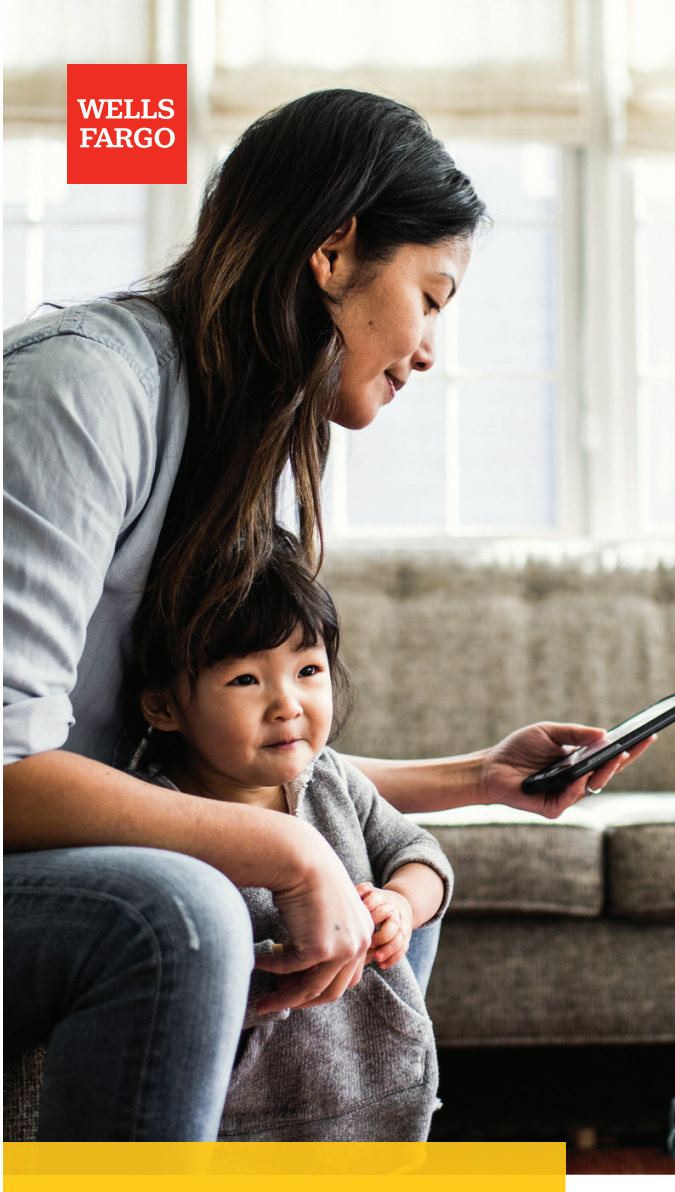
Where to visit us

- In person at a Wells Fargo branch
- Online at **wellsfargo.com/fraud**
- On the *Wells Fargo Mobile®* app – available for download in the app store

How to report fraud

Contact us immediately if your Wells Fargo account may have been compromised or you suspect fraud.

Type of fraud	Phone number
ATM, debit card, or checking fraud • Suspicious or unauthorized ATM or debit card purchases or withdrawals • Lost or stolen debit card, ATM card, or checks • Lost or stolen account numbers	1-800-869-3557
Credit card fraud • Suspicious or unauthorized credit card transactions • Lost or stolen credit card	1-800-642-4720
***Wells Fargo Online®* services fraud** Suspicious or unauthorized activity with a Wells Fargo service: • Bill Pay • Online transfers • Zelle® • Online wires • Online profile changes	1-866-867-5568
Suspicious phishing email or text messages If you receive a suspicious email or text message and you: • **Did** respond by clicking on a link, opening an attachment, or providing sensitive information, call us immediately. • **Did not** respond, forward the suspicious email to **reportphish@wellsfargo.com**.	1-866-867-5568
Suspicious phone call If you receive a suspicious phone call from someone claiming to be from Wells Fargo, and you shared sensitive information, call us immediately.	1-800-869-3557
Identity theft If you are a victim of identity theft, visit **identitytheft.gov** for more information.	1-800-869-3557
Hearing-impaired customers • 24 hours a day, 7 days a week • Telecommunications Relay Service calls accepted	TDD/TTY: 1-800-877-4833



We're helping you stay on top of your account security

Learn how to protect yourself

Wells Fargo is consistently enhancing our security measures, including 24/7 fraud monitoring. We may send a text or call if we notice unusual activity on your card. We also provide customers with helpful tips and a variety of security options so you can choose what works best for you.

Follow these safety tips

- **Secure your sign-on.** Use a long password with at least one letter and one number. The longer the password, the harder it is to crack. Consider using an uncommon phrase that's memorable to you, but not others. You can also set up 2-Step Verification at Sign-On for an extra layer of protection.
- **Be wise about Wi-Fi.** Don't access your financial accounts through public Wi-Fi networks, such as those available in coffee shops or airports.
- **Avoid phishing emails and text messages.** Don't click on links, open attachments, or provide sensitive information — including your access code — through a suspicious-looking email or text message.
- **Track your funds.** Set up alerts[1] for ATM withdrawals and card activity, and if you spot suspicious charges, report them immediately.
- **Pause before you post.** Don't overshare on social media, especially information used by your bank or other companies to verify your identity. Also review the privacy settings for your social media accounts.
- **Is it Wells Fargo on the line?** Watch out for scammers who spoof their number or caller ID so the call appears to be from Wells Fargo. When in doubt, hang up and call us using the number on the back of your card.

For more fraud prevention tips, visit **wellsfargo.com/fraudtips**.

Spot common scams

Scams can take many forms. Don't be fooled by scammers who impersonate your bank or other companies to convince you to divulge your personal and account information. When in doubt, don't respond. Read up on three common schemes:

- **Phishing scams** – Phishing is usually a two-part scam involving an email, text message, or social media post containing links to a fraudulent website requesting sensitive information such as username, password, and account details. The scammer typically pretends to be a reputable company, using compelling language to gain your trust or scare you into sharing your information. Once obtained, your personal and financial information can be used to access your account and steal money.
- **Tech support scams** – These scams may originate from an unexpected call or pop-up message on your computer warning of an issue, such as a virus or other malware. The caller or pop-up claims to be from tech support and requests remote access to your computer to resolve the issue. Once they have control of your computer, the scammer may require payment for technical assistance, install malicious software, change settings to leave your computer vulnerable, or ask you to log in to online banking to gain access to your bank account.
- **Bank imposter scams** – In this scheme, a scammer calls unsuspecting customers posing as a bank representative. The reason for the call is typically suspicious activity detected on your account. The caller may ask you to verify your identity by providing your login information, Social Security number, Personal Identification Number (PIN), or access code. If you provide this information, you may be giving the scammer the keys to your account to commit fraud.

Explore the Security Center

The Security Center at **wellsfargo.com/fraud** is a one-stop shop for fraud prevention and security resources. Get the latest on trending scams and security options, and test your knowledge with our cybersecurity quiz.

And when you're ready to customize your security features, sign on to the *Wells Fargo Mobile®* app[2] to activate fingerprint or facial recognition, set up alerts,[1] and turn on 2-Step Verification at Sign-On.

[1] 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.

[2] Availability may be affected by your mobile carrier's coverage area. Your mobile carrier's message and data rates may apply.