WELLS FARGO

Fraud & Scam Solutions

What you need to know
and what to watch for

In 2024, scams became the **leading form of fraud**, surpassing digital payment fraud

The share of scam-related fraud increased by

56%

Source: PYMNTS, The State of Fraud and Financial Crime in the U.S. — November 2024.

Making your security a priority

At Wells Fargo, we are dedicated to keeping your accounts safe. In addition to proactive 24/7 fraud protection and transaction monitoring, we work to help you spot the warning signs of fraud and avoid common scams.

Here are actions and advice to help protect yourself and your family.

Scams on the rise

The growing role of AI in scams

Artificial intelligence (AI) is making it harder to know what's real and what's not. Scammers are now using AI to create fake voices, videos, and images that look realistic. They can use these fakes on social media, websites, in texts, and emails to trick you into thinking you're providing your information to someone you trust. Here are some tips to help stay safe:

- Pause before taking action. Be critical of requests and the source.
- Validate any request for information or money — ask a family member or friend for something only they would know.
- Don't engage with unexpected communications.

Elder fraud and scams

Many scams focus on older adults because they make up a large segment of the population and often have significant savings.

Common scams to watch for are investment opportunities, family emergencies, government imposter, and tech support scams. To help keep yourself and your loved ones safe:

- Don't rely on caller ID.
- Don't provide access to your device to anyone who contacts you.
- Keep social connections intact and consult a trusted family member or friend about new relationships or sketchy situations.
- Don't be pressured to move or send money by someone who contacts you claiming there is fraud on your account. A legitimate company will not ask you to do this.

Spot the red flags of a scam

Unexpected contact

A person or company contacts you out of the blue by phone, text, or email — often about fraud on your account or an order, delivery, invoice, or charge you didn't know about. They may insist on staying on the phone. Hang up.

Everything is urgent

Scammers will create a false sense of urgency and use pressure tactics like rude or pushy language to get you to act immediately.

Emotional, manipulative, or threatening situation

Scammers play on your emotions — fear, love, curiosity — to engage you and get you to pay or give up your sensitive information.

Unusual payment requests

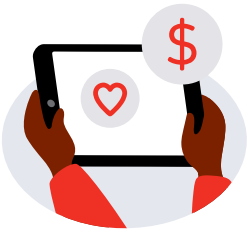
Scammers prefer payment methods that make it difficult or impossible to get your money back. Be cautious if anyone asks you to pay with gift or prepaid cards, cryptocurrency, wire transfers, or a payment app. These payment methods are like sending cash. Remember that requests for gift cards are almost always a scam.

Watch for common scams

The check scam

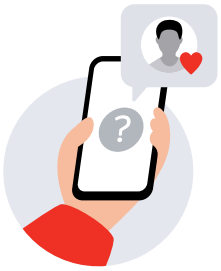
Be alert if anyone asks you to cash a check and send back a portion of the deposit. These checks are typically fraudulent and can take weeks to discover it's fake.

The romance scam



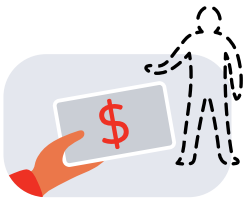
A new online love interest bombards you with sweet talk but doesn't meet you in person. Suddenly, they ask you to send them money for a guaranteed investment, hardship, or emergency.

The family member scam



Fraudsters play on your emotions by identifying themselves as a friend or family member calling or texting about an emergency. They may **use Artificial Intelligence (AI) to clone voices or images** to convince you it is someone you know.

The imposter scam



Scammers pose as Wells Fargo, the IRS, a utility, or other well-known organizations to convince you to provide your personal financial information. They may pressure you to wire money, withdraw cash, or use prepaid debit or gift cards to resolve an account issue or pay a fake bill.

Stay safe with these tips

Guard your information

Don't share your password, personal identification number (PIN), or one-time access codes. Scammers may pose as a Wells Fargo employee and ask you to share this private information because there is a "problem" with your account. Your account sign-on information should never be shared with anyone.

Don't rely on Caller ID

Scammers can imitate Caller ID so their phone calls appear legitimate.

Be cautious when sending money

Don't be pressured to send money without carefully verifying the request is legitimate and the information you've been given is accurate.

Never allow remote access to your computer

Scammers may contact you to offer a refund or help remove a virus. If you allow them access to your computer, you may be tricked into sending them money or sharing your sign-on information.

Avoid engaging

Don't click links, download attachments, or call phone numbers that come with unexpected communications.

Contact us directly

When in doubt, hang up or don't respond. Instead, contact us using the phone number on the back of your card or from wellsfargo.com. You can also contact us using the Wells Fargo Mobile® app[1].

Take action

Visit the Security Center in our mobile app

See where your account security stands and quickly check and add extra features to help protect your accounts. You can also visit the Security Center online at wellsfargo.com/security.

Activate account alerts[2]

Push notification, email, and text alerts are an easy way to be notified whenever there is activity on your account, so you can contact us quickly if something doesn't look right.

Add enhanced security options

Consider using two-step verification, mobile biometrics, a passkey, or voice recognition. These services help us know it's you.

Watch for changes to your credit report

Enroll in Credit Close-Up® to get credit monitoring alerts, view your Experian® credit report, and more, to help spot identity theft.[3]

Get access to the Security Center and more with the Wells Fargo Mobile® app

Scan the QR code with your device's camera, or visit us online at wellsfargo.com/mobile-online-banking/apps/ or your app store.

1. Availability may be affected by your mobile carrier's coverage area. Your mobile carrier's message and data rates may apply.
2. Sign-up may be required. Availability may be affected by your mobile carrier's coverage area. Your mobile carrier's message and data rates may apply.
3. You must be a Wells Fargo account holder of an eligible Wells Fargo consumer account with a FICO® Score available, and enrolled in Wells Fargo Online. Eligible Wells Fargo consumer accounts include deposit, loan, and credit accounts, but other consumer accounts may also be eligible. Contact Wells Fargo for details. Availability may be affected by your mobile carrier's coverage area. Your mobile carrier's message and data rates may apply.

   Please note that the score provided under this service is for educational purposes and may not be the score used by Wells Fargo to make credit decisions. Wells Fargo looks at many factors to determine your credit options; therefore, a specific FICO® Score or Wells Fargo credit rating does not guarantee a specific loan rate, approval of a loan, or an upgrade on a credit card.

   Wells Fargo and Fair Isaac are not credit repair organizations as defined under federal and state law, including the Credit Repair Organizations Act. Wells Fargo and Fair Isaac don't provide credit repair services or advice or assistance with rebuilding or improving your credit record, credit history, or credit rating.

We're here to help

Contact us right away if you've experienced fraud, identity theft, or a scam, and notify the police and the Federal Trade Commission (FTC) for additional support and reporting.

- Lost or stolen cards or checks.
- Suspicious or unauthorized purchases, withdrawals, or transactions.
- Identity theft.

We accept all relay calls, including 711.

Personal accounts	Business accounts	Credit cards
1-800-869-3557	1-800-225-5935	1-800-642-4720

If you have experienced unauthorized profile changes, suspicious activity, or fraud using services provided by Wells Fargo Online® or in the Wells Fargo Mobile® app[1], please contact us at 1-866-867-5568.

Help us fight Wells Fargo impersonators

Phishing emails or texts

- If you clicked a suspicious link, opened an attachment, or provided one-time access codes or any personal account information, call right away, 1-866-867-5568.
- If you did not respond, forward the suspicious email/text message to reportphish@wellsfargo.com.[2]

Suspicious phone calls

- If you received a call, sent a payment, provided one-time access codes, or personal account information to someone claiming to be from Wells Fargo, call us immediately at 1-800-869-3557.

Elder fraud

If you or an older or dependent person have experienced suspicious activity or fraud, call us right away at 1-800-869-3557, or speak with a branch employee.

You can also call the **National Elder Fraud Hotline** at 1-833-FRAUD-11 (1-833-372-8311).

To learn more visit us at wellsfargo.com/scams

1. Availability may be affected by your mobile carrier's coverage area. Your mobile carrier's message and data rates may apply.
2. Please note that due to technical reasons, some email messages forwarded to reportphish@wellsfargo.com may be rejected by our server. If this occurs, please delete the suspicious email or text message. Wells Fargo regularly works to detect fraudulent emails and websites. Thank you for taking steps to protect your personal and financial information.