Fraud
Prevention

10 STEPS TO MINIMIZE
YOUR RISK OF FRAUD AND THEFT

1. Never reply to emails, phone calls, or text messages that request your personal information

U.S. Bank will never contact you by phone or email to ask for your account numbers, PIN numbers, or any other confidential information. U.S. Bank only asks you for confidential information to verify your identity when you initiate contact with us. To contact us online, type usbank.com on your Internet browser. To contact us by phone, dial one of the toll-free or local numbers listed online or in your account statement.

2. Make a list of the contents of your wallet

Make a list of every ATM or debit card, credit card, driver's license number and other forms of ID you carry in your wallet or purse. Keep the list in a safe place at home and update it regularly. You will need this list if your wallet or purse is ever lost or stolen. Never carry your Social Security Number in your wallet or purse. Also, never carry in your wallet any paper onto which you've jotted down PINs, passwords, or login information.

Click here to learn what to do if your wallet is lost or stolen. [usbank. com/pdf/online-security/security-lost-wallet.pdf]

3. Sign up for U.S. Bank Security Alerts

When you sign up for this free service from U.S. Bank, you'll receive automatic text messages or email alerts whenever U.S. Bank is given instructions for changes to your account, including:

- Address, email or phone number changes
- PIN number change
- Request for an additional or replacement ATM/check card or credit card
- And many more…
  Click Here to sign up now!
  [https://www.usbank.com/online-banking/text-email-alerts.html]

4. Go paperless

Click here to sign up for U.S. Bank's free Online Statements and Internet Bill Pay [Go to www.usbank.com/online-banking/bank-any-where.html, then click "Get Online Statements" from the list on the right.]

5. Monitor your paper statement, bills, and online accounts

Check the transactions listed on your bank statements, credit card bills, utility bills, and online accounts regularly for unauthorized transactions. If you spot something suspicious, report it immediately.

6. Only do business with companies you know and trust

When making online transactions, be sure the website uses secure encryption.

Click here to learn more about secure websites. [usbank.com/online-security/how-to-spot-fraud.html, then click "Fraudulent Websites"]

7. Protect your PC with up-to-date anti-virus software

Click here to learn more about protecting your computer from viruses and other malware. [usbank.com/online-security/fraud-prevention.html, then click "Protect Your Computer"]

8. Be cautious when sharing a computer

If you use a shared computer – such as a library or lab computer – or share a computer with roommates, log out and clear cookies after every computer session.

9. Password protect your electronics

Enable the password feature on your cellphone, laptop, Kindle, iPad, or any electronic devices that contain personal information about you – including, phone numbers, banking information – anything you don't want in the hands of strangers. If your pass-word-protected device is lost or stolen, your personal information is not immediately accessible to others.

Additionally, most devices have "remote wipe" capability that allows you to erase addresses, phone numbers, emails, photos and other sensitive content on a lost or stolen phone. Wiping a lost or stolen phone restores the device it to its factory settings. Refer to the manufacturer's website to learn specifics for your device.

10. Watch your U.S. Postal mail

Missing bills or statements may indicate someone is tampering with your mail or your identity.

Click here to learn more. [usbank.com/pdf/online-security/security-beyond-the-bank.pdf] To prevent mail fraud:

- Consider going paperless for your banking needs.
- If you will be away from home for 3 - 30 days, sign up for "Hold Mail Service." The Post Office has a forwarding service if you will be gone more than 30 days.
- Call the U.S. Postal Service at 800-275-8777 or submit a "Mail Hold" request online. [https://holdmail.usps.com/holdmail]