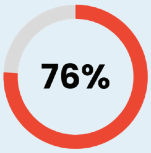
councilor
ADVISORS | CPAs

QUICK REFERENCE

Payment Fraud Prevention

A Vendor Banking Change Could Put Your Organization's Funds at Risk

Fraudsters may pose as legitimate vendors and request banking changes, diverting payments intended for those vendors into accounts they control. Because vendor updates are a normal part of doing business, fraudulent requests can go unnoticed.



According to a recent study by the Association for Financial Professionals, more than three - quarters of U.S. organizations experienced attempted or actual payment fraud in 2025.

Here's how it works:

Fraudsters use highly personalized spoofed emails, hacked vendor accounts, and phishing links to ask accounts payable teams to update ACH, wire, or direct deposit banking instructions. They may also send a request to update vendor information alongside a fraudulent invoice, diverting funds to an account they control.

Often, the fake request creates urgency, claiming a payment is due or overdue. The email may also ask for confidentiality, discouraging the recipient from checking with others. These tactics are designed to bypass normal procedures and make a fraudulent request appear legitimate.

Essential Prevention Steps:



Independently verify vendor banking changes.

Always verify changes through a trusted contact method before taking any action. Never rely solely on an email request or reply. Do not use phone numbers provided or trust incoming caller ID.



Strengthen internal controls.

Separate responsibility for maintaining vendor information from payment approval whenever practical. Dual approval workflows can add another layer of protection from scams.



Watch for signs of impersonation.

Look for misspellings or subtle differences in an email address, such as ".co" instead of ".com.". Even a familiar sender name does not guarantee that a request is legitimate.



Provide ongoing employee training.

Regularly reinforce verification procedures and how to recognize suspicious requests. Fraud tactics evolve, and employees need to know how to recognize and respond to them.



Use automated guardrails.

Payment platforms like BILL, Ramp, and similar tools help enforce approval workflows and controls, but technology and dual approvals do not replace independent verification.



Councilor's Accounting & Financial Advisory Services Can Help

Our Accounting & Financial Advisory Services team works with organizations to strengthen financial operations, improve internal controls, and manage risk. We bring expertise in accounting, strategy, and financial processes to help you protect resources and make informed decisions.

→ Contact a Councilor advisor to discuss ways to reduce payment fraud risk and protect your organization's resources.