
**A criminal can commit fraud by impersonating a legitimate vendor and asking that payments be sent to a different bank.**

## Here's how it works:

The criminal sends a fraudulent email or a letter that appears to be on bank letterhead, indicating the vendor's banking information has changed. The accounting staff updates the information in the system. The deception may not be discovered for weeks or even months, when the vendor contacts the agency to say payments weren't received.

## How can you reduce your risk of this type of fraud?

Create and enforce strong internal procedures:

- Provide the vendor with your **most recent direct deposit authorization form**.
- Confirm requests for payment change instructions directly with the vendor **using known contact information** from agency records.
- **Be wary of emails.**
  - Consider the overall context and whether the request makes sense for that vendor with its history.
  - Examine the email address closely for minor changes and understand even exact email addresses can be "spoofed."
  - Look for red flags such as a sense of urgency and poor grammar or sentence structure.
  - Conduct regular phishing exercises.
  - Consult your manager if an email contains suspicious links or the request is unusual. When in doubt, verify with the vendor directly.
- **Check with the agency contract manager** about any changes in payment processing.

**Glenn Hegar**
Texas Comptroller of Public Accounts

## KNOW FRAUD:

Review additional fraud prevention tips and best practices at **https://fmx.cpa.texas.gov/fraud**