Lowenstein Sandler

Client Alert

Data, Privacy & Cybersecurity

December 20, 2024

Emerging Threat: Task-Based Employment Scams Target Businesses and Their Employees

By Matthew P. Hintz, Kathleen A. McGee, and Pati Candelario

A new wave of sophisticated gamified job scams, often called task scams, is targeting both companies and job seekers, according to recent Federal Trade Commission (FTC) data. These scams trick people into performing simple, fake tasks with promises of payments that never materialize. Scammers are using legitimate companies' information to lure people into the schemes, and clients should be on the lookout for potential signs of brand impersonation and fraudulent activity.

Understanding the Scam

The numbers are alarming: Victims lost over $220 million in just the first six months of 2024, far outpacing previous years' losses.[1] Here's how these scams typically work:

- Scammers send unsolicited messages offering easy online work.
- They ask victims to perform simple tasks such as "liking" videos, claiming this will earn them commissions.
- After showing victims their supposed "earnings," scammers demand deposits or fees to access the money.
- The promised payments never arrive, and any money sent is lost.
- Many scammers use cryptocurrency, making it nearly impossible to recover stolen funds.

Business Impact and Legal Risks

When scammers impersonate legitimate companies in these schemes, the damage goes beyond the immediate victims. Businesses face several serious risks:

- Reputation Damage: When scammers use your company's name, brand, and trademarks in fraudulent job posts, it erodes public trust in your business.
- Legal Exposure: Victims may sue your company, claiming you should have prevented the misuse of your brand and trademarks. Even if these claims do not succeed, defending against them costs time and money.
- Regulatory Issues: Your company could face scrutiny of whether it took reasonable steps to protect its brand and trademarks from misuse in employment scams.
- Hiring Disruption: The flood of fake job offers impersonating your company can make it harder to conduct legitimate recruitment.

Risk Mitigation Recommendations

This is an ideal time for companies to update their cybersecurity and preventive measures. Take these concrete steps to shield your business:

- **Strengthen Internal Controls**: Create clear protocol for all official company communications and for reporting suspicious job offers using company branding and trademarks.
- **Educate Your Team**: Train your employees to spot fake job offers, make sure everyone knows how scammers operate, and create channels for reporting suspicious communications.
- **Guard Your Brand**: Monitor unauthorized use of the company's trademarks in job postings on online job boards like LinkedIn and Indeed, and maintain an updated careers page stating official recruitment and employment practices.
- **Document and Report**: Keep records of all impersonation incidents, report confirmed scams to the FTC, and consult legal counsel when needed.

---

[1] According to FTC data, reported losses from these scams have increased dramatically: $90 million (2020), $131 million (2021), $179 million (2022), $286 million (2023), and $223 million (just through June 2024). See Federal Trade Commission, Fraud Reports, https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/SubcategoryPaymentContact?utm_source=govdelivery.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

MATTHEW P. HINTZ
Partner
T: 973.597.2596
mhintz@lowenstein.com

KATHLEEN A. MCGEE
Partner
T: 646.414.6831
kmcgee@lowenstein.com

PATI CANDELARIO
Associate
T: 862.926.6569
pcandelario@lowenstein.com