WELLS FARGO

Account takeover fraud and impostor fraud: Protect your company's accounts

What can you do to protect your company and its accounts from fraud? Be vigilant and aware of serious fraud threats, which include account takeover fraud and impostor fraud. Here's more information about both.

	Account takeover fraud	Impostor fraud
What it is	A fraudster obtains confidential information — including user IDs, passwords, PINs, and token codes — and uses them to access your accounts and transfer money or commit other fraudulent acts.	A fraudster poses as a person or entity you know and trust — an executive of your company, a vendor, even the IRS — and requests a payment or a change to vendor payment instructions. Impostor fraud is different from a fraudster stealing online banking credentials and using them to make fraudulent payments. With impostor fraud, your organization's authorized users make the payments, so they look like normal payments to your bank. If you fall for the scam, any payments you send go the fraudster instead of where you intended.
How it's perpetrated	Account takeover fraud is facilitated by: **Social engineering** • You or your employees are manipulated into performing actions for or divulging confidential information to someone impersonating a trustworthy entity. • It occurs by email (phishing or spear phishing), text message (smishing), or voice (vishing). **Malware** • Malicious software is installed on a computer or mobile device without a user's consent. • The malware records keystrokes and screen shots, redirects the browser, and displays fake web pages. • Malware carriers include: – Infected documents attached to emails. – Links in emails connected to an infected site. – Infected search engine results and documents. – Videos, photos, and banner ads posted on legitimate sites — particularly social networking sites.	There are two primary variations of impostor fraud: **Executive impostor** • A fraudster posing as an executive of your company, such as the controller or chief executive officer, instructs you to make one or more payments outside of normal channels — usually by wire. The impostor may tell you to keep the payments confidential. **Vendor impostor** • A fraudster posing as a vendor requests that you change the vendor's payment instructions — the bank name, routing/transit number, or account number. • An employee of your company or a vendor company copies or scans a real vendor invoice and creates a counterfeit invoice from it, directing the payment to their own account. • A hacker breaches your email system and studies the pattern of payment requests received by your accounts payable department. The hacker then submits a fraudulent invoice that looks legitimate except for subtle changes to payment instructions or, posing as a representative of your company, instructs your trading partners to direct payments to an alternate account.

Together we'll go far

	Account takeover fraud	Impostor fraud
How you can protect against it	• Implement dual custody — and use it properly. – Require that all payments, account number, or user modifications initiated by one user be approved by a second user on a different device. – For dual custody to work as intended, both the wire initiator and the approver must pay close attention to the details — not just give them a rubber stamp. The best practice for initiators and approvers: Verify before you initiate. Verify before you approve. • Update all your antivirus programs. • Be cautious of unexpected token prompts or on-screen messaging within your *Commercial Electronic Office®* (*CEO®*) portal session. The *CEO* portal doesn't prompt for a token during sign-on. – Users are prompted for a token only when attempting to access high-risk payment services (such as Wires, ACH, Foreign Exchange) and when accessing administrative functions within the *CEO* portal. – If you receive a request to enter your token code at any other point during your *CEO* portal session, contact your Treasury Management representative immediately. • Never give out your online banking access credentials. Instruct employees to follow the same rule. • Don't click on links in emails or text messages, and don't download attachments or install programs unless you're certain they're from a trusted sender. • Be wary of unsolicited phone calls from individuals who identify themselves as Wells Fargo employees calling to help you with unreported system issues. If you receive a call like this, do not follow the caller's instructions. Immediately contact your Wells Fargo bank representative. • Monitor online accounts daily to detect suspicious activity. Use notification and alert services to receive text or email notifications informing you of electronic debits from your accounts.	• **Verify all requests.** Set a policy to authenticate *all* requests that are by email, from outside normal channels, for new accounts, or to new countries, and that ask to change bank account information. Use the contact information you have on file to verify the requestor. Never use the contact information that comes with the request — it's fraudulent, too. • **Educate your staff and business partners.** Anyone at your company — and the companies with which you do business — can be a target. This includes executives and managers, your accounts payable staff, any departments that communicate with your vendors, and your trading partners. • **Make sure your organization uses proper fraud-fighting controls.** Internal controls include using dual custody properly, monitoring your accounts daily, and verifying unusual payment or account change requests. But these measures alone will not protect your assets.

What to do if you suspect fraud

Immediately contact your Wells Fargo representative and tell them you suspect fraud, or call 1-800-AT-WELLS.