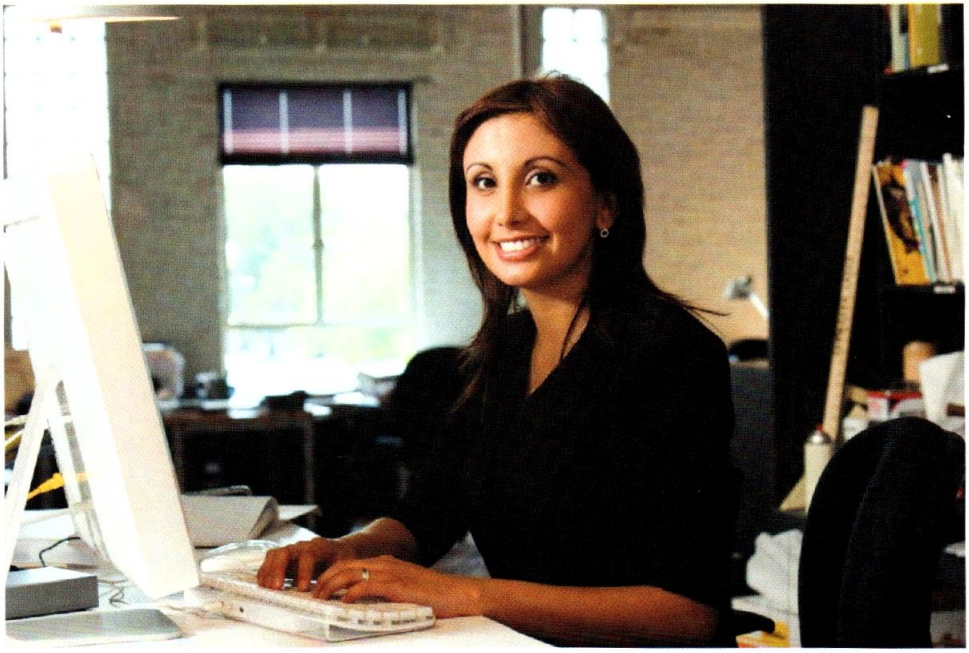
WELLS FARGO

Protecting your business from fraud



Together we'll go far

Safeguarding your business

For more than 150 years, Wells Fargo has been dedicated to customer safety and protection, and our mission remains as strong as ever. We continue to make improvements in security to protect you and your business.

When you come to our stores, call the Wells Fargo National Business Banking Center, or visit us online at wellsfargo.com/biz, we follow certain procedures to protect you. We may:

- Ask you to provide additional identification.
- Ask for verification when we receive an address change request.
- Impose holds on deposited checks.

Our policy allows only for validation of account numbers. We will not verify customer funds for a third party over the phone.

The following tips are presented to help you protect your business.

Prevent fraud by limiting your use of paper

Almost 85% of identity theft cases start with stolen paper statements, bills or checks.[1] Consider online alternatives available through *Wells Fargo Business Online*® to minimize the use of paper that includes sensitive information.

You can receive electronic versions of your bank account statements, credit card statements and checks.

Manage your accounts online, anytime

Regular account review helps to quickly detect and stop fraudulent activity. With Wells Fargo Business Online you can monitor your account online any time and as frequently as you like.

Key features include:

- **Online Statements –** View and download online statements, eliminating the need to have them mailed, ensuring rapid delivery, and reducing the potential of statements being stolen from an unlocked mailbox. If printing statements, be sure to store them in a locked and secure location.
- **Check Images –** Access copies of most checks online soon after they post to your account, eliminating the need to have them mailed and reducing the risk of stolen mail, which could have sensitive information printed on it.
- **Alerts** – Monitor your accounts using customizable email alerts, which update you on account transactions that are important to you. Receive notifications on deposits, withdrawals, posted checks, credit card transactions and more, so you are quickly alerted to any suspicious transactions.
- **Transfers –** Transfer money quickly and securely between your Wells Fargo accounts or to other Wells Fargo customer accounts. PIN

authorization is required for certain transfers, making these transactions even more secure.

- **Payments** – Make a wide variety of business payments through the *Wells Fargo Online Payment Suite*® – pay bills and business taxes, make next-day payments to employees and vendors, and send payments in over 100 foreign currencies.[2]

Protect your business against fraud

Never give out your account information unless you initiate the contact using legitimate sources of contact information, such as the telephone number on account statements or on the back of your credit or debit card.

- Notify Wells Fargo immediately if you receive a suspicious request to verify your identity or provide sensitive information.
- Be especially wary of calls, emails or pop-up windows on your computer requesting account information to "award a prize," "verify a statement" or for any other reason.

If you encounter a suspicious email or website that says it's from Wells Fargo, do not respond to it or provide any personal or account information.

Monitor your account 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.
- Require an owner to periodically perform accounting duties, such as reconciling your account or making a deposit. This will often deter embezzlers.

- View your account balance, returned items, and Overdraft Protection status with an alert section on the top of the page.

Separate bank account 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, the wrongdoer often tries to hide fraudulent activities by intercepting any mail that might reveal his/her activities.
- Notify Wells Fargo immediately when an employee who was authorized to transact business on your account(s) leaves your company, so his/her name can be removed from all signature cards and business online banking access.

Review and reconcile statements as you receive them

- Notify Wells Fargo immediately if you notice any unauthorized activity on your account.
- Contact Wells Fargo immediately if you do not receive your statement when you would normally expect to.

Ensure the highest level of print security features by using Wells Fargo authorized check printers

Examples of check security features include:

- Safety stain to indicate chemical tampering.
- Microprint (MP) lines printed on the front and back of the check.
- Padlock icon directs readers to the back for a checklist that outlines the security features of the check.
- Security screen on the back of each original document displays an "ORIGINAL DOCUMENT" screen that prevents reproduction copying and helps prevent erasure of information.
- Color signal paper shows small colored marks when solvent alteration is attempted.

If using computer checks, request one of our enhanced-security check stocks.

Keep checks and other confidential banking information 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.

Protect yourself and your business from online fraud

Bank online with confidence

With *Wells Fargo Business Online*, we guarantee that you will be covered for 100% of funds removed from your Wells Fargo accounts in the unlikely event that someone you haven't authorized removes those funds through our Online Services. For details on the Wells Fargo Online Security Guarantee, please visit our website at wellsfargo.com/privacy_security/online/guarantee. You are responsible for keeping your online password, account numbers, personal identification information and other account data confidential.

Maximize online security

Online banking can reduce exposure to certain types of fraud. Keep these tips in mind when banking online:

- Change your Wells Fargo Business Online password periodically and never disclose it to anyone. Create passwords using a combination of numbers, letters and special characters.
- Do not leave your computer unattended while you are accessing your accounts. Sign off when you have finished your online banking.

Note: Wells Fargo's security system automatically times out your computer after 10 minutes of inactivity.

- Install anti-virus software on your computer and keep it updated.
- Use a current version of your computer's operating system to ensure virus definitions are up to date.
- Install a firewall on your computer.

Avoid fraudulent websites

Phishing, a type of online fraud, is usually a two-part scam involving emails and websites that spoof a legitimate company and try to convince you to share your personal or account information.

To learn more about phishing emails, visit wellsfargo.com/privacy_security/fraud/operate/recognize.

For additional protection:

- Make sure any internet purchase activity you engage in is secured with encryption. Look for "secure transaction" symbols, like a lock symbol in the lower right-hand corner of your web browser window, or "https://..." in the address bar of the website. The "s"

Report or forward suspicious emails that claim to be from Wells Fargo to reportphish@wellsfargo.com and then delete them.

indicates "secured" and means the web page uses encryption.

- Conduct online banking activities on secure computers only. Public computers (computers at internet cafes, copy centers, etc.) should be used with caution, due to shared use and possible tampering. Online banking activities and viewing or downloading sensitive documents (statements, etc.) should only be conducted on a computer you know to be safe and secure.

Prevent online scams

Notify Wells Fargo immediately if you are involved in a situation that fits one of the following descriptions, as it could be a scam:

- You are selling an item online and the amount of a check written to you is for more than the selling price of the item.
- The check written to you is drawn on a business or individual different from the person buying your item or product.

For more online security tips, go to wellsfargo.com/biz/education to view our Protecting Your Business video or the Strategies & Solutions For Your Business® publication, Online Security Savvy edition.

Identity Theft Protection

Identity Theft Protection, a comprehensive service provided by Trilegiant Corporation, helps customers stay informed about their credit information to minimize their risk of becoming victims of identity theft, and offers support if identity theft occurs. Identity Theft Protection provides daily credit monitoring through the three major credit reporting agencies, helping to safeguard customers against criminal attempts to steal their identities.*

To learn more, go to:
wellsfargo.com/insurance
or call 1-888-877-1605

*Identity Theft Protection is:

Not provided by Wells Fargo Bank
Not a deposit of or guaranteed by the bank
Not insured by the FDIC or any federal government agency

The best line of defense begins with you.

- Do not sign blank checks.
- Consider using electronic payment options such as Business Bill Pay and real-time online transfers.
- 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.

Safeguard your Wells Fargo Business Debit Card

- Sign the back of your card as soon as you receive it.
- Memorize your Personal Identification Number (PIN) and never share it with anyone, including bank personnel.
- Never allow anyone else to use, borrow or obtain your card and/or PIN. The account owner will be responsible for all transactions made by anyone to whom the account owner gives the card and/or PIN.
- Shield your entry from view of others when you type in your PIN at an ATM or other device.
- If your card is lost or stolen or no longer secure, immediately notify us at 1-800-CALL WELLS (1-800-225-5935).

Your Business Debit Card comes with important security benefits at no cost to you.

- Business owners have zero liability for unauthorized transactions as long as they are reported promptly and the business maintains appropriate internal controls against card misuse. For more information about liability for unauthorized transactions, please refer to the Wells Fargo Business Account Agreement.

[1]Javelin Strategy & Research, 2007 & 2008.

[2]Fees may apply. Visit wellsfargo.com/biz, or talk to your banker for details.

How can we help?

Visit us

Visit one of our banking locations to learn about Wells Fargo products and services

1-800-869-3557

Call and talk to one of our knowledgeable bankers 24/7

wellsfargo.com/biz