



<<MemberFirstName>> <<MemberLastName>>

<<Date>> (Format: Month Day, Year)

<<Address1>>

<<Address2>>

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

Dear <<MemberFirstName>> <<MemberLastName>>,

At U.S. Bank, we are committed to protecting your confidential information and making sure you are aware of situations that may affect you. We recently discovered a data security incident involving a third party that may have exposed some of your personal data. Although we have no indication that any information about you was stolen from U.S. Bank or that our systems were compromised, we are taking this issue very seriously. It's important to note that this incident happened outside the U.S. Bank environment, and it has been addressed and resolved. However, we wanted to reach out to explain what happened and how you can protect yourself.

What happened?

Earlier this year, someone fraudulently accessed a limited number of current and former employees' W-2 information using a third-party online portal. The unauthorized individuals used confidential personal information from other sources to potentially establish a registration in your name. This affected about two percent of U.S. Bank employees, some of whom also had fraudulent tax returns filed in their names. We took immediate steps to address this situation once we learned about it, and we are reviewing processes with our vendor partners to ensure this does not happen again.

What information was involved?

We believe the fraudsters used your name, Social Security number (SSN) and date of birth without your permission. We do not know how they obtained this information. Using that data, they were able to download your W-2, which includes your name, SSN, home address, and information about your income, tax withholding, and payroll deductions.

What steps did we take?

We shut down access to the third-party online portal, and no current or former employees can access it. While this may be inconvenient for some of you, we believe this was the right thing to do for now. If you need a copy of your W-2, please contact the U.S. Bank Employee Service Center at 800.806.7009.

What are we doing to help?

We take situations like this seriously and we want to do the right thing, so we asked Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Theft Insurance, Identity Consultation, and Identity Restoration.

Visit kroll.idMonitoringService.com to enroll and take advantage of your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-855-269-6546. Additional information describing your services is included with this letter. To take full advantage of the two years of free coverage, we strongly suggest you activate these services within 90 days of this letter.

What else can you do?

Please review the "Additional Resources" materials included with this letter. This information describes steps you can take to help protect yourself, including recommendations from the Federal Trade Commission about identity theft protection and how to place a fraud alert or a security freeze on your credit file.

If you know or think you might be a victim of tax-related identity theft, the Internal Revenue Service (IRS) recommends you take the following actions:

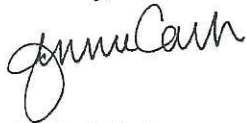
- Respond immediately to any IRS notice; call the number provided or, if instructed, go to [IDVerify.irs.gov](https://idverify.irs.gov).
- Complete IRS Form 14039, Identity Theft Affidavit, if your e-filed return is rejected because of a duplicate filing under your SSN or if you are instructed to do so. Use a fillable form at [IRS.gov](https://irs.gov), print, then attach the form to your return and mail according to instructions.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.

For more information, consult the "Taxpayer Guide to Identity Theft," which can be found at <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft>.

If you have more questions, please call 1-855-269-6546, Monday through Friday from 8 a.m. to 5 p.m. Central Time. Please have your membership number ready.

Protecting your information is important to us. Thank you for your understanding and consideration.

Sincerely,



Jennie P. Carlson
Executive Vice President of Human Resources
U.S. Bank

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

For Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is \$5.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Triple Bureau Credit Monitoring and a TransUnion Credit Report.

You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll investigator, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals buy, sell, and trade personal information. You'll be promptly notified if evidence of your identity information being traded or sold is discovered.

Public Persona

Public Persona monitors public record databases for names, aliases, and addresses that are associated with your Social Security number. If information is found, an alert email is sent.

Quick Cash Scan

Quick Cash Scan monitors thousands of short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll investigator for more information.

\$1 Million Identity Theft Insurance

Reimburses you for out-of-pocket expenses totaling up to \$1 million in legal costs for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Identity Consultation

You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Restoration

If you become a victim of identity theft, an experienced licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your investigator can dig deep to uncover all aspects of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.