

Fraud Prevention

Protecting Your Account and Identity

The best line of defense against fraud begins with you. The following list of valuable tips is presented to help you protect yourself. Working together, we'll ensure you enjoy a safe relationship with Wells Fargo and help you avoid falling victim to account fraud or identity theft.

Preventing account fraud

Protect your accounts. Never loan your credit or ATM card or share your passwords with anyone who is not authorized on your account. Do not share your account numbers with anyone unless you initiated the contact. Report lost or stolen checks or credit cards immediately. Review new checks to make sure none were stolen in transit. Be aware of the expiration date on your credit card; if you do not receive a reissued card before the expiration date, notify customer service.

Store new and cancelled checks securely and always use tamper-resistant checks. Wells Fargo checks include many safety features, such as tamper-resistant packaging and chemically sensitive paper to deter alterations. Question suspicious emails or phone inquiries. Unless you initiated the contact, Wells Fargo will not request your personal information (account number, Social Security number, or mother's maiden name) through email, U.S. mail, or by phone. Please notify us immediately if you receive odd calls or emails claiming to come from Wells Fargo. Be especially wary of those requesting account information to "award a prize" or "verify a statement."

Guard your ATM and online banking information. Avoid using obvious or easily

obtainable information as your password. Don't share your passwords with anyone or write them down. For more tips, read our Security FAQs. Curtail the use of paper documents. Your Wells Fargo Banker can discuss the many electronic payment options available, such as Bill Pay and free online account access with Wells Fargo Online®.

Preventing identity theft:

- Don't give out financial information online or on the phone unless you initiated the contact, and know the party you're dealing with.
- Shred unnecessary financial documents, including old bank statements, invoices, and unwanted pre-approved credit offers.
- Promptly retrieve incoming mail, and don't put outgoing mail in your residential mailbox.
- If regular bills or statements stop reaching you, take action. Call the company's customer service number. Someone may have filed a false change-of-address notice to divert your mail.
- Don't ignore suspicious charges. If doubtful or unauthorized charges appear on your bills or statements, call immediately to resolve the discrepancy.
- Keep personal numbers off your checks. Never preprint your driver's license or Social Security number on your checks.

Check your credit report:

As part of your ongoing vigilance against identity theft, Wells Fargo recommends that you periodically check your credit report. For a small fee, you can obtain a copy of your credit report at any time from one of the three major credit bureaus:

For additional information about account fraud and identity theft, you can refer to

www.consumer.gov/idtheft — the U.S. government's central Web site for information about identity theft.

Avoiding Identity Theft

According to the Federal Trade Commission, more than a half-million Americans will have their identities stolen this year.

Common types of identity theft are using or opening a credit-card account fraudulently; opening cell-phone or utility accounts fraudulently; and getting loans or working in another person's name.

Victims of identity theft spend an average of 175 hours and \$800 to clear their names.

Here are tips from the FTC on how to avoid identity theft:

- Scrutinize your credit-card and bank-account statements for any unauthorized activity.
- Call your credit-card company or bank if an account statement is late. A missing bill may mean someone impersonated you and changed the billing address.
- Do not give out personal information on the phone, through the mail, or online unless you initiate the contact or know the caller. Thieves often pose as bank representatives, Internet service providers, government agents, and the like to get you to reveal personal information.
- Shred any documents you are tossing out that contain personal information. These include credit-card receipts, insurance forms, physician and bank statements, and credit-card offers.
- Deposit outgoing mail directly into post office boxes, not in your own mailbox. If you are going on vacation,

place a hold on your mail at the post office.

- Do not carry your Social Security card with you, and give out your Social Security number only when absolutely necessary.
- Carry a minimum number of ID and credit cards with you.
- Cancel any credit cards you do not need or use.
- Do not print your Social Security or driver's license numbers on your checks.

Order a copy of your credit reports once a year to verify their accuracy.

If you are really worried, subscribe to a credit-watch program that sends regular updates on any credit activity done in your name.

Learn more about identity theft at:

www.consumer.gov/idtheft

Equifax: 800-685-1111 or

www.equifax.com

Experian: 888-397-3742 or

www.experian.com

TransUnion: 800-916-8800 or

www.transunion.com