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 or a senior executive. The impostor contacts you by phone, email, fax, or postal mail and submits an invoice or requests a payment or a change to 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 type
- 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 request or payment change request.

☐ **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 rely on 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.