 purpose unrelated to the person or data collector's business or
11 subject to further unauthorized disclosure.