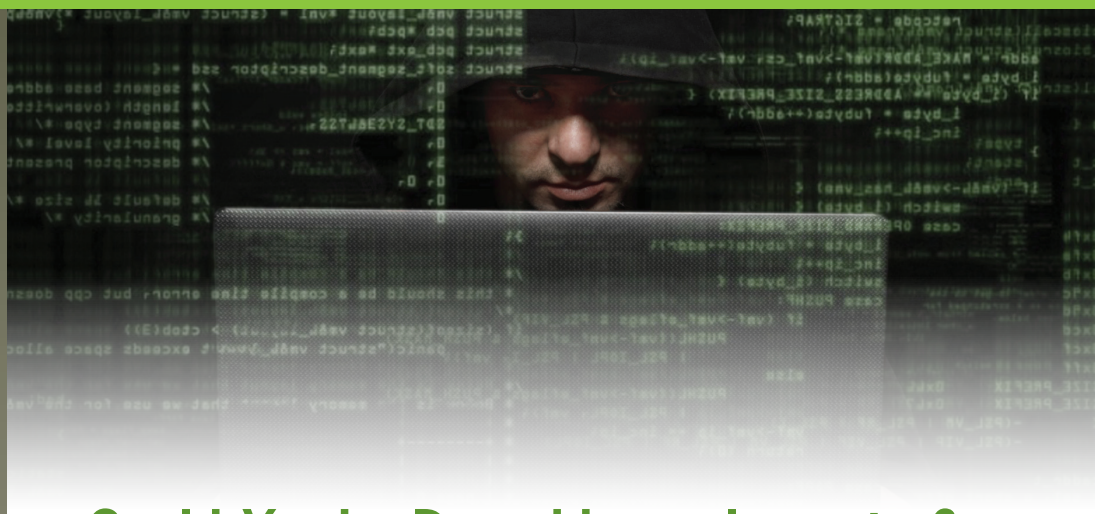
Treasury Management **Advisor**
Issue 106



Could *You* be Duped by an Imposter? Arm Yourself with Simple Solutions for Preventing Wire Fraud

Sam Prudhomme | Vice President, Wire Transfer & Integrated Payment Services

Imagine it has been an aggravating morning in traffic. You finally arrive at the office, sit down at your desk, and just when you have settled in with your coffee and begin dealing with the urgent and important swirling in a sea of emails and voice messages, the phone rings. It is a representative from your organization's most trusted vendor, and he is requesting that you wire funds as soon as possible in order to release a critical shipment your CEO is expecting. Your CEO is at a conference and unreachable, and he didn't mention this particular shipment, but then again that isn't out of the ordinary. Fearing impacts to your clients if you don't send the wire for the goods to be delivered, you only pause momentarily before you act. After all, this guy is a vendor with whom your organization works closely, so the request is legitimate, or so you think.

Corporations and small business alike continue to face growing concerns as wire transfer has become a target for increased fraudulent activity. Wire payments continue to be an attractive vehicle for criminals due to the speed and finality of settlement, coupled with the fact that wire originators and volume continue to grow, making the collective target larger.

Understanding the changing tactics fraudsters employ to perpetuate wire fraud is the first step toward prevention. Ensuring that internal controls and strategies are in place also will help protect your financial assets. If you haven't already considered the solutions available to help neutralize the threat, your electronic transfers could be at high risk.

Impostor fraud is on the rise

Just as in our scenario, impostor fraud involves a fraudster posing as a person whom you know and trust, such as an executive of your company or a vendor or government agency. The impostor makes contact via usual channels—phone, email, fax, or mail—and submits an invoice, requests an electronic payment, or maybe makes a change to vendor payment instructions. If you act upon the request based upon the perceived trusted relationship, any payments executed will then go to the fraudster instead of the legitimate benefactor.

Imposter fraud differs from schemes where online banking credentials are stolen and used to make fraudulent payments. With impostor fraud, your organization's authorized users actually make the payments in the normal course of business, so the payments appear as normal payments to the bank.

continued

learn more

Resources for Defending Against Wire Fraud:

- Visit regions.com/stopfraud for fraud prevention resources, including best practices and available webinars
- Visit regions.com/onlinesecurity for simple and effective online security hints, and more information about dual control approval for ACH and wire transactions

How Fraudsters Compromise Accounts and Wire Transfers

- Methods of compromise: malware, social engineering, phishing, vishing, smishing, email compromise
- Points of compromise: online, mobile, customers, employees, vendors
- Methods of initiation: online, email, fax, employee

Solutions For Detecting Wire Fraud

- Manual review
- Dual control
- Educating employees on fraud tactics and behavioral anomaly detection

This typically means the fraud is not quickly identified, which makes it even harder to recover the funds, particularly if sent by wire.

The number of those who fall prey to imposter fraud continues to grow rapidly, so it is very important to be cognizant of such schemes.

Prevention and defense

Financial loss is something that companies are experiencing more and more. To help mitigate your risk of potential loss due to fraudulent activity, we encourage you to institute the following best practice:

As stated by the Federal Trade Commission:

"Know that wiring money is like sending cash." Wired money is nearly impossible to recover should fraud occur due to the funds being transferred immediately.

Four effective practices to help protect against wire fraud:

1 If a request to initiate a wire comes via email, initiate a phone call to **verify the authenticity of the request** as being legitimate. Call a number that you know to verify.

2 **Review all wire approval limits** that you have established for your employees, for both telephone and iTreasury℠ wires, to ensure they are appropriately defined. Your Treasury Management officer can assist you with adjusting limits accordingly, as you should conduct an annual review of all wire approval limits.

3 **Institute dual control** for initiating and releasing wire transfers. Dual control consists of the separation of duties (as in one employee initiates the wire and a second employee approves it) and is an easy-to-implement control that not only prevents or decreases the risk of internal errors or irregularities, but also protects against unauthorized transactions initiated by a hacker.

4 Launch a fraud awareness and prevention initiative and **keep team members educated** about online risks and best practices on an ongoing basis.

Stop. Review. Release.

Before you click "Release" to finalize each wire transfer, first **stop and review**.

Stop: Always verify the legitimacy of the requestor and the wire beneficiary as well as the transfer amount.

Review: Look for signs of potential fraud including wire transfer requests received through a means that is non-standard for your business; for example, by email if that is not the standard means of request. Also, if a request is deemed urgent or confidential, a fraudster could be attempting to encourage quick action to discourage you from thoroughly verifying the legitimacy of the wire request.

Remember, if something seems amiss, chances are something is. Always stop and review to verify wire transfers before you click release. ▲

reporting fraud

Immediately report anything you feel is suspicious, including e-mails that appear to be from Regions, application pop-ups, unexpected error messages, or any unfamiliar login screens to Regions Client Services by calling 1-800-787-3905.