usbank.com

[Letter date]

[Recipient's name]
[Address]
[City, State Zip]

Dear [Recipient's name]:

We value your confidence in us and place the privacy and security of your information as a top priority, which is why we are writing to let you know about an incident that involved your personal information.

What happened:
You may have already become aware of this incident. However, as a precautionary measure, we're informing you via letter. During the week of April 8, 2025, due to a technical configuration error, your account was accessed by a fraudulent actor and personal information was made visible. The information included your account number, name, address, phone and email address.

What U.S. Bank is doing:
To limit exposure of your information, we updated the system to prevent the unauthorized user from accessing your account. Additionally, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the two major credit reporting companies.

To enroll in this service, go to the *my*TrueIdentity website at **mytrueidentity.com. I**n the space referenced as "Enter Activation Code," enter the following 12-letter Activation Code and follow the three steps to receive your credit monitoring service online within minutes.

Unique activation code: << TU Code>>
Once you are enrolled, you will be able to obtain an initial 3-in-1 credit report and credit scores along with one year of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian® and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes dark web internet identity monitoring, the ability to lock and unlock your TransUnion credit report, access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Certain policy limitations and exclusions may apply.)

If you believe you may be a victim of identity theft, please call the TransUnion Fraud Response Services toll-free hotline at 855-288-5422**.** When prompted, enter the following 6-digit telephone pass code 698500 to speak to a TransUnion representative about your identity theft issue.

You can sign up for the *my*TrueIdentity online credit monitoring anytime between now and December 31st, 2025. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, Experian and Equifax or an address in the United States (or its territories) and a valid Social Security number or are under the age of 18. Enrolling in this service will not affect your credit score.

What you can do:
Whether or not you enroll in credit monitoring, we recommend that you place a "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies, so you do not need to contact each of them separately.

You can also request a free Security Freeze (aka "Credit Freeze") on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a credit freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A credit freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit.

The contact information for the three nationwide credit reporting companies is:

Equifax	**TransUnion**	**Experian**
PO Box 740256	PO Box 2000	PO Box 9554
Atlanta, GA 30374	Chester, PA 19016	Allen, TX 75013
equifax.com	transunion.com/fraud	experian.com/fraud
800-525-6285	800-680-7289	888-397-3742

Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 877-322-8228 or make a request online at annualcreditreport.com. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. You have a right to obtain a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the Federal Trade Commission (FTC) at identitytheft.gov or at 877-ID-THEFT (438-4338) or send the complaint to the Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. Also visit the FTC's website at ftc.gov/idtheft to review their free identity theft resources such as their comprehensive step-by-step guide "*Identity Theft - A Recovery Plan.*"

Finally, we recommend that you check your bank accounts regularly and look for unusual withdrawals, deposits and transactions. If you have questions regarding this notice or have questions about activity on your account, please call U.S. Bank 24-Hour Banking at 800-USBANKS (872-2657).

I want to thank you on behalf of U.S. Bank for your business, as well as the confidence you place in us. We take that trust seriously and are sorry that this situation has occurred.

Sincerely,

Justin Windschitl
Executive Vice President
U.S. Bank