central bank of kansas city

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

<<MailID>>
<<Name 1>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>>, <<State>><<Zip>>
<<Country>>

<<Date>>

<<Variable Data 1>>

Dear <<Name 1>>:

Central Bank of Kansas City ("CBKC") is a bank that offers both personal and business banking solutions to its clients. We are writing to notify you of an incident that may impact some of your information. This notice provides you with details about the incident, our response, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened?

Our security controls identified unusual activity involving a CBKC email account. We immediately took steps to secure the account and investigated the activity. The investigation determined that certain CBKC email accounts may have been accessed by an unknown individual between January 16 and January 19, 2024. We reviewed the accounts for sensitive information and completed this review on May 13, 2024.

What Information Was Involved?

The investigation determined that your name and the following types of information relating to you were present in an involved email account at the time of the incident: <<Breached Elements>>.

What We Are Doing.

We take this incident and the security of the information in our care very seriously. Upon identifying the unusual activity, we took steps to secure the employee email account, assess the security of the email environment, and investigate the activity. We also proactively notified federal law enforcement and relevant regulators of this incident.

CBKC has an ongoing commitment to safeguarding the privacy and security of information provided to us. As part of that commitment, we reviewed our existing policies and procedures and implemented additional security measures within our email environment.

As an added precaution, we are offering you access to monitoring services for twenty-four (24) months at no cost to you. Information about these services and instructions on how to activate them may be found in the *Steps You Can Take to Help Protect Personal Information* section of this notice. Please note, due to privacy restrictions, we are unable to enroll you in these services on your behalf.

What You Can Do.

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next twelve (12) to twenty-four (24) months. Suspicious activity should be promptly reported to relevant parties including a financial institution. More information and resources can be found in the attached *Steps You Can Take to Help Protect Personal Information* section of this notice. Additionally, we encourage you to enroll in the offered complimentary monitoring services.

For More Information.

We recognize you may have additional questions not addressed by this letter. If you have questions or concerns, please call our dedicated assistance line at 888-498-5232 Monday through Friday, between 9:00 AM and 9:00 PM Eastern time.

Sincerely,

Central Bank of Kansas City

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

Identity Defense

<<Name 1>>
Enter your Activation Code: <<ActivationCode>>
Enrollment Deadline: <<Deadline>>
Service Term: <<CM Duration>>*

Identity Defense Complete – Key Features:

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- $1 Million Identity Theft Insurance**

Enrollment Instructions – To enroll in Identity Defense, visit app.identitydefense.com/enrollment/activate/cbkc

1. **Enter your unique Activation Code** <<ActivationCode>>

   Enter your Activation Code and click 'Redeem Code'.

2. **Create Your Account**

   Enter your email address, create your password, and click 'Create Account'.

3. **Register**

   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.

4. **Complete Activation**

   Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Deadline>>. After **<<Deadline>>**, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by <<Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at **866.622.9303**.

* Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.
** Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should consumers wish to place a fraud alert, please contact any of the three (3) major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two (2) to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three (3) major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348	Experian Fraud Alert P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze P.O. Box 105788, Atlanta, GA 30348	Experian Credit Freeze P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094

Additional Information

As a best practice, consumers should change all passwords to their personal accounts on a regular basis, use strong passwords, and refrain from using the same password for multiple accounts. Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or

suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.