Have more questions?

Visit us

Visit your local Wells Fargo retail banking store

Make an appointment online to meet with a banker at **wellsfargo.com/appointments**

Call us

Telecommunications Relay Services accepted

Customer service for existing accounts:
1-800-225-5935 24 hours a day

Go online

For more information on how to prevent fraud, go to **wellsfargo.com/fraud**

For more educational information and resources, go to **wellsfargoworks.com**

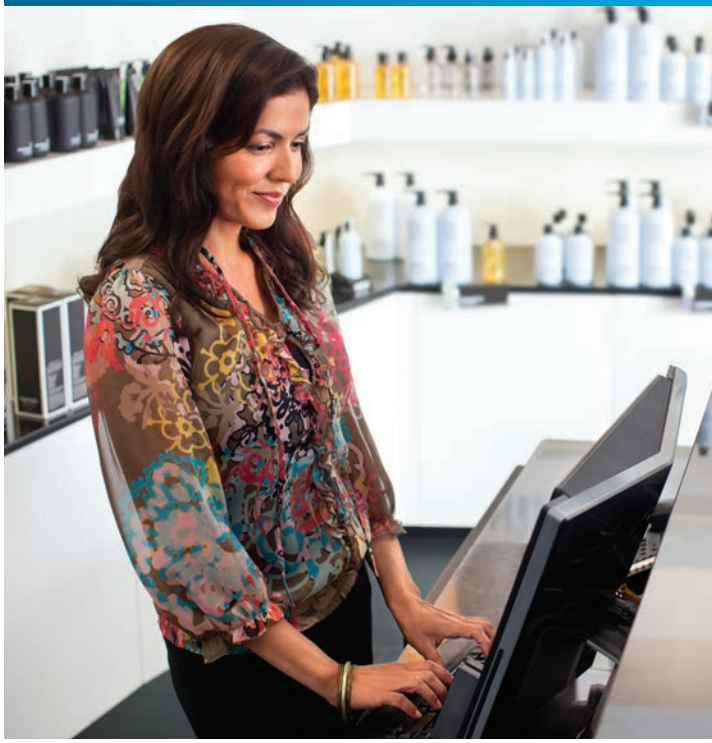
The information provided in this brochure is for your consideration and is not legal advice. Please consult with your own technology and legal advisors before taking action based on this information.

BBG2922 (02/17) ECG-3551502

Wells FargoWorks *for Small Business*

WELLS FARGO

Helping you protect your business from fraud



Together we'll go far

Safeguard your banking accounts

Guard your account information

- Only share your account information if you initiate the contact using legitimate sources of information, such as the telephone number on account statements or on the back of your business credit or debit card
- Be especially wary of calls, emails, or pop-up windows requesting account information to "award a prize," "verify a statement," or for any other reason

Monitor your accounts for unusual or suspicious activity

- Review your transaction activity for unexpected fluctuations. For example, compare the percentage of cash deposits to total deposit size. Most businesses will maintain a constant average. A large fluctuation might indicate embezzlement.
- Watch for checks cashed out of sequence and checks made out to cash. These could be red flags for embezzlement.
- Notify Wells Fargo immediately if you notice any unauthorized activity on your accounts or if you do not receive your statement on time

Separate employee responsibilities

- Assign two different individuals to be responsible for reconciling statements on your account(s). They should be different from the individual who issues checks.
- Require that an owner opens statements. If fraud exists, those responsible often try to hide their activities by intercepting any mail that might reveal them.
- Notify Wells Fargo immediately when an employee who was authorized to transact business on your account(s) leaves your company, so his or her name can be removed from all signature cards and business online banking access

Keep checks secure

- Store your check supply under lock and key. Secure your working supply when not in use. Stolen checks are a common method of embezzlement.
- Destroy any checks that you do not intend to use
- Never sign blank checks
- Notify Wells Fargo immediately if any unused checks are missing, you discover your checks have been stolen, or you find a discrepancy in your records

Help protect yourself and your business from online fraud

Maximize online and mobile security

Keep these tips in mind:

- **Secure your sign on.** Use a unique username and password for your Wells Fargo accounts, update them regularly, and do not use any part of your email address as your username or password.
- **Protect your PIN.** Cover the keypad when entering your Personal Identification Number (PIN) at an ATM, grocery store, or other location.
- **Be wise about Wi-Fi.** Do not access your financial accounts through public Wi-Fi networks, such as those in a coffee shop or library.
- **Stay current.** Keep the operating system, anti-virus software, and security patches up to date on all your devices.
- **Avoid phishing emails.** Do not click on links, open attachments, or provide sensitive information through a suspicious-looking email or text message.
- **Keep it clean.** Delete text messages from financial institutions before loaning out your device. Use the device's "wipe" feature to clear out personal information when selling or discarding the device.
- **Set up alerts.** Set up account alerts so you will be notified of withdrawals and deposits to your account, as well as any suspicious card activity. Report suspicious activity as soon as it is detected.
- **Pause before you post.** Do not overshare on social media by providing information used by your bank or other companies to verify your identity. Also review the privacy settings for your social media accounts.
- **Secure your data.** If you use a cloud-based service or website to store financial documents, ensure that the site has security features such as required log-in and data encryption denoted by "https" in the address bar.
- **Stay ahead of scammers.** If you are uncomfortable with a phone call you did not initiate or if the caller requests access to your computer, hang up and contact the company using legitimate sources such as a phone number on the company's website.

To learn more about phishing and other scams, visit **wellsfargo.com/scams**

How to report fraud for small business

Contact us immediately using the following numbers if you think one of your Wells Fargo accounts may have been compromised or you suspect fraud.

Type of fraud	Contact information
ATM, Checking, or Debit/Credit Card fraud	**1-800-225-5935**
***Wells Fargo Online*® services fraud** Suspicious or unauthorized activity with a Wells Fargo service: • Online wires • Bill Pay • Online transfers • Online profile changes	**1-866-867-5568**
Suspicious phishing emails or text messages If you receive a suspicious email or text message and you: • *Did* respond by clicking a link, opening an attachment, or providing personal information, call us immediately • *Did not* respond, forward the email to us at **reportphish@wellsfargo.com**	**1-866-867-5568**