Protecting Your Staffing Company from the Rising Threat of Fraud

Julie Ann Bittner

TRICOM 35 Years
The Expert Solution for a Strategic Partnership℠
A WINTRUST COMPANY

1

It Can Happen to Any of Us

Not all fraud comes from inside your company or candidate poll.

Sometimes, it comes right through *a call disguised as a new client*!

2

The Setup

A *"new client"* approaches a staffing firm, often claiming rapid growth and/or urgent need for payroll support.

3

The Bait

The "new client" submits employee lists to be payrolled or funded. The names, SSNs, and timesheets look legitimate.

4

The Trap

The staffing firm processes/funds payroll, expecting reimbursement from the “new client”.

5

The Fallout

The “new client” delays payment for 45-60 days and disappears. The staffing firm discovers the “employees” were fake - bank accounts lead to fraudsters.

Losses in these cases often run $500,000 - $1MM

Two US agencies reported $690k and $703k losses in 2023

6

Why This Type of Fraud is Increasing

- Remote and digital onboarding make in-person verification rare.
- Generative AI allows convincing documents, fake LinkedIn profiles, and fabricated company websites.
- Staffing firms are eager to onboard new clients quickly in a competitive market and in a down market – fraudsters exploit that speed.

7

Warning Signs of Fraudulent "Client"

- Rush to fund payroll before verifying credit or site visit.
- Inconsistencies in company information.
- Email address does not contain company name.
- All communications handled by one individual who defers/resists direct contact with "employees"

8

Prevention & Detection Strategies

- Client Verification: Require all new clients go through a thorough verification of tax ID, company credit, website, owners, phone numbers and email.
- Site Verification: Conduct a physical or virtual site visit before processing first payroll.
- Dual Verification: Have two internal departments (operations & sales or management) approve any new payrolling client.
- Technology: Use data tools that mismatched EINs, identical bank routing for multiple “employees” or fraudulent SSNs
- Fraud Policy: Build clear escalation procedures and communicate them to staff (Red Flag Emails) – No exceptions for “urgent” deals.

9

Response

- Immediately freeze payroll and funding to the suspected client.
- Alert your banking partner/funding partner and legal counsel.
- Preserve communications and payment records for law enforcement. File a police report.
- Use the incident to educate your team and clients about being vigilant with following procedures.

10

Common Fraud Schemes in Our Industry

- The Bait and Switch: You interview one person, but another person shows up for the assignment.
- Internal Misappropriation: The theft or misuse of your company's assets by an internal employee or group of employees for personal use.
- The Man in the Middle: You receive an email purporting to be from your employee or vendor requesting a change to banking information.

11

Common Fraud Schemes in Our Industry

- The Trade Dress Grifter: Someone poses as your company to defraud unknown candidates based on the goodwill you've built.
- The Payroll Scheme: You receive a request to payroll employees with fraudulent identities and payment going to the fraudster's bank account.

12

Call to Action

- Review your internal controls
- Maintaining credit or background check requirements (especially for new clients)
- Audit vendor changes; especially bank accounts
- Schedule staff training
- Establish a reporting protocol

13

Call to Action

Fraud has always been a risk within the staffing industry. Follow the process. ***Do Not Deviate From It!***

14

Thank You

TRICOM® 35 Years
The Expert Solution for a Strategic Partnership®
A WINTRUST COMPANY

15