
THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 1458 Session of
2009

INTRODUCED BY PAYTON, BELFANTI, BOBACK, BRENNAN, CASORIO,
D. COSTA, CREIGHTON, DONATUCCI, FABRIZIO, FLECK, FREEMAN,
GEIST, GEORGE, GOODMAN, HARHAI, HENNESSEY, HORNAMAN, JOSEPHS,
KORTZ, KULA, MCGEEHAN, MCILVAINE SMITH, MELIO, MILLARD,
MILNE, MUNDY, MURT, M. O'BRIEN, PALLONE, PYLE, SAYLOR,
SIPTROTH, K. SMITH, SWANGER, VULAKOVICH, J. TAYLOR, WATSON,
WHITE AND YOUNGBLOOD, MAY 7, 2009

REFERRED TO COMMITTEE ON CONSUMER AFFAIRS, MAY 7, 2009

AN ACT

1 Regulating the use of credit reports, business records, Social
2 Security numbers and other personal information.

3 TABLE OF CONTENTS

4 Chapter 1. Preliminary Provisions

5 Section 101. Short title.

6 Section 102. Definitions.

7 Chapter 3. Procedures

8 Section 301. Business records.

9 Section 302. Distribution of information.

10 Section 303. Dispute procedure.

11 Chapter 5. Confidentiality of Social Security Numbers

12 Section 501. Prohibitions.

13 Section 502. Limitations of use of Social Security numbers by
14 governmental entities.

15 Chapter 11. Miscellaneous Provisions

1 Section 1101. Damages.
2 Section 1102. Violations.
3 Section 1103. Effective date.

4 The General Assembly of the Commonwealth of Pennsylvania
5 hereby enacts as follows:

6 CHAPTER 1

7 PRELIMINARY PROVISIONS

8 Section 101. Short title.

9 This act shall be known and may be cited as the Personal
10 Information Protection Act.

11 Section 102. Definitions.

12 The following words and phrases when used in this act shall
13 have the meanings given to them in this section unless the
14 context clearly indicates otherwise:

15 "Consumer." A natural person who resides in this
16 Commonwealth.

17 "Credit report." Any written, oral or other communication of
18 any credit information by a credit reporting agency, as defined
19 in the Fair Credit Reporting Act (Public Law 91-508, 15 U.S.C. §
20 1681 et seq.), which operates or maintains a database of
21 consumer credit information bearing on a consumer's
22 creditworthiness, credit standing or credit capacity.

23 "Credit reporting agency." Any person who, for monetary
24 fees, dues or on a cooperative nonprofit basis, regularly
25 engages in whole or in part in the practice of assembling or
26 evaluating consumer credit information or other information on
27 consumers for the purpose of furnishing consumer reports to
28 third parties and who uses any means or facility of interstate
29 commerce for the purpose of preparing or furnishing consumer
30 reports. The term does not include:

1 (1) A check acceptance service which provides check
2 approval and guarantees services to merchants.

3 (2) Any governmental agency whose records are maintained
4 primarily for traffic safety, law enforcement or licensing
5 purposes.

6 CHAPTER 3

7 PROCEDURES

8 Section 301. Business records.

9 (a) General rule.--A business or public entity shall destroy
10 or arrange for the destruction of a customer's records within
11 its custody or control which contain personal information, which
12 is no longer to be retained by the business or public entity, by
13 shredding, erasing or otherwise modifying the personal
14 information in those records to make it unreadable,
15 undecipherable or nonreconstructible through generally available
16 means.

17 (b) Disclosure of security breach.--A business that conducts
18 business in this Commonwealth or any public entity that compiles
19 or maintains computerized records that include personal
20 information shall disclose any breach of security of those
21 computerized records following discovery or notification of the
22 breach to any customer who is a resident of this Commonwealth
23 whose personal information was, or is reasonably believed to
24 have been, accessed by an unauthorized person. The disclosure
25 shall be made in the most expedient time possible and without
26 unreasonable delay, consistent with the legitimate needs of law
27 enforcement and measures necessary to determine the scope of the
28 breach and restore the reasonable integrity of the data system.
29 Disclosure shall not be required if the business or public
30 entity establishes that misuse of the information is not

1 reasonably possible. Any determination shall be documented in
2 writing and retained for five years. A business or public entity
3 that compiles or maintains computerized records that include
4 personal information on behalf of another business or public
5 entity shall notify that business or public entity, which shall
6 notify its Commonwealth customers of any breach of security of
7 the computerized records immediately following discovery if the
8 personal information was or is reasonably believed to have been
9 accessed by an unauthorized person.

10 (c) Attorney General.--A business or public entity required
11 under this section to disclose a breach of security of a
12 customer's personal information shall, in advance of the
13 disclosure to the customer, report the breach of security and
14 any information pertaining to the breach to the Office of
15 Attorney General for investigation or handling, which may
16 include dissemination or referral to other appropriate law
17 enforcement entities. The notification shall be delayed if a law
18 enforcement agency determines that the notification will impede
19 a criminal or civil investigation and that agency has made a
20 request that the notification be delayed. The notification shall
21 be made after the law enforcement agency determines that its
22 disclosure will not compromise the investigation and notifies
23 that business or public entity.

24 (d) Notice.--For purposes of this section, notice may be
25 provided by one of the following methods:

26 (1) Written notice.

27 (2) Electronic notice, if the notice provided is
28 consistent with the provisions regarding electronic records
29 and signatures set forth in the Electronic Signatures in
30 Global and National Commerce Act (Public Law 106-229, 15

1 U.S.C. § 7001 et seq.).

2 (3) Substitute notice, if the business or public entity
3 demonstrates that the cost of providing notice would exceed
4 \$250,000, that the affected class of subject persons to be
5 notified exceeds 500,000 or that the business or public
6 entity does not have sufficient contact information.

7 Substitute notice shall consist of all of the following:

8 (i) E-mail notice when the business or public entity
9 has an e-mail address.

10 (ii) Conspicuous posting of the notice on the
11 Internet website of the business or public entity if the
12 business or public entity maintains one.

13 (iii) Notification to major Statewide media.

14 (e) Exception.--Notwithstanding subsection (d), a business
15 or public entity that maintains its own notification procedures
16 as part of an information security policy for the treatment of
17 personal information and is otherwise consistent with the
18 requirements of this section shall be deemed to be in compliance
19 with the notification requirements of this section if the
20 business or public entity notifies subject customers in
21 accordance with its policies in the event of a breach of
22 security of the system.

23 (f) Additional notification.--In addition to any other
24 disclosure or notification required under this section, in the
25 event that a business or public entity discovers circumstances
26 requiring notification pursuant to this section of more than
27 1,000 persons at one time, the business or public entity shall
28 also notify, without unreasonable delay, all consumer reporting
29 agencies that compile or maintain files on consumers on a
30 nationwide basis, as defined by section 603(p) of the Fair

1 Credit Reporting Act (Public Law 91-508, 15 U.S.C. § 1681a(p)),
2 of the timing, distribution and content of the notices.
3 Section 302. Distribution of information.

4 A credit reporting agency shall create reasonable procedures
5 to prevent a consumer credit report or information from a
6 consumer's file from being provided to any third party for
7 marketing purposes or for any offer of credit not requested by
8 the consumer. This section does not apply to the use of
9 information by a credit grantor for purposes related to an
10 existing credit relationship.

11 Section 303. Dispute procedure.

12 If the completeness or accuracy of information contained in a
13 consumer's file is disputed by the consumer and the consumer
14 notifies the consumer reporting agency of the dispute, the
15 agency shall reinvestigate the disputed information free of
16 charge and record the current status of the disputed information
17 no later than the 30th business day after the date on which the
18 agency receives the notice. The consumer reporting agency shall
19 provide the consumer with the option of notifying the agency of
20 a dispute concerning the consumer's file by speaking directly to
21 a representative of the agency. No disputed debt shall be
22 included in a credit report without first obtaining a written
23 record indicating that judgment has been entered in favor of a
24 debt collector.

25 CHAPTER 5

26 CONFIDENTIALITY OF SOCIAL SECURITY NUMBERS

27 Section 501. Prohibitions.

28 (a) General rule.--A person or entity, not including a State
29 or local agency, shall not do any of the following:

30 (1) Publicly post or publicly display in any manner an

1 individual's Social Security number.

2 (2) Print an individual's Social Security number on any
3 card required for the individual to access products or
4 services provided by the person or entity.

5 (3) Require an individual to transmit the individual's
6 Social Security number over the Internet website unless the
7 connection is secure or the Social Security number is
8 encrypted.

9 (4) Require an individual to use the individual's Social
10 Security number to access an Internet website unless a
11 password or unique personal identification number or other
12 authentication device is also required to access the Internet
13 website.

14 (5) (i) Print an individual's Social Security number on
15 any materials that are mailed to the individual unless
16 Federal or State law requires the Social Security number
17 to be on the document to be mailed.

18 (ii) Notwithstanding subparagraph (i), applications
19 and forms sent by mail may include Social Security
20 numbers.

21 (b) Applicability.--Except as provided in subsection (c),
22 subsection (a) applies to the use of Social Security numbers on
23 or after January 1, 2010.

24 (c) Use prior to effective date.--Except as provided in
25 subsection (e), a person or entity, not including a State or
26 local entity that has used prior to January 1, 2010, an
27 individual's Social Security number in a manner inconsistent
28 with subsection (a), may continue using that individual's Social
29 Security number in that manner on or after January 1, 2010, if
30 all of the following conditions are met:

1 (1) The use of the Social Security number is continuous.
2 If the use is discontinued for any reason, subsection (a)
3 shall apply.

4 (2) The individual is provided an annual disclosure,
5 commencing in the year 2010, informing the individual that
6 the individual has the right to discontinue use of the
7 individual's Social Security number in a manner prohibited by
8 subsection (a).

9 (3) If a written request by an individual to discontinue
10 the use of the individual's Social Security number in a
11 manner prohibited by subsection (a) is received, the person
12 or entity shall implement the request within 30 days of the
13 receipt of the request. The person or entity may not impose a
14 fee or charge for implementing the request.

15 (4) The person or entity, not including a State or local
16 agency, does not deny services to the individual because the
17 individual makes a written request pursuant to this
18 subsection.

19 (d) Construction.--This section shall not be construed to
20 prohibit the collection, use or release of a Social Security
21 number as required by Federal or State law or the use of a
22 Social Security number for internal verification or
23 administrative purposes by a person or entity.

24 (e) Exceptions.--In the case of a health care service plan,
25 a provider of health care, an insurer or pharmacy benefits
26 manager or an agent of any of these, this section shall become
27 operative as follows:

28 (1) On or before July 1, 2010, a health care service
29 plan, a provider of health care, an insurer or pharmacy
30 benefits manager or an agent of any of these shall comply

1 with subsection (a) (1), (3), (4) and (5) as these
2 requirements pertain to existing individual policyholders.

3 (2) On or before July 1, 2010, a health care service
4 plan, a provider of health care, an insurer or pharmacy
5 benefits manager or an agent of any of these shall comply
6 with subsection (a) as these requirements pertain to new
7 individual policyholders and new employer groups for policies
8 issued on or after July 1, 2010.

9 (f) Cooperation.--A health care service plan, a provider of
10 health care, an insurer or pharmacy benefits manager or an agent
11 of any of these entities shall make reasonable efforts to
12 cooperate, through systems testing and other means, to ensure
13 the requirements of this chapter are implemented on or before
14 the dates specified in this chapter.

15 Section 502. Limitations of use of Social Security numbers by
16 governmental entities.

17 Prior to posting or requiring the posting of a document in a
18 place of general public circulation, an agency, board,
19 department, commission, committee, branch, instrumentality or
20 authority of the Commonwealth or an agency, board, committee,
21 department, branch, instrumentality, commission or authority of
22 any political subdivision of the Commonwealth shall take all
23 reasonable steps to redact any Social Security numbers from the
24 documents.

25 CHAPTER 11

26 MISCELLANEOUS PROVISIONS

27 Section 1101. Damages.

28 Any consumer damaged by an intentional, reckless or negligent
29 violation of this act may bring an action for and shall be
30 entitled to recovery of actual damages, plus reasonable attorney

1 fees, court costs and other reasonable costs of prosecution of
2 the suit.

3 Section 1102. Violations.

4 (a) Concealment.--A person having knowledge of a security
5 breach requiring notice to individuals under this act who
6 intentionally and willfully conceals the fact of or information
7 related to the security breach commits a felony of the first
8 degree.

9 (b) Unlawful use of identifying information.--During and in
10 relation to any felony violation, a person who knowingly
11 obtains, accesses or transmits, without lawful authority, a
12 means of identification of another person may, in addition to
13 the punishment provided for the felony, be sentenced to serve up
14 to two additional years of imprisonment.

15 Section 1103. Effective date.

16 This act shall take effect in 60 days.