PRINTER'S NO. 708

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 759 Session of 2023

INTRODUCED BY SOLOMON, PISCIOTTANO, MADDEN, KINSEY, ZABEL, ISAACSON, FREEMAN, GUENST, MERSKI, RABB, HILL-EVANS, SANCHEZ, CIRESI AND KINKEAD, MARCH 30, 2023

REFERRED TO COMMITTEE ON COMMERCE, MARCH 30, 2023

AN ACT

Providing for breach of information, for reporting requirements and for civil relief.

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 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:

"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. 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, whether or not organized to operate at a profit, including a financial institution or parent or subsidiary of the financial organization that is organized, chartered or holding a license or authorization certificate under Federal law, the laws of this Commonwealth or any other state or country. The term includes an entity that destroys records.

"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 the data 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.

"Entity." A State agency, political subdivision or an

individual or a business conducting business in this Commonwealth.

"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.

"Individual." A natural person.

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

"Notice." As follows:

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

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

(3) Email notice, if a prior business relationship exists and the person or entity has a valid email address for the individual.

(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.

(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) The first name or first initial and last name of a resident of this Commonwealth in combination with any one or more of the following data elements that relate to that individual:

(i) Social Security number.

(ii) Driver's license number or Federal or State identification card number.

(iii) 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 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/or 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.

"Records." Material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed or electromagnetically transmitted. The term does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number.

"Redact." The term includes alteration or truncation such 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 data.

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

"State agency." An agency, board, commission, authority or department of the Commonwealth or the General Assembly.

"Substitute notice." Any of the following:

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

(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 3. Notification of breach.

(a) General rule.--An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of a breach of the security of the system following discovery of the breach of the security of the system to a 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 under 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 subsection, 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 is committed by a person with access to or who otherwise learns of the encryption key.

(c) Vendor notification.--A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of a breach of the security of the system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.

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.

Section 5. Notification to consumer reporting agencies.

When an entity provides notification under this act to more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in section 603 of the Fair Credit Reporting Act under 15 U.S.C. § 1681a (relating to definitions; rules of construction) of the timing, distribution and number of notices.

Section 6. Notice exemption.

(a) Information privacy or security policy.--An entity that maintains notification procedures as part of an information, privacy or security policy for the treatment of personal information and is consistent with the notice requirements of this act shall be deemed to be in compliance with the notification requirements of this act if the entity notifies

subject persons in accordance with the policies of the entity in the event of a breach of the security of the system.

(b) Compliance with Federal requirements.--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, published at 70 Fed. Reg. 59, 15736 (March 29, 2005), is deemed to be in compliance with this act. 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 in compliance with this act.

Section 7. Protection of personal information.

Any person who conducts business in this Commonwealth and owns, licenses or maintains personal information shall 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 8. Civil relief for financial institution's liability.

(a) Reimbursement.--Whenever 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 reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of the entity's cardholders or to continue to provide services to cardholders, including any cost incurred in connection with:

(1) the cancellation or reissuance of any access device affected by the breach;

(2) the closure of a deposit, transaction, share draft or other accounts affected by the breach and any action to stop payments or block transactions with respect to the accounts;

(3) the opening or reopening of a deposit, transaction, share draft or other accounts affected by the breach;

(4) a refund or credit made to a cardholder to cover the cost of an unauthorized transaction relating to the breach; or

(5) the notification of cardholders affected by the breach.

(b) Recovery of damages.--The financial institution shall also be entitled to recover costs for damages paid by the financial institution to cardholders injured by a breach of the security of the system of a person or entity that has violated this section. Costs may not include any amounts recovered from a credit card company by a financial institution. The remedies under this subsection are cumulative and do not restrict any other right or remedy otherwise available to the financial institution.

Section 9. 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.

Section 10. 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, to secure the system and personal information of residents of this Commonwealth that is not redacted.

(b) Liability.--Whenever 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 11. Access devices and breach of security.

(a) Security or identification information and retention prohibited.--No person or entity conducting business in this Commonwealth that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code number or the full contents of any tract magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. A person or entity is in violation of this section if the person's or entity's service provider retains the data subsequent to the authorization of the transaction or, in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

(b) Liability.--Whenever 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 reimburse the financial institution that issued any access devices affected by the breach for the costs

of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of the financial institution's cardholders or to continue to provide services to cardholders, including any cost incurred in connection with:

(1) the cancellation or reissuance of any access device affected by the breach;

(2) the closure of any deposit, transaction, share draft or other accounts affected by the breach and any action to stop payments or block transactions with respect to the accounts;

(3) the opening or reopening of any deposit, transaction, share draft or other account affected by the breach;

(4) any refund or credit made to a cardholder to cover the cost of any unauthorized transaction relating to the breach; and

(5) the notification of cardholders affected by the breach.

(c) Recovery.--The financial institution shall also be entitled to recover costs for damages paid by the financial institution to cardholders injured by a breach of the security of the system of a person or entity that has violated this section. Costs do not include any amounts recovered from a credit card company by a financial institution. The remedies under this subsection are cumulative and do not restrict any other right or remedy otherwise available to the financial institution.

Section 12. Preemption.

This act relates to 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 in this Commonwealth regarding the matters expressly provided in this act.

Section 13. Applicability.

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

Section 14. Effective date.

This act shall take effect in 60 days.