Unmasking impostor fraud
7 essential steps

Impostor fraud is on the rise. This sneaky scam happens when a fraudster poses as a person you know and trust — a company executive, a vendor, even the IRS. The impostor contacts you by phone, email, fax, or mail and requests a payment, submits an invoice, or asks to change vendor payment instructions or bank account information. If you fall for the scam, any payments you send go to the fraudster instead of where you intended.

Arm yourself against impostor fraud.
Remember, the best way to fight fraud is to build strong defenses within your company.

Educate your executives and staff
• Alert management and supply chain personnel to the threat of vendor and executive impostor fraud.
• Instruct all staff, especially AP staff, to question unusual payment requests received by email — even from executives.
• Make sure your AP staff is aware of the threat, because fraudsters may target them directly.

Alert vendors and partners
• Warn vendors that they are targets for fraud, too.
• Tell vendors you no longer accept changes to bank account information by email.
• Instruct your trading partners not to change their remittance information without verifying the request with you.

Protect your email account
• Never give your company email address or log-on credentials to anyone you don’t know who contacts you by telephone, email, or text message.

Authenticate all requests
• Verify electronic or unusual requests.
• Verify by a channel other than that through which the request was received.
• Use official contact information on file to verify; never use contact information provided in the request.

Use dual custody properly
• Pay close attention to the payment details.
• Authenticate a request before initiating the payment and before approving the payment.

Watch for red flags
• Pay close attention to the details of all payment requests.
• If something doesn’t seem right, it probably isn’t.

Monitor account activity
• Reconcile accounts daily to help spot fraudulent activity.

Contact your client services officer immediately if you suspect fraud, or call 1-800-AT-WELLS.