Security

Frequently-asked questions

Got questions? We have answers. From questions about identity theft and more, we have a list of questions and answers to guide you along.

Q: What is identity theft?

A: Identity theft is a criminal offense involving a person who knowingly transfers or uses, without lawful authority, another person's identification. It occurs when a criminal steals key pieces of personally identifying information, including a name, address, date of birth, Social Security number and mother's maiden name to gain access to a person's financial accounts. They may open new accounts, apply for loans and purchase expensive items—all in someone else's name.

Q: How do I protect myself from identity theft?

A: Never carry your Social Security card in your wallet or print it on your checks. Don't provide your SSN, bank account or credit cards information to anyone who contacts you by telephone. Report lost or stolen credit cards as soon as possible. Keep a photocopy list of all your credit cards, bank accounts and investments in a secure place so you can quickly contact these companies in case your credit cards are lost or stolen. Create strong, hard to guess passwords and don't use personally identifying information in your passwords. Never share your passwords or PIN numbers with anyone else and shred any credit card offers you receive in the mail.

Q: How do I protect myself from check fraud?

A: One of the first lines of defense against check fraud is you. Here are some tips to protect you from check fraud:

- Never respond to unsolicited requests for your checking account number, Social Security number or other financial information
- Never have your Social Security number or driver's license number printed on your checks
- Never leave your checkbook unattended
- Shred unused checks before disposal, even if they're from a closed account
- Notify your bank if you notice any discrepancies on your checks or you aren't receiving your statements
- Never write checks in pencil
- When mailing checks, use a security-lined envelope or wrap them in paper so they can't be read through the envelope
- Always spell out the name of the payee on the pay to line so that it cannot be altered. Never use abbreviations
- Check bank statements against your checkbook register regularly and report any discrepancies to your financial institution

Q: How do I protect myself when banking online?

A: Follow these tips when banking online to protect yourself against fraud:

- Carefully choose your password. Use a combination of letters and numbers and never use your name, address or telephone number
- Change your password frequently
- Never reveal your password to anyone, including your financial institutions. Northwest will never ask you for your password
- Don't leave your account on the screen when your computers is unattended. Log off before leaving your computer
- Always log off properly by using the exit instructions
- Don't send any personal or financial information by regular email, which is generally not encrypted
- Don't reply to any email that requests your personal account information
- Always be sure that you're using a secure browser connection when providing your personal account information online
- Consider installing anti-virus software on your computer to safeguard against known computer viruses. Northwest offers IBM Trusteer Rapport, online fraud protection software, to all our customers free of charge