July 2025 | CSN-Q3-2025

Leading security practices for small businesses.

Wire Transfer Fraud

Summary

Fraudsters are attempting a new ploy to trick commercial businesses into providing their bank account information and other sensitive information: wire transfer fraud. Insufficient internal controls, lack of employee training, and a lapse in good judgment can enable this fraud — and once funds have been wired, it is very difficult to retrieve them.

How This Scam Works

A business is contacted by a fraudster impersonating the company's bank or credit union regarding a wire transfer.

The fraudster claims to be questioning the validity of a wire transfer request and asks the victim to verify their bank account, multi-factor authentication, and wire transfer reference numbers.

Once the fraudster has the wire transfer information, they can create a fraudulent wire transfer to another bank account they've already established. They will monitor its activity, immediately verify receipt of the money, and withdraw the funds.

Fraud Facts

- The median loss for organizations with <100 employees was $141,000, and $200,000 for those with >10,000 employees. (2024) – *Association of Certified Fraud Examiners*
- Wire fraud can result in direct financial loss, including expenses related to an investigation(s) and legal fees. Businesses with insurance coverage may be responsible for deductibles and increased premiums. – *BILL*
- The Federal Bureau of Investigation (FBI) and the United States Secret Service are the primary federal agencies that investigate wire transfer fraud. - *FBI*

What's Your Risk?

Wire transfer fraud is a significant risk, especially for businesses (and individuals) that frequently use this payment method. Learn the following tactics, techniques, and processes to bolster your security response and use the internal controls listed below to safeguard your business.

Tactics	Technique and Process
Urgency and scarcity	Scammers create a sense of urgency or claim to have limited time and opportunity. The intent is to pressure victims into acting quickly without noticing the risk.
Sophisticated impersonation	Fraudsters do their homework to impersonate legitimate individuals or financial institutions, making it very hard to detect scams.
Business Email Compromise (BEC)	Fraudsters compromise email accounts belonging to the owner of your business or someone from a vendor and initiate fake transfers or approve fraudulent ones.

Internal Controls	
Educate employees	Use freely available security training material (e.g., EPCORPymts) to train your employees so they can recognize the most common social engineering tactics (e.g., pretext calling, phishing, smishing, etc.)
Avoid sharing sensitive information	Never share restricted or confidential information.
Be suspicious of unexpected requests	Remain vigilant against unexpected callers, emails, invoices, and the like.
Implement strong internal controls	Incorporate dual controls so that a second person sees and approves wire transfer requests. Verify the legitimacy of wire transfer requests via phone, email, or text. Contact your financial institution for additional technical controls.
Use secure communication channels	Avoid relying solely on emails.
Knowing how you will respond	If your small business utilizes wire transfers, establishing internal controls and using a tested, documented incident response plan will reduce your risk. This enables you to quickly respond in the event you experience fraud.
Verify contact information	Verify the caller's identity through alternate and legitimate sources.

! As a reminder, your financial institution will never ask you to provide sensitive account information it already has.

Resources

- What To Know Before You Wire Money, Federal Trade Commission
- The Fraud Risk Management Guide, Association of Certified Fraud Examiners
- Common Frauds and Scams, FBI

What to Do if You Are Scammed

- Contact your financial institution immediately so they can act and provide recommendations.
- Keep detailed records and document all communication, actions taken, and the timeline of

events.

- Identify and secure systems by examining communication channels (emails, phone calls) for any signs of phishing or unauthorized access.
- If you are the victim of burglary, vandalism, or theft, contact your local law enforcement agency.
- If your Social Security or individual tax identification number was stolen, immediately report it to IdentityTheft.gov.
- Report suspicious activity to the Internet Crime Center, www.ic3.gov, and/or your local law enforcement agency.

12120 Sunset Hills Rd, Reston
VA 20190