AN ACT

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

TABLE OF CONTENTS

Chapter 1. Preliminary Provisions

Section 101. Short title.

Section 102. Definitions.

Chapter 3. Procedures

Section 301. Business records.

Section 302. Distribution of information.

Section 303. Dispute procedure.

Chapter 5. Confidentiality of Social Security Numbers

Section 501. Prohibitions.

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

CHAPTER 1

PRELIMINARY PROVISIONS

Section 101. Short title.

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

Section 102. Definitions.

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

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

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

"Credit reporting agency." Any person who, for monetary fees, dues or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties and who uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. The term does not include:
A check acceptance service which provides check
approval and guarantees services to merchants.

Any governmental agency whose records are maintained
primarily for traffic safety, law enforcement or licensing
purposes.

CHAPTER 3

PROCEDURES

Section 301. Business records.

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

(b) Disclosure of security breach.--A business that conducts
business in this Commonwealth or any public entity that compiles
or maintains computerized records that include personal
information shall disclose any breach of security of those
computerized records following discovery or notification of the
breach to any customer who is a resident of this Commonwealth
whose personal information was, or is reasonably believed to
have been, accessed by an unauthorized person. The disclosure
shall be made in the most expedient time possible and without
unreasonable delay, consistent with the legitimate needs of law
enforcement and measures necessary to determine the scope of the
breach and restore the reasonable integrity of the data system.
Disclosure shall not be required if the business or public
entity establishes that misuse of the information is not
reasonably possible. Any determination shall be documented in writing and retained for five years. A business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, which shall notify its Commonwealth customers of any breach of security of the computerized records immediately following discovery if the personal information was or is reasonably believed to have been accessed by an unauthorized person.

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

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

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in the Electronic Signatures in Global and National Commerce Act (Public Law 106-229, 15
U.S.C. § 7001 et seq.).

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

Substitute notice shall consist of all of the following:

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

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

(iii) Notification to major Statewide media.

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

(f) Additional notification.--In addition to any other disclosure or notification required under this section, in the event that a business or public entity discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the business or public entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis, as defined by section 603(p) of the Fair Credit Reporting Act.
Credit Reporting Act (Public Law 91-508, 15 U.S.C. § 1681a(p)),
of the timing, distribution and content of the notices.

Section 302. Distribution of information.

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

Section 303. Dispute procedure.

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

CHAPTER 5

CONFIDENTIALITY OF SOCIAL SECURITY NUMBERS

Section 501. Prohibitions.

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

(1) Publicly post or publicly display in any manner an
individual's Social Security number.

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

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

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

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

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

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

(c) Use prior to effective date.--Except as provided in subsection (e), a person or entity, not including a State or local entity that has used prior to January 1, 2010, an individual's Social Security number in a manner inconsistent with subsection (a), may continue using that individual's Social Security number in that manner on or after January 1, 2010, if all of the following conditions are met:
(1) The use of the Social Security number is continuous. If the use is discontinued for any reason, subsection (a) shall apply.

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

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

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

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

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

(1) On or before July 1, 2010, a health care service plan, a provider of health care, an insurer or pharmacy benefits manager or an agent of any of these shall comply
with subsection (a)(1), (3), (4) and (5) as these requirements pertain to existing individual policyholders.

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

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

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

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

CHAPTER 11
MISCELLANEOUS PROVISIONS

Section 1101. Damages.

Any consumer damaged by an intentional, reckless or negligent violation of this act may bring an action for and shall be entitled to recovery of actual damages, plus reasonable attorney
fees, court costs and other reasonable costs of prosecution of
the suit.

Section 1102. Violations.

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

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

Section 1103. Effective date.

This act shall take effect in 60 days.