

HB 997 -- Redline

Printer's No. PN1621 to Printer's No. PN2381 -- An Act amending the act of December 22, 2005 (P.L.474, No.94), known as the Breach of Personal Information Notification Act, 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.

Deletions ~~struck~~ · Insertions underlined

PRIOR PRINTER'S ~~NO.~~NOS.

~~1086~~1086, 1621 PRINTER'S NO.

~~1621~~2381 THE GENERAL ASSEMBLY OF PENNSYLVANIA HOUSE BILL Session of No.

997 2025 INTRODUCED BY SOLOMON, HILL-EVANS, CERRATO, HOWARD, FREEMAN, ~~KAZEEM, GIRAL, GUENST, MERSKI, CEPEDA-FREYTIJZ, PIELLI,~~ SANCHEZ, D.

WILLIAMS, CIRESI, STEELE, SHUSTERMAN, DEASY, GREEN, ~~DALEY~~DALEY, GILLEN, RIVERA, WEBSTER AND GILLEN, MADSEN, MARCH 24, 2025 AS ~~REPORTED~~AMENDED FROM COMMITTEE ON COMMERCE, SECOND CONSIDERATION, HOUSE OF REPRESENTATIVES, ~~AS~~SEPTEMBER AMENDED, 30, MAY 6, 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 of exemption;

providing for protection of personal information, for civil ~~relief for financial institution's liability, for civil~~ relief, for information ~~security, for access devices and~~ ~~breach of~~ security and for applicability;

"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, ~~20250HB0997PN1621~~20250HB0997PN2381 - 2 - 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.

* * * ~~20250HB0997PN1621~~20250HB0997PN2381 - 3 - "Notice." [May be provided by any of the following methods of notification] As follows:

~~20250HB0997PN1621~~20250HB0997PN2381 - 4 - (ii) Substitute notice shall consist of all of the following:

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

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

(ii) Driver's license number or a Federal or State identification card number [issued in lieu of a driver's ~~20250HB0997PN1621~~20250HB0997PN2381 - 5 - license].

(2) The term does not include publicly available ~~20250HB0997PN1621~~20250HB0997PN2381 - 6 - information that is lawfully made available to the general public from Federal, State or local government records or widely distributed media.

(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 ~~20250HB0997PN2381~~ - 7 - section 4 or in order ~~20250HB0997PN1621~~ - 7 - 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.

* * * (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 ~~20250HB0997PN1621~~20250HB0997PN2381 - 8 - 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.

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.

~~Civil relief for financial institution's liability.~~

~~-- (a) Reimbursement.-- If there is a breach of the security of 20250HB0997PN1621 - 9 - 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.~~

~~20250HB0997PN1621 - 10 - Section 11 10.~~

~~-- (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:~~

A contract entered into on or after the effective ~~20250HB0997PN1621~~ 20250HB0997PN2381 - 1110 - date of this section shall not include language that requires arbitration or restricts a resident's right to legal action.

Section(H) 12REBUTTABLE 11-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.

~~-- (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.~~

~~Section 13-12.~~

~~Access devices and breach of security.~~

~~-- (a) Security or identification information and retention prohibited.-- A person or entity conducting business in this Commonwealth that accepts an access device in connection with a transaction may not 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 20250HB0997PN1621 - 12 - 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 20250HB0997PN1621 - 13 - 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 14 12.~~

~~—~~ 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.

20250HB0997PN2381 - 11 - [Section 29.

~~20250HB0997PN1621~~20250HB0997PN2381 - ~~14~~12 -