How Companies Can Respond to the Surge in Job Scams

MARCH 7, 2023

The ubiquity of remote work and online hiring has led to a sharp rise in job scams across industries. In these swindles—sometimes called employment scams or recruitment scams—fraudsters impersonate job recruiters from real companies and convince job seekers, who have often posted their résumés on job recruiting websites or social media platforms, that they are taking part in legitimate recruitment processes or have landed jobs, which are in fact phony and nonexistent. Usually communicating through email or text message, the fake recruiters induce victims to hand over personal information, cash bogus checks, or send money for training or office equipment.

These are profitable crimes. The financial losses of job scams swelled when the COVID-19 pandemic hit, from $174.2 million in 2020 to $209.1 million in 2021, to $367.4 million in 2022, according to the Federal Trade Commission (FTC), a 110% increase in just two years.

Job scams may grow more common with the rapid adoption of chatbots that can mimic human-conversation. These programs may make it easier for malicious actors whose first language is not English to converse convincingly with English-speaking victims. (For a discussion of this and other legal and business risks of chatbots and generative artificial intelligence, see WilmerHale's recent client alert.)

In addition to the victimized jobseekers, these frauds harm the impersonated companies, by tarnishing their brands and harming their reputations in the contest for talent, all while creating significant distractions and unplanned costs. Every case is different, and a business should work with counsel to respond to the circumstances of each situation. But in general, companies should consider the following key steps when responding to a job scam incident.

- ***Act Quickly.*** Malicious actors are likely to keep at a fraud so long as it is successful, and to desist and move on to the next victim if the company or law enforcement take steps to impede the swindle.
- ***Speak Out.*** To warn potential victims of the fraudulent activity, companies should consider posting a public statement advising jobseekers of the fraud to their websites, social media accounts, and profiles on recruiter websites, such as LinkedIn, Indeed, and ZipRecruiter, once they learn of it.

- ***Report Impersonation Accounts.*** Fraudsters often set up webpages and email accounts that impersonate a legitimate company's website to give the scam a believable gloss. For example, a fraudster targeting XYZConsulting.com may create the website XYZConsultingJobs.org, to which it can lure victims for their "job interviews." Impersonation campaigns often infringe on a company's intellectual property and violate the domain hosts' terms of service. Businesses, either on their own or working with counsel, can usually have these impersonation sites taken down by filing reports with the web or email domain hosting companies. Likewise, companies should report phony job posts to job recruitment websites or social media platforms.
- ***Keep Records.*** Companies should hold on to documentation both of the scams and the financial harm caused by the scammers to jobseekers and the company.
- ***Contact Law Enforcement.*** The FBI is responsible for investigating job scams, and companies, either directly or through counsel, should consider reporting job scams to the FBI's Internet Crime Complaint Center ("IC3") and directly to the relevant FBI field office. Law enforcement may ask for the documentation both of the scams and of the financial harm caused by the scammers to jobseekers and the company.
- ***Send Cease-and-Desist Letters.*** Companies may choose through counsel to send a cease-and-desist letter to the malicious actors directly.

WilmerHale has significant experience helping companies address job scams and other forms of disinformation, what we call Disinformation and Deepfakes Risk Management (DDRM). Please click here to view WilmerHale's thought leadership in this area. WilmerHale will continue to follow developments on these matters. To stay updated with our writings on this topic, please subscribe to the WilmerHale Privacy and Cybersecurity Blog.