

<<Mail Date>>

<<FirstName>> <<LastName>>

<<Street Address>>

<<City>>, <<State>> <<Zip Code>>

RE: Notice of Security Incident

Dear <<FirstName>> <<LastName>>,

The Citizens Bank of Philadelphia (“TCB”) values and respects the privacy and security of your information. We are writing to inform you of a data security incident that may have involved some of your information. This letter includes information about the incident, our offer of free credit monitoring and identity theft protection services, and additional steps you can take to help protect your personal information, should you feel it appropriate to do so.

What Happened? Upon detecting suspicious activity within our computer network, TCB immediately retained cybersecurity experts and took action to secure our network, launched an investigation to determine the extent of the incident, and notified our banking regulators and law enforcement. The investigation determined that an unknown third-party temporarily accessed the email account of one of our employees. We conducted a comprehensive review of the affected data in that account to determine if any personal information was impacted. We determined that some of your personal information was potentially involved in the incident. However, there is no evidence to indicate that any information has been misused. Nonetheless, we are providing this notice to you out of an abundance of caution.

What Information Was Involved? The personal information involved may have included your <<Letter Text>>.

What We Are Doing. Please know that protecting personal information is something we take very seriously. Upon discovery of the incident, we took immediate action to stop any further access to affected email account. We also quickly brought in cybersecurity experts to conduct a diligent investigation to determine the nature, scope, and impact of the incident. We also supplemented our existing security measures to further strengthen our network and reduce the likelihood of a similar incident occurring in the future.

As an added precaution, we are offering you <<Credit Monitoring Duration>> of free credit monitoring and identity theft protection through Experian’s IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. This letter contains additional information on these services, including instructions on how to activate your complementary membership.

What You Can Do. You can enroll in the complementary credit monitoring and identity theft protection being offered to you. There is no cost for you to enroll in these services. This letter also includes other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or suspicious activity on a regular basis.

For More Information. We sincerely regret any inconvenience or concern this incident may cause. If you have additional questions, please call us at 601-656-4692 between 9:00 a.m. and 5:00 p.m. Central Time, Monday through Friday (excluding major U.S. holidays).

Sincerely,

The Citizens Bank of Philadelphia

STEPS YOU CAN TAKE

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for <<Credit Monitoring Duration>>.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for <<Credit Monitoring Duration>> from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary <<Credit Monitoring Duration>> membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by 12/31/2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: <<Activation Code>>

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian at 1-833-931-7577 or Experian's customer care team at 1-877-890-9332 by 12/31/2024. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR <<CREDIT MONITORING DURATION>> EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Freeze Your Credit File

You have a right to place a 'security freeze' on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Note that a security freeze generally does not apply to existing account relationships and when a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a security freeze.

To place a security freeze on your credit report, contact each of the three major consumer reporting agencies using the contact information listed below:

Equifax

P.O. Box 740241
Atlanta, GA 30374
1-800-525-6285
www.equifax.com

Experian

P.O. Box 4500
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-888-680-7289
www.transunion.com

To request a security freeze, you will need to provide the following:

1. Your full name with middle initial and any suffixes;
2. Social Security number,
3. Date of birth;
4. Current address and previous addresses for the past five (5) years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. Other personal information as required by the applicable credit reporting agency.

If you request a security freeze via toll-free telephone or online, the credit reporting agencies have one (1) business day after receiving the request to place the freeze. In the case of a request made by mail, the bureaus have three (3) business days after receiving your request to place a security freeze on your credit report. If you request a lift of the security freeze online or by phone, the credit reporting agency must lift the freeze within one (1) hour. If you request a lift of a credit freeze by mail, then the credit reporting agency must lift the credit freeze no later than three (3) business days after receiving your request.

Fraud Alerts

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is an alert lasting 7 years. Contact one of the credit reporting agencies listed above to activate an alert.

Monitor Your Account Statements and Report Fraud

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, carefully reviewing your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity. Report suspicious or fraudulent charges to your insurance statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor and law enforcement.

Order Your Free Annual Credit Report

Visit www.annualcreditreport.com or call 877-322-8228 to obtain one free copy of your credit report from each of the three major credit reporting bureaus annually. Periodically review a copy of your credit report for discrepancies and identify any accounts you did not open or inquiries you did not authorize.

File or Obtain a Police Report

You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report incidents of identity theft to local law enforcement or to the Attorney General.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself by contacting the Federal Trade Commission (FTC) or state Attorney General. The FTC provides information at www.ftc.gov/idtheft. The FTC can also be reached by phone: 1-877-438-4338; TTY: 1-866-653-4261 or by writing: 600 Pennsylvania Ave., NW, Washington, D.C. 20580.

Fair Credit Reporting Act

You also have rights under the federal Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Please note that identity theft victims and active duty military personnel may have additional rights under the FCRA.

For residents of New York: The Attorney General may be contacted at: Office of Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For residents of the District of Columbia: The Attorney General may be contacted at: 400 6th Street NW, Washington, D.C. 20001, by phone at (202) 727-3400; and, <https://oag.dc.gov/>. You may obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.