PRIOR PRINTER'S NOS. 1086, 1621 PRINTER'S NO. 2381

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 997 Session of 2025

INTRODUCED BY SOLOMON, HILL-EVANS, CERRATO, HOWARD, FREEMAN, KAZEEM, GIRAL, GUENST, MERSKI, CEPEDA-FREYTIZ, PIELLI, SANCHEZ, D. WILLIAMS, CIRESI, STEELE, SHUSTERMAN, DEASY, GREEN, DALEY, GILLEN, RIVERA, WEBSTER AND MADSEN, MARCH 24, 2025

AS AMENDED ON SECOND CONSIDERATION, HOUSE OF REPRESENTATIVES, SEPTEMBER 30, 2025

AN ACT

Amending the act of December 22, 2005 (P.L.474, No.94), entitled "An act providing for security of computerized data and for the notification of residents whose personal information data was or may have been disclosed due to a breach of the security of the system; and imposing penalties," further providing for definitions, for notification of the breach of the security of the system, for exceptions and for notice exemption; repealing provisions relating to civil relief; providing for protection of personal information, for civil relief, for information security and for applicability; and repealing provisions relating to applicability.

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

Section 1. The definitions of "breach of the security of the system," "business," "encryption," "notice" and "personal information" in section 2 of the act of December 22, 2005 (P.L.474, No.94), known as the Breach of Personal Information Notification Act, amended June 28, 2024 (P.L.427, No.33), are amended and the section is amended by adding definitions to read:

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:

"Access device." A card issued by a financial institution that contains a magnetic stripe, microprocessor chip or other means for storage of information, including a credit card, debit card or stored value card.

"Breach of the security of the system." The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth. [Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.] The term does not include good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.

"Business." A sole proprietorship, partnership, corporation, association or other group, however organized and whether or not organized to operate at a profit.[, including a financial institution organized, chartered or holding a license or authorization certificate under the laws of this Commonwealth,

any other state, the United States or any other country, or the parent or the subsidiary of a financial institution.] The term includes an entity that destroys records. The term does not include a financial institution.

"Card security code." The three-digit or four-digit value printed on an access device or contained in the microprocessor chip or magnetic stripe of an access device that is used to validate access device information during the authorization process.

* * *

"Encryption." The use of an algorithmic process to transform data into a form [in] which [there is] has a low probability of assigning meaning without use of a confidential process or key.

"Encryption key." The confidential key or process designed to render the encrypted personal information useable, readable and decipherable.

* * *

"Financial institution." An office of a bank, bank and trust, trust company with banking powers, savings bank, industrial loan company, savings association, credit union or regulated lender.

* * *

"Identity theft." The possession and use, by a person, through any means, of identifying information of another person without consent of the other person to further an unlawful purpose.

* * *

"Magnetic stripe data." The data contained in the magnetic stripe of an access device.

* * *

"Notice." [May be provided by any of the following methods of notification] As follows:

(1) Written notice to the last known home address for the individual.

(2) Telephonic notice, if the individual can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the individual to provide personal information and the individual is provided with a telephone number to call or Internet website to visit for further information or assistance.

(3) E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual.

[(3.1) Electronic notice, if the notice directs the person whose personal information has been materially compromised by a breach of the security of the system to promptly change the person's password and security question or answer, as applicable, or to take other steps appropriate to protect the person's online account to the extent the entity has sufficient contact information for the person.

(4) (i) Substitute notice, if the entity demonstrates one of the following:

(A) The cost of providing notice would exceed $100,000.

(B) The affected class of subject persons to be notified exceeds 175,000.

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

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

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

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

(C) Notification to major Statewide media.]

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

(i) The cost of providing notice would exceed $100,000.

(ii) The affected class of subject persons to be notified exceeds ~~$175,000~~ 175,000. <--

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

"Person." An individual, corporation, business trust, estate trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, agency or instrumentality, public corporation or any other legal or commercial entity.

"Personal information." The following:

(1) [An individual's] The first name or first initial and last name of a resident of this Commonwealth in combination with and linked to any one or more of the following data elements [when the data elements are not encrypted or redacted] that relate to that individual:

(i) Social Security number.

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

license].

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

[(iv) Medical information in the possession of a State agency or State agency contractor.

(v) Health insurance information.

(vi) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.]

(iv) Passport number.

(v) A username or email address, in combination with a password or security question and answer that would permit access to an online account.

(vi) Medical history, medical treatment by a health care professional, diagnosis of a mental or physical condition by a health care professional or deoxyribonucleic acid profile.

(vii) Health insurance policy number, subscriber identification number or any other unique identifier used by a health insurer to identify the person.

(viii) Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes and collected from measurements or analysis of human body characteristics resulting from the uploading or electronic storage of a likeness, whether still or video capture.

(ix) An individual taxpayer identification number.

(2) The term does not include publicly available

information that is lawfully made available to the general public from Federal, State or local government records or widely distributed media.

"PIN." A personal identification code that identifies the cardholder.

"PIN verification code number." The data used to verify cardholder identity when a PIN is used in a transaction.

* * *

"Service provider." A person or entity that stores, processes or transmits access device data on behalf of another person or entity.

* * *

"Substitute notice." Any of the following:

(1) Email notice when an entity has an email address for the subject person.

(2) Conspicuous posting of the notice on the entity's Internet website if the entity maintains an Internet website.

(3) Notification to major Statewide media.

Section 2. Sections 3(a) and (b), 4 and 7(b) of the act are amended to read:

Section 3. Notification of the breach of the security of the system.

(a) General rule.--An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following [determination] 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. Except as provided in

section 4 or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.

* * *

(b) Encrypted information.--An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach [involves] is committed by a person with access to or who otherwise learns of the encryption key.

* * *

Section 4. Exceptions.

The notification required by this act may be delayed for up to three days if a law enforcement agency determines and advises the entity in writing specifically referencing this section that the notification will impede a criminal or civil investigation. [The notification required by this act shall be made after the law enforcement agency determines that it will not compromise the investigation or national or homeland security.]

Section 7. Notice exemption.

* * *

(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 is deemed to be in compliance with this act.]

(2) An entity[, a State agency or a State agency's contractor] that complies with OR, IN GOOD FAITH, ACTS TO COMPLY WITH the notification requirements or procedures pursuant to the rules, regulations, procedures or guidelines established by the entity's[, State agency's or State agency's contractor's] primary State or functional Federal regulator, shall be in compliance with this act. <--

(3) This act shall not apply to an entity, an affiliate of an entity or data subject to the Gramm-Leach-Bliley Act (Public Law 106-102, 113 Stat. 1338).

Section 3. Section 8 of the act is repealed:

[Section 8. Civil relief.

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. 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.]

Section 4. The act is amended by adding sections to read:

Section 9. Protection of personal information.

Any person who conducts business in this Commonwealth and owns, licenses or maintains personal information shall implement and maintain OR, IN GOOD FAITH, ACT TO IMPLEMENT AND MAINTAIN reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure or destruction of personal information collected or maintained in the regular course of business. <--

Section 10. Civil relief.

(a) Remedies for residents.--A resident of this Commonwealth who is adversely affected by a violation of this act, in addition to and cumulative of all other rights and remedies available at law, may bring an action to:

(1) Enjoin further violations of this act.

(2) Recover the greater of actual damages or $5,000 for each separate violation of this act.

(b) Attorney General.--The Attorney General may bring an action against a person who violates this act to:

(1) Enjoin further violations of this act.

(2) Recover a civil penalty not to exceed $10,000 per violation.

(c) Limitation period.--An action under this section must be brought within three years after the violation is discovered or by the exercise of reasonable diligence that should have been discovered, whichever is earlier.

(d) Repeated violations.--In an action under this section, the court may increase a damage award to an amount equal to not more than three times the amount otherwise available under this section if the court determines that the defendant has engaged in a pattern and practice of violating this section.

(e) Attorney fees and costs.--A prevailing plaintiff in any action commenced under this section shall be entitled to recover reasonable attorney fees and costs.

(f) Arbitration.--The rights of residents of this Commonwealth and a resident's access to the courts of this Commonwealth are in addition to and are not barred by any arbitration provision in a contract between residents and businesses. A contract entered into on or after the effective

date of this section shall not include language that requires arbitration or restricts a resident's right to legal action.

(g) Violations.--For the purpose of this section, multiple violations of this act resulting from any single action or act shall constitute one violation.

(H) REBUTTABLE PRESUMPTION.--COMPLIANCE WITH THE PROVISIONS OF THIS ACT CREATES A REBUTTABLE PRESUMPTION IN FAVOR OF AN ENTITY AGAINST A CIVIL LIABILITY CLAIM ARISING FROM CONDUCT RELATED TO THE PROVISIONS OF THIS ACT. <--

Section 11. Information security.

(a) Security or identification information.--An entity that maintains, stores or manages computerized data that includes personal information shall ~~take reasonable measures, consistent with the nature and size of the entity~~, CONSISTENT WITH THE NATURE AND SIZE OF THE ENTITY, TAKE REASONABLE MEASURES OR, IN GOOD FAITH, ACT TO TAKE REASONABLE MEASURES, to secure the system and personal information of residents of this Commonwealth that is not redacted. <--

(b) Liability.--If there is a breach of the security of the system of a person or entity that has violated this section, or that person's or entity's service provider, that person or entity shall compensate the person affected by the breach for identity theft and fraudulent charges in the amount of $5,000 for each separate violation of this act or the actual damages incurred, whichever is greater.

Section 12. Applicability.

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

Section 5. Section 29 of the act is repealed:

[Section 29. Applicability.

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

Section 6. This act shall take effect in 60 days.