20329

usbank.com

[Letter date]

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

Re: Your U.S. Bank account ending in XXXX

Dear [Customer Name]:

Thank you for choosing U.S. Bank as your financial services provider. We're here to help safeguard your data and want to let you know that our security team identified what is called a credential reuse attack on your account.

What is a credential reuse attack:
Credential reuse attacks occur when unauthorized parties use stolen user ID and passwords that are generally obtained from a compromised site where you used the same log in credentials. That's why it's recommended that you choose a unique ID and password for each online account and not one that has been used previously.

What information was involved:
In addition to your user ID and password, we have reason to believe that your account information may be at risk. This includes information such as your account number, name, address and phone number.

What are we doing:
To limit exposure of your information, we immediately suspended your online and mobile banking access (user ID) and have since placed restraints on your account. We also attempted to call you directly to issue a new account number and online profile for you.

What you can do:
- Please call the U.S. Bank Fraud Liaison Center at 877.595.6256, so we can issue you a new account number.
- Remember to check your accounts regularly and look for unusual transactions. For more ways to help keep yourself safe from fraud, visit **usbank.com/security**.

Please accept our apologies for any inconvenience this may cause, but know the security of your account is of the utmost importance to us. We appreciate your business and look forward to continuing to serve you.

Sincerely,

U.S. Bank

usbank

The security of your information is a top priority for U.S. Bank. We recently noticed some suspicious log in attempts that may impact your account. **As a precautionar measure, we have locked your Online Banking account and are asking you t reset your password**. To reset your password, visit the app or go to usbank.com and click "Get login help."

We also encourage our customers to monitor their financial accounts closely on a regular basis. Here are some steps you can take to protect yourself from fraudulen activity on your accounts:

- When resetting your password, it's recommended to choose a unique password and not one that has been used previously.
- U.S. Bank will never initiate a request for your sensitive information like you Personal ID, Password, Social Security Number, Personal Identification Number (PIN) or Account Number. For your safety, never share this information with anyone, at any time.
- Monitor your accounts regularly and watch for unusual transactions.
- Activate fraud watches, email and text alerts on all accounts (checking, saving, credit cards) to help spot unusual transactions quickly.
- Read security alerts when you receive them. U.S. Bank will send a security alert when certain changes are made to your account—pay attention to these, they are designed to help identify fraud quickly.
- Leverage two factor authentication (i.e.: register your mobile number), whenever available. By using this type of authentication process, you reduc the likelihood of someone being able to fraudulently change or access your account.

We are always here to assist. Please contact us at 800.USBANKS (800.872.265 if you have any questions or identify any suspicious activity on your account.

Get the app 

Email intended for: sumedh.nandedkar1@usbank.com

Protecting your privacy is our priority. We'll never initiate a request via email for your sensitive information like your Personal ID, Password, Social Security Number, Personal Identification Number (PIN) or Account Number. For your safety, never share this information with anyone, at any time. If you receive an email asking for your sensitive information, or would like to report a suspicious email, forward it to fraud_help@usbank.com or call U.S. Bank Customer Service immediately at 800.USBANKS (872.2657).

Get more details about recognizing online fraud issues.

Note: If you'd rather not follow links from this email, you can access information on all U.S. Bank products and services at usbank.com.

To ensure that you continue to receive email from us, please add us to your Address Book (1800USBanks@email.usbank.com). Thank you.

You are receiving this email as a service to your account because you are a U.S. Bank customer.

View the U.S. Bank Privacy Pledge.

U.S. Bank, EP-MN-L20D, 200 South 6th Street, Minneapolis, MN 55402

© 2021 U.S. Bank. Equal Housing Lender. Member FDIC.