WELLS FARGO

Fraud Protection Best Practices

Impostor fraud: Do you know whom you're paying?

Impostor fraud is on the rise, with companies worldwide reporting billions of dollars in losses. To protect your accounts, put a strong verification process and best practices in place.

What is impostor fraud?

Impostor fraud involves a fraudster posing as a person or entity you know and trust — an executive of your company, a vendor, even the IRS. The impostor contacts you by phone, email, fax, or mail and submits an invoice or requests a payment or a change to vendor payment instructions. If you fall for the scam, any payments you send go to the fraudster instead of where you intended.

This is very 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. This typically means the fraudis not quickly identified, which makes it harder to recover the funds, particularly if they're sent by wire.

There are several ways impostor fraud is perpetrated:

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.
- A hacker breaches your vendor's accounts receivable system and generates a fraudulent invoice or payment request from it.

Best practices to help reduce your risk

Alert your staff — especially your management team and accounts payable department — to the threat of impostor fraud. Apply these best practices to reduce your organization's risk:

Verify the requestor

Set a policy requiring all requests for unusual payments made outside normal channels and for changes to vendor remittance information to be verified. If the request came by mail, fax, or email, verify it with a phone call. If the request came by phone, verify it by email.

Always use the contact information you have on file to verify the requestor — the officer's phone number in the company directory or the vendor contact in the master file. Never use the contact information that comes with the request — it's fraudulent, too.

Use dual custody

Dual custody gives you a second chance to spot a payment as fraudulent before it goes out the door. But, for dual custody to work as intended, both the wire initiator and approver must pay close attention to the wire details — not just give them a rubber stamp. The best practice for initiators and approvers is: Verify before you initiate. Verify before you approve.

Monitor account activity

Impostor fraud is one more good reason to reconcile your accounts daily. If you spot an unauthorized transaction or unusual activity, immediately contact your dedicated client services officer or call 1-800-AT-WELLS.

For more information, contact your treasury management representative.

Wires best practices

Verify all account change requests

Use the contact information you have on file, not what is contained within the email