WELLS FARGO

Treasury Management

Impostor fraud protection checklist

Don't become an impostor fraud victim.

Impostor fraud, also known as business email compromise (BEC), occurs when a criminal impersonates someone you know and trust such as a vendor, executive, or the IRS. The impostor contacts you by phone, email, fax, or postal mail and submits an invoice or requests a payment or a change to vendor payment instructions. This results in your payment going to the fraudster rather than where you intended. Unlike other types of fraud, impostor fraud is difficult to detect because the transactions made on your account are consistent with regular payments and are made by authorized personnel. Always verify sensitive requests using this checklist to help ensure you don't miss an important step.

Use this checklist to reduce your risk of impostor fraud.

☐ **Check for red flags.** Red flags include, but aren't limited to:

- High degree of urgency
- Request to keep the payment confidential
- Switching from a commercial beneficiary to an individual beneficiary
- Request to change payment instructions such as bank details or payment types
- Changing from an organization's email domain to a public email domain, such as gmail
- Subtle changes to the organization's name in the email address
- Requests containing typos, spelling errors or poor grammar
- Payment amount doesn't match the invoice or request
- Beneficiary's name, mailing address, or account number don't match the information you have on file.
- Request for change where bank and beneficiary are not located in the same geographic region or country.

☐ **Verbally verify all payment requests and requests for changes to payment instructions** - such as account and routing transit numbers, payment type, amount, financial institution, mailing address, and other key details using a different communication channel than the one used by the requestor.

- Always use the contact information you have on file to verify requests. Remember, you can't safely use the contact information found in a payment request or payment change request since it could be fraudulent.
- If you're making a large payment, you should use multiple communication methods to double and triple check the validity of the payment requests and payment change requests.

☐ **Use dual custody as it's intended to be used** - no rubber stamp approvals.

- Dual custody gives you a second chance to spot a fraudulent payment before it goes out the door. Both the payment initiator and approver must pay close attention to the payment details.
  - **Initiator** - Verify before you initiate, using this checklist to ensure you review each of the key details.
  - Approver - Verify before you approve. Do not trust the initiator's verification or assume the payment is appropriate because you recognize part of the beneficiary's information.

Additional tips to help protect yourself and your organization.

- Monitor account activity - if you reconcile your accounts daily, it increases your chances of catching a fraudulent payment and stopping it before funds are sent. It also enables you to detect anything out of the ordinary.
- Protect your email account and your devices - never give your login credentials to anyone, especially online or over the phone.

Laura Hylton <lhylton@lpsd.com>

Impostor fraud remains a major threat

1 message

Wells Fargo Digital Solutions <WellsFargoDigitalSolutions@mail1.wellsfargo.com> Thu, Sep 12, 2024 at 11:02 AM
Reply-To: Wells Fargo Treasury Services <reply-fec1167472660375-2074_HTML-505233-7277748-25@wellsfargo.com>
To: lhylton@lpsd.com

Take steps to limit your impostor fraud risk

We'd like to remind you to remain vigilant and apply the appropriate safeguards to help prevent fraudsters from taking advantage of your organization.

According to a recent Association for Financial Professionals (AFP) survey, **80% of organizations were targets of payments fraud activity in 2023 – an increase from 65% in 2022.**
Source: AFP: 2024 Payments Fraud and Control Survey[1]

How it works

In impostor fraud, or business email compromise, a fraudster poses as a person (or entity) you know and trust. This could be an executive in your organization or a vendor.

- **Step 1.** The fraudster gains access to your trusted contact's email or instant message (IM) account. Or they may spoof the contact's information.
- **Step 2.** The fraudster impersonates your contact and sends you a request for a payment or a payment instruction change.

Keep in mind fraudsters may use phone, text, or other communication methods as well.

How to protect yourself

- Never send funds or change payment instructions based on an email, IM, or any other single form of communication. Always verify payment-related requests and use a different communication method than the one the requestor used.
- Verify email or IM instructions by making a phone call to the requestor using a phone number you already have on file for them. Don't use contact information that is included with the request to ensure you don't verify with the impostor inadvertently.
- Implement dual custody to serve as a second chance to identify potential fraud. Verify before initiating and verify before approving – on separate devices.

Use the impostor fraud checklist for every payment

Fraudsters make requests for payment and changes to payment instructions seem urgent, so you'll feel pressure to act quickly without verifying them. Always verify sensitive requests using this checklist to help ensure you don't miss an important step. Download the impostor checklist (PDF) for quick access.

Questions

For more information, visit our Treasury Insights Fraud & Security page.

If you have questions, contact your client service officer directly or call Global Treasury Management Service.

- **From the U.S. or Canada:** Dial **1-800-AT-WELLS** (**1-800-289-3557**).
- **From Mexico:** Dial 001-800-289-3557.
- **From other countries:** Dial the country's international prefix (00 for most countries) + 800-0289-3557 (00-800-0289-3557).

Note: We'll share this message with you in the "Service Updates" section of the Message Center. You'll need to sign on to view the message.

Thank you. We appreciate your business.

Anil Khilnani
Fraud Prevention Consultant
Global Treasury Management

Please do not reply to this message. To have your questions answered as quickly as possible, contact us using the information provided above.

[1]Wells Fargo has provided this link for your convenience but does not control or endorse the website and is not responsible for the products, services, content, links, privacy policy, or security policy of the website.

Privacy, Cookies, Security & Legal (https://www.wellsfargo.com/privacy-security/)

420 Montgomery Street, San Francisco, CA 94104

W5193-33 IHA7926602

WELLS FARGO

Take steps to protect your company from check fraud

You play a key role in fighting the threat of check fraud at your company by implementing recommended bank services and ensuring that internal procedures are in place to protect your assets and bank accounts.

Task	Steps to perform
Review account activity daily	Perform a daily review of your accounts (transactions and balances) to help you detect unusual or suspect activity in a timely manner.
Manage issued checks	Keep check registers, both internal and positive pay files, at the bank and update them daily, including intraday.
Reconcile accounts in a timely manner	• Ensure all transactions are authorized. • Report any unauthorized ACH transactions immediately so that return entries for non-consumer transactions can be made available by the opening of business on the second banking day following the settlement date of the original ACH entry. • Identify errors (including fraud) and report them within 30 days of the statement mail date. • Compare the payee name on checks with the payee names listed on your check register.
Segregate duties	• Assign check writing and reconcilement functions to different individuals. • Implement dual control for ARP Register Maintenance and Positive Pay exception review. • Rotate personnel in financially sensitive assignments. • Limit the number of authorized signers and require more than one signature on high-dollar checks.
Use separate accounts	Separate accounts to allow for more timely and focused review of payment activity, such as: • By payment type (check payments, ACH, wire transfers, etc.). • By purpose (accounts payable, taxes, payroll, etc.).
Control check stock	Store all check stock, deposit slips, check-writing equipment, and other banking documents in a locked space and: • Limit access to authorized personnel. • Minimize personnel responsible for handling or ordering check stock and rotate them periodically. • Change the locks when authorized personnel leave the company. • Conduct regular inventory of check stock. • Shred unused or outdated check stock. • Mail checks immediately after signing.
Secure deposited checks	Ensure that checks deposited electronically (remote deposit capture) are stored securely and destroyed properly.
Conduct surprise audits	Perform unscheduled audits; this often deters employees from committing fraudulent activities. Most embezzlers only commit fraud when they think they will not be caught.
Know your vendors	• Require that all changes to vendor payment account numbers are made in writing and on the vendor's letterhead, and verify the changes with a follow-up call to the vendor's telephone number that you have in your files. • Secure all Accounts Payable records and addresses from tampering. • Reconcile vendor payments to their paid invoices or outstanding balance.
Know your employees	Perform credit and background checks on employees who have access to accounts, account records, and cash. Call at least three references to verify information.

Task	Steps to perform
Protect access credentials	Ensure that your employees have individual IDs and passwords; use strong passwords for your accounts, and never write down or give out your user IDs or passwords.
Proactively manage users on financial applications	• Audit your users regularly, reviewing activities and transactions in which they have engaged. • Review user privileges to ensure that they only have the capabilities necessary to perform their functions. • Separate duties entailing financial transactions. • Delete or disable users who have changed jobs and no longer need the function or who are no longer employed by you.
Report suspected or attempted fraud to Wells Fargo	• Immediately notify Wells Fargo for help in assessing the situation and taking appropriate action, which may include placing holds on your accounts to help detect future fraud attempts. • **Online Fraud Hotline:** If calling from the U.S., Canada, or Mexico, dial 800-AT-WELLS (800-2893557). If dialing from a country that supports UIFN (Universal International Freephone Number), dial the international dialing code and then the UIFN phone number, which is 8000-ATWELLS (8000-289-3557). • **Bogus emails or websites:** reportphish@wellsfargo.com

WELLS FARGO

Fraud Protection Best Practices

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

Impostor fraud is on the rise, with companies in the U.S. and worldwide reporting billions of dollars in losses. It's extremely difficult for your bank to defend against or even to detect this type of fraud. To protect your accounts, you need a strong accounts payable policy and verification process in place within your organization.

What is impostor fraud?

Impostor fraud involves a fraudster posing as a person or entity you know and trust — a vendor, an executive of your company, even the IRS. You make payments according to instructions the impostor gives you, and, instead of going where you intended, the payments go to the fraudster.

As with other types of fraud, there are several variations and ways impostor fraud is perpetrated:

Vendor version

- A fraudster posing as a vendor requests that you change the payment instructions you have on file for the vendor — the bank, routing transit number, and/or account number. The request may come by phone, email, or letter.
- 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 phony payment request.

Executive version

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 for a high dollar amount. The request may come by phone, fax, or email, and the impostor may even tell you to keep the payments "confidential."

How to help reduce your risk

Alert your staff — especially your management team and your accounts payable department — to the possibility of impostor fraud. Apply vigilance and tighten internal controls to reduce your company's risk of becoming a victim.

- **Verify your vendor.** Set a policy requiring all requests for changes to vendor payment information be verified by the usual contact at the vendor company through a different channel than how the request was made.

  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.

  Communicate only to the phone numbers, email addresses, and contact names in your master vendor files.

- **Verify your requestor.** Set a policy requiring all requests for unusual payments made outside normal channels to be verified with a phone call to the requestor. Call only the phone number in your internal phone directory.

- **Watch your wires.** Set up Dual Custody on your online wires service. Instruct all wire initiators and approvers not to rubber stamp wires but to verify the full details. Verify before you initiate. Verify before you approve.

- **Audit your activity.** Reconcile your bank accounts every day, and notify the bank immediately if you spot an unauthorized transaction. Wire payments are final within seconds, so it may be too late to recall that transaction. But the bank can put a stop on payments to that beneficiary to prevent further losses.

For more information, contact your treasury management representative.

TM-3000 07/14