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 AND GILLEN, MARCH 24, 2025

AN ACT

1 Amending the act of December 22, 2005 (P.L.474, No.94), entitled
2   "An act providing for security of computerized data and for
3   the notification of residents whose personal information data
4   was or may have been disclosed due to a breach of the
5   security of the system; and imposing penalties," further
6   providing for definitions, for notification of the breach of
7   the security of the system, for exceptions and for notice
8   exemption; repealing provisions relating to civil relief;
9   providing for protection of personal information, ~~for civil~~ <--
10   ~~relief for financial institution's liability,~~ for civil
11   relief, for information security~~, for access devices and~~ <--
12   ~~breach of security~~ and for applicability; and repealing
13   provisions relating to applicability.

14   The General Assembly of the Commonwealth of Pennsylvania

15 hereby enacts as follows:

16   Section 1. The definitions of "breach of the security of the

17 system," "business," "encryption," "notice" and "personal

18 information" in section 2 of the act of December 22, 2005

19 (P.L.474, No.94), known as the Breach of Personal Information

20 Notification Act, amended June 28, 2024 (P.L.427, No.33), are

21 amended and the section is amended by adding definitions to

22 read:

1 Section 2. Definitions.

2   The following words and phrases when used in this act shall

3 have the meanings given to them in this section unless the

4 context clearly indicates otherwise:

5   "Access device." A card issued by a financial institution

6 that contains a magnetic stripe, microprocessor chip or other

7 means for storage of information, including a credit card, debit

8 card or stored value card.

9   "Breach of the security of the system." The unauthorized

10 access and acquisition of computerized data that materially

11 compromises the security or confidentiality of personal

12 information maintained by the entity as part of a database of

13 personal information regarding multiple individuals and that

14 causes or the entity reasonably believes has caused or will

15 cause loss or injury to any resident of this Commonwealth. [Good

16 faith acquisition of personal information by an employee or

17 agent of the entity for the purposes of the entity is not a

18 breach of the security of the system if the personal information

19 is not used for a purpose other than the lawful purpose of the

20 entity and is not subject to further unauthorized disclosure.]

21 The term does not include good faith acquisition of personal

22 information by an employee or agent of the entity for the

23 purposes of the entity if the personal information is not used

24 for a purpose other than the lawful purpose of the entity and is

25 not subject to further unauthorized disclosure.

26   "Business." A sole proprietorship, partnership, corporation,

27 association or other group, however organized and whether or not

28 organized to operate at a profit.[, including a financial

29 institution organized, chartered or holding a license or

30 authorization certificate under the laws of this Commonwealth,

1 any other state, the United States or any other country, or the

2 parent or the subsidiary of a financial institution.] The term

3 includes an entity that destroys records. The term does not

4 include a financial institution.

5 "Card security code." The three-digit or four-digit value

6 printed on an access device or contained in the microprocessor

7 chip or magnetic stripe of an access device that is used to

8 validate access device information during the authorization

9 process.

10 * * *

11 "Encryption." The use of an algorithmic process to transform

12 data into a form [in] which [there is] has a low probability of

13 assigning meaning without use of a confidential process or key.

14 "Encryption key." The confidential key or process designed

15 to render the encrypted personal information useable, readable

16 and decipherable.

17 * * *

18 "Financial institution." An office of a bank, bank and

19 trust, trust company with banking powers, savings bank,

20 industrial loan company, savings association, credit union or

21 regulated lender.

22 * * *

23 "Identity theft." The possession and use, by a person,

24 through any means, of identifying information of another person

25 without consent of the other person to further an unlawful

26 purpose.

27 * * *

28 "Magnetic stripe data." The data contained in the magnetic

29 stripe of an access device.

30 * * *

1   "Notice." [May be provided by any of the following methods

2 of notification] As follows:

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

4   the individual.

5   (2) Telephonic notice, if the individual can be

6   reasonably expected to receive it and the notice is given in

7   a clear and conspicuous manner, describes the incident in

8   general terms and verifies personal information but does not

9   require the individual to provide personal information and

10   the individual is provided with a telephone number to call or

11   Internet website to visit for further information or

12   assistance.

13   (3) E-mail notice, if a prior business relationship

14   exists and the person or entity has a valid e-mail address

15   for the individual.

16   [(3.1) Electronic notice, if the notice directs the

17 person whose personal information has been materially

18 compromised by a breach of the security of the system to

19 promptly change the person's password and security question

20 or answer, as applicable, or to take other steps appropriate

21 to protect the person's online account to the extent the

22 entity has sufficient contact information for the person.

23   (4) (i) Substitute notice, if the entity demonstrates

24   one of the following:

25   (A) The cost of providing notice would exceed

26            $100,000.

27   (B) The affected class of subject persons to be

28   notified exceeds 175,000.

29   (C) The entity does not have sufficient contact

30   information.

1   (ii) Substitute notice shall consist of all of the

2   following:

3   (A) E-mail notice when the entity has an e-mail

4   address for the subject persons.

5   (B) Conspicuous posting of the notice on the

6   entity's Internet website if the entity maintains

7   one.

8   (C) Notification to major Statewide media.]

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

10   the following:

11   (i) The cost of providing notice would exceed

12   $100,000.

13   (ii) The affected class of subject persons to be

14   notified exceeds $175,000.

15   (iii) The entity does not have sufficient contact

16   information.

17   "Person." An individual, corporation, business trust, estate

18   trust, partnership, limited liability company, association,

19   joint venture, government, governmental subdivision, agency or

20   instrumentality, public corporation or any other legal or

21   commercial entity.

22   "Personal information." The following:

23   (1) [An individual's] The first name or first initial

24   and last name of a resident of this Commonwealth in

25   combination with and linked to any one or more of the

26   following data elements [when the data elements are not

27   encrypted or redacted] that relate to that individual:

28   (i) Social Security number.

29   (ii) Driver's license number or a Federal or State

30   identification card number [issued in lieu of a driver's

1   license].

2   (iii) Financial account number, credit or debit card

3   number, in combination with any required security code,

4   access code or password that would permit access to [an

5   individual's] a resident's financial account.

6   [(iv) Medical information in the possession of

7   a State agency or State agency contractor.

8   (v) Health insurance information.

9   (vi) A user name or e-mail address, in combination

10   with a password or security question and answer that

11   would permit access to an online account.]

12   (iv) Passport number.

13   (v) A username or email address, in combination with

14   a password or security question and answer that would

15   permit access to an online account.

16   (vi) Medical history, medical treatment by a health

17   care professional, diagnosis of a mental or physical

18   condition by a health care professional or

19   deoxyribonucleic acid profile.

20   (vii) Health insurance policy number, subscriber

21   identification number or any other unique identifier used

22   by a health insurer to identify the person.

23   (viii) Unique biometric data generated from

24   measurements or analysis of human body characteristics

25   for authentication purposes and collected from

26   measurements or analysis of human body characteristics

27   resulting from the uploading or electronic storage of a

28   likeness, whether still or video capture.

29   (ix) An individual taxpayer identification number.

30   (2) The term does not include publicly available

1   information that is lawfully made available to the general

2   public from Federal, State or local government records or

3   widely distributed media.

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

5   cardholder.

6   "PIN verification code number." The data used to verify

7   cardholder identity when a PIN is used in a transaction.

8   * * *

9   "Service provider." A person or entity that stores,

10   processes or transmits access device data on behalf of another

11   person or entity.

12   * * *

13   "Substitute notice." Any of the following:

14   (1) Email notice when an entity has an email address for

15   the subject person.

16   (2) Conspicuous posting of the notice on the entity's

17   Internet website if the entity maintains an Internet website.

18   (3) Notification to major Statewide media.

19   Section 2. Sections 3(a) and (b), 4 and 7(b) of the act are

20   amended to read:

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

22   system.

23   (a) General rule.--An entity that maintains, stores or

24   manages computerized data that includes personal information

25   shall provide notice of any breach of the security of the system

26   following [determination] discovery of the breach of the

27   security of the system to any resident of this Commonwealth

28   whose unencrypted and unredacted personal information was or is

29   reasonably believed to have been accessed and acquired by an

30   unauthorized person. Except as provided in section 4 or in order

1 to take any measures necessary to determine the scope of the

2 breach and to restore the reasonable integrity of the data

3 system, the notice shall be made without unreasonable delay. For

4 the purpose of this section, a resident of this Commonwealth may

5 be determined to be an individual whose principal mailing

6 address, as reflected in the computerized data which is

7 maintained, stored or managed by the entity, is in this

8 Commonwealth.

9   * * *

10   (b) Encrypted information.--An entity must provide notice of

11 the breach if encrypted information is accessed and acquired in

12 an unencrypted form, if the security breach is linked to a

13 breach of the security of the encryption or if the security

14 breach [involves] is committed by a person with access to or who

15 otherwise learns of the encryption key.

16   * * *

17 Section 4. Exceptions.

18   The notification required by this act may be delayed for up

19 to three days if a law enforcement agency determines and advises

20 the entity in writing specifically referencing this section that

21 the notification will impede a criminal or civil investigation.

22 [The notification required by this act shall be made after the

23 law enforcement agency determines that it will not compromise

24 the investigation or national or homeland security.]

25 Section 7. Notice exemption.

26   * * *

27   (b) Compliance with Federal requirements.--

28   [(1) A financial institution that complies with the

29   notification requirements prescribed by the Federal

30   Interagency Guidance on Response Programs for Unauthorized

1   Access to Customer Information and Customer Notice is deemed

2   to be in compliance with this act.]

3   (2) An entity[, a State agency or a State agency's

4   contractor] that complies with the notification requirements

5   or procedures pursuant to the rules, regulations, procedures

6   or guidelines established by the entity's[, State agency's or

7   State agency's contractor's] primary State or functional

8   Federal regulator, shall be in compliance with this act.

9   (3) This act shall not apply to an entity, an affiliate

10   of an entity or data subject to the Gramm-Leach-Bliley Act

11   (Public Law 106-102, 113 Stat. 1338).

12   Section 3. Section 8 of the act is repealed:

13   [Section 8. Civil relief.

14   A violation of this act shall be deemed to be an unfair or

15   deceptive act or practice in violation of the act of December

16   17, 1968 (P.L.1224, No.387), known as the Unfair Trade Practices

17   and Consumer Protection Law. The Office of Attorney General

18   shall have exclusive authority to bring an action under the

19   Unfair Trade Practices and Consumer Protection Law for a

20   violation of this act.]

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

22   Section 9. Protection of personal information.

23   Any person who conducts business in this Commonwealth and

24   owns, licenses or maintains personal information shall implement

25   and maintain reasonable procedures and practices to prevent the

26   unauthorized acquisition, use, modification, disclosure or

27   destruction of personal information collected or maintained in

28   the regular course of business.

29   Section 10. Civil relief for financial institution's liability. <--

30   (a) Reimbursement. If there is a breach of the security of

1 ~~the system of a person or entity that has violated this section,~~

2 ~~or that person's or entity's service provider, that person or~~

3 ~~entity shall reimburse the financial institution that issued any~~

4 ~~access devices affected by the breach for the costs of~~

5 ~~reasonable actions undertaken by the financial institution as a~~

6 ~~result of the breach in order to protect the information of the~~

7 ~~entity's cardholders or to continue to provide services to~~

8 ~~cardholders, including any cost incurred in connection with:~~

9 ~~(1) the cancellation or reissuance of any access device~~

10 ~~affected by the breach;~~

11 ~~(2) the closure of a deposit, transaction, share draft~~

12 ~~or other accounts affected by the breach and any action to~~

13 ~~stop payments or block transactions with respect to the~~

14 ~~accounts;~~

15 ~~(3) the opening or reopening of a deposit, transaction,~~

16 ~~share draft or other accounts affected by the breach;~~

17 ~~(4) a refund or credit made to a cardholder to cover the~~

18 ~~cost of an unauthorized transaction relating to the breach;~~

19 ~~or~~

20 ~~(5) the notification of cardholders affected by the~~

21 ~~breach.~~

22 ~~(b) Recovery of damages. The financial institution shall~~

23 ~~also be entitled to recover costs for damages paid by the~~

24 ~~financial institution to cardholders injured by a breach of the~~

25 ~~security of the system of a person or entity that has violated~~

26 ~~this section. Costs may not include any amounts recovered from a~~

27 ~~credit card company by a financial institution. The remedies~~

28 ~~under this subsection are cumulative and do not restrict any~~

29 ~~other right or remedy otherwise available to the financial~~

30 ~~institution.~~

1 Section ~~11~~ 10. Civil relief.   <--

2   (a) Remedies for residents.--A resident of this Commonwealth

3 who is adversely affected by a violation of this act, in

4 addition to and cumulative of all other rights and remedies

5 available at law, may bring an action to:

6   (1) Enjoin further violations of this act.

7   (2) Recover the greater of actual damages or $5,000 for

8   each separate violation of this act.

9   (b) Attorney General.--The Attorney General may bring an

10 action against a person who violates this act to:

11   (1) Enjoin further violations of this act.

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

13   violation.

14   (c) Limitation period.--An action under this section must be

15 brought within three years after the violation is discovered or

16 by the exercise of reasonable diligence that should have been

17 discovered, whichever is earlier.

18   (d) Repeated violations.--In an action under this section,

19 the court may increase a damage award to an amount equal to not

20 more than three times the amount otherwise available under this

21 section if the court determines that the defendant has engaged

22 in a pattern and practice of violating this section.

23   (e) Attorney fees and costs.--A prevailing plaintiff in any

24 action commenced under this section shall be entitled to recover

25 reasonable attorney fees and costs.

26   (f) Arbitration.--The rights of residents of this

27 Commonwealth and a resident's access to the courts of this

28 Commonwealth are in addition to and are not barred by any

29 arbitration provision in a contract between residents and

30 businesses. A contract entered into on or after the effective

1 date of this section shall not include language that requires

2 arbitration or restricts a resident's right to legal action.

3   (g) Violations.--For the purpose of this section, multiple

4 violations of this act resulting from any single action or act

5 shall constitute one violation.

6 Section ~~12~~ 11. Information security.   <--

7   (a) Security or identification information.--An entity that

8 maintains, stores or manages computerized data that includes

9 personal information shall take reasonable measures, consistent

10 with the nature and size of the entity, to secure the system and

11 personal information of residents of this Commonwealth that is

12 not redacted.

13   (b) Liability.--If there is a breach of the security of the

14 system of a person or entity that has violated this section, or

15 that person's or entity's service provider, that person or

16 entity shall compensate the person affected by the breach for

17 identity theft and fraudulent charges in the amount of $5,000

18 for each separate violation of this act or the actual damages

19 incurred, whichever is greater.

20 ~~Section 13. Access devices and breach of security.~~   <--

21 ~~(a) Security or identification information and retention~~

22 ~~prohibited. A person or entity conducting business in this~~

23 ~~Commonwealth that accepts an access device in connection with a~~

24 ~~transaction may not retain the card security code data, the PIN~~

25 ~~verification code number or the full contents of any tract~~

26 ~~magnetic stripe data, subsequent to the authorization of the~~

27 ~~transaction or in the case of a PIN debit transaction,~~

28 ~~subsequent to 48 hours after authorization of the transaction. A~~

29 ~~person or entity is in violation of this section if the person's~~

30 ~~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.--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 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

1   ~~of the system of a person or entity that has violated this~~

2   ~~section. Costs do not include any amounts recovered from a~~

3   ~~credit card company by a financial institution. The remedies~~

4   ~~under this subsection are cumulative and do not restrict any~~

5   ~~other right or remedy otherwise available to the financial~~

6   ~~institution.~~

7   Section ~~14~~ 12. Applicability.   **<--**

8   This act shall apply to the discovery or notification of a

9   breach in the security of personal information that occurs on or

10   after the effective date of this section.

11   Section 5. Section 29 of the act is repealed:

12   [Section 29. Applicability.

13   This act shall apply to the determination or notification of

14   a breach of the security of the system that occurs on or after

15   the effective date of this section.]

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