[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