PRINTER'S NO. 2925

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 2006 Session of 2005

INTRODUCED BY PRESTON, FLICK, THOMAS, BAKER, BELFANTI, BOYD, CALTAGIRONE, CLYMER, GERGELY, GRUCELA, HARHAI, HERMAN, JAMES, JOSEPHS, MARKOSEK, McCALL, MUNDY, O'NEILL, PALLONE, PETRARCA, PETRONE, READSHAW, REICHLEY, RUBLEY, SAINATO, SANTONI, SIPTROTH, SHAPIRO, SOLOBAY, SURRA, TANGRETTI, E. Z. TAYLOR, TIGUE, WALKO AND WOJNAROSKI, OCTOBER 25, 2005

REFERRED TO COMMITTEE ON CONSUMER AFFAIRS, OCTOBER 25, 2005

AN ACT

Providing for breach of security of identifying information and for penalties.

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

Section 1. Short title.

This act shall be known and may be cited as the Breach of Personal Information Data Notification Act.

Section 2. 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:

"Breach of the security of a system." The unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal

information regarding multiple individuals and that causes or the individual or entity reasonably believes has caused or will cause identity theft or other fraud to any resident of this Commonwealth. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system if the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

"Encrypted." Transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key or securing the information by another method that renders the data elements unreadable or unusable.

"Entity." The term includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies or instrumentalities or any other legal entity, whether for profit or not for profit.

"Financial institution." The term as defined in section 509(3) of the Gramm-Leach-Bliley Act (Public Law 106-102, 15 U.S.C. § 6809(3)).

"Individual." A natural person.

"Notice." All of the following methods of notification:

(1) Notification to major Statewide media.

(2) One of the following methods of notification:

(i) Written notice.

(ii) Electronic notice, if the notice provided is consistent with the provisions regarding electronic

records and signatures set forth in section 701 of the Electronic Signatures in Global and National Commerce Act (Public Law 106-229, 15 U.S.C. § 7001).

(iii) (A) Substitute notice, if the entity demonstrates one of the following:

(I) The cost of providing notice would exceed $50,000.

(II) The affected class of subject persons to be notified exceeds $100,000.

(III) The entity does not have sufficient contact information.

(B) Substitute notice shall consist of all of the following:

(I) E-mail notice when the entity has an e-mail address for the subject persons.

(II) Conspicuous posting of the notice on the entity's Internet website, if the entity maintains one.

"Personal information."

(1) The first name or first initial and last name linked to any one or more of the following data elements that relate to a resident of this Commonwealth, when the data elements are neither encrypted or redacted:

(i) Social Security number.

(ii) Driver's license number or State identification card number issued in lieu of a driver's license.

(iii) Financial account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a resident's financial accounts.

(2) The term does not include information that is lawfully obtained from publicly available information or from Federal, State or local government records lawfully made available to the general public.

"Redact." Alteration or truncation of data so that no more than the last four digits of a Social Security number, driver's license number, State identification card number or account number is accessible as part of the personal information.

Section 3. Disclosure of breach of security of computerized personal information by an individual or entity.

(a) General rule.--An individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes or the individual or entity reasonably believes has caused or will cause identity theft or other fraud to any resident of this Commonwealth. Except as provided in subsection (d) or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the disclosure shall be made without unreasonable delay.

(b) Encrypted information.--An individual or entity must disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that the breach has caused or will cause identity theft or other

fraud to any resident of this Commonwealth.

(c) Notification.--An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery.

(d) Delay in notification.--Notice required by this section may be delayed if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or jeopardize homeland or national security. Notice required by this section must be made without unreasonable delay after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security.

Section 4. Procedures deemed in compliance with security breach requirements.

(a) Information privacy or security policy.--An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of this act shall be deemed to be in compliance with the notification requirements of this act if it notifies residents of this Commonwealth in accordance with its procedures in the event of a breach of security of the system.

(b) Compliance with Federal requirements.--

(1) A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice shall be

deemed to be in compliance with this act.

(2) An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures or guidelines established by the entity's primary or functional Federal regulator shall be deemed to be in compliance with this act.

Section 5. Preemption.

This act deals with subject matter that is of Statewide concern and it is the intent of the General Assembly that this act shall supersede and preempt all rules, regulations, codes, statutes or ordinances of all cities, counties, municipalities and other local agencies within this Commonwealth regarding the matters expressly set forth in this act.

Section 6. Violations.

(a) Unfair or deceptive act or practice.--A violation of this act shall be deemed to be an unfair or deceptive act or practice in violation of the act of December 17, 1968 (P.L.1224, No.387), known as the Unfair Trade Practices and Consumer Protection Law. Except as provided in subsection (b), the Office of Attorney General shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this act.

(b) Certain violations.--The primary governmental regulating agency of a State-chartered or State-licensed financial institution shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation by a State-chartered or State-licensed financial institution of this act.

(c) Additional penalties.--In addition to any penalties provided for by the Unfair Trade Practices and Consumer

Protection Law, the Office of Attorney General or a primary governmental regulating agency may bring a civil action to obtain one of the following:

(1) Actual damages for a violation of this act.

(2) A civil penalty not to exceed $150,000 per breach of a security system or a series of breaches of a security system that are similar in nature and discovered in a single investigation.

Section 7. Applicability.

This act shall apply to the discovery or notification of a breach of the security of the system that occurs on or after the effective date of this act.

Section 20. Effective date.

This act shall take effect in 120 days.