FP Weekly Checklist: Avoiding the New Breed of Workplace Scams in the Remote Work Era

Insights
1.30.23

Each week, FP Weekly members receive a practical and cutting-edge checklist of issues to consider, action steps to take, and goals to accomplish to ensure you remain on the top of your game when it comes to workplace relations and employment law compliance. This week we provide you a checklist of items to consider when it comes to avoiding the new breed of workplace scams that have blossomed given the rise of remote and hybrid work over the last few years.

Understanding the New Trends

Workplace scams have been around long before work-from-home became a popular trend, but they have certainly accelerated in the last three years. The very nature of WFH or hybrid work leads to particular situations and loopholes that can be exploited by unscrupulous parties looking to take advantage of the unique conditions at play. Given this shift in the modern workplace, there are four specific cons that have exploded of late that you should familiarize yourself with if your business has adopted the WFH model in whole or in part.

Employers Getting Scammed By Fake Applicants

The most troubling new scam was recently called out by the FBI. According to federal criminal authorities, scammers are using a combination of deepfakes* and stolen Personally Identifiable Information (PII) when applying for a variety of remote work and work-at-home positions. If that person gets hired under a false identity, they will have security clearance to obtain company logins, passwords, accounts, and other sources of data – allowing them free access to sensitive company and third-party information. Then, they can exploit this information in countless ways, each more damaging than the next.

**For those unfamiliar, deepfake technology allows users to present a manipulated video, image, or recording that is so convincing it permits the scammer to misrepresent themselves as another person. You can read more about it here.*

Employers Getting Scammed By Overemployed Workers

Are your employees secretly juggling multiple full-time jobs? We've seen the rise of applicants seeking to work in a full-time remote role without telling their prospective employer that they

seeking to work in a full-time remote role without telling their prospective employer that they already have full-time jobs with other organizations – sometimes 10 or more. While you may not care if your remote workers hold multiple positions, it becomes a problem if applicants forge their resumes to look underqualified (or to hide other jobs they hold) and then put in the least amount of work possible hoping to slide by and collect paychecks for as long as they can. This can be especially problematic in industries with worker shortages – where employers may be willing to tolerate subpar work for longer periods of time. It can also be troublesome if your employees conduct work for organizations in direct conflict with your own.

Applicants Getting Scammed By Fake Employers

Scams can be initiated from the "employer" side, too. In fact, your newsfeed is probably replete with stories of applicants being duped by fake companies. The Wall Street Journal, for example, just reported that scammers are targeting laid-off tech workers given the high number of RIFs and the popularity of remote work in that field. Or you may even know of someone who was going through the interview process – or perhaps was even "hired" – before realizing they were being scammed.

The Federal Trade Commission reported just how big of a problem this has become. The number of reported job scams nearly tripled to 104,000 in recent years, causing workers to lose more than $200 million last year alone.

The scenarios usually start the same – an applicant (oftentimes a tech-savvy professional) believes they are going through a standard remote work application process, sometimes even receiving a job offer. Sometimes the applicant is contacted by someone purporting to be a recruiting representative from an established company, but many times the applicant falls for a fake job listing found on LinkedIn or elsewhere.

They might turn over personal information along the way – like SSNs or bank account information for direct deposit purposes – which is then exploited for nefarious purposes by the criminals running the scam. Or the company might ask them to buy electronic equipment they'll need for the job (laptops, cell phone, external hard drives, printers, etc.) and tell them to send the equipment to the "company" for "formatting." The scammers may promise reimbursement, or sometimes even sending a check that will only be reported as fake days or weeks after it is deposited.

Of course, this equipment actually lands in the hands of scammers. Meanwhile, several days have gone by before the applicant or new hire realizes they have been compromised — and now they're out hundreds or thousands of dollars and nowhere closer to landing their dream remote job.

Employees Getting Scammed By Fake Coworkers

Many employers are already familiar with the tried-and-true scam that leads unsuspecting workers to purchase gift cards or wire money to off-shore accounts for someone they believe to be a coworker – often a superior – but is actually a criminal. These so-called "spearfishing" schemes have been around for quite some time, preying on a sense of urgency and the perceived power

imbalance in the request (administrative personnel are much more likely to quickly respond when they believe the CEO is asking them to complete an emergency request).

But these scams have taken on a new prominence given the uptick in remote work arrangements. The use of deepfakes allows scammers to use the voice of a coworker – or even their likeness in a video communication – to trick employees into fulfilling requests. And since the workers are separated by hundreds or thousands of miles, it's harder to verify the validity of the request.

Your Checklist to Avoid the Modern Scam

_____ Offer a clear notice on the hiring/recruiting page on your website outlining what your company will and won't do during the interview and hiring process. ("We'll never ask you to purchase your own tech equipment and ship it to us," for example.) Let applicants know that they will be speaking with a live human at some point and the hiring process will not be in a 100% electronic format. Tell them that only job listings from your website can be confirmed as authentic, and that any recruiter you work with will have an official email address from your company and not a third party.

_____ Reconsider the type and quantity of information you ask job applicants to provide and ensure you are only requesting the bare minimum needed to process the application and confirm that the applicant is who they claim to be and not an imposter. After all, seeking a treasure trove of data from applicants may end up unintentionally deterring job seekers who are worried that you are scamming them. You should balance the need to verify identity against the risk of over-collection of data.

_____ Be alert for oddities during the video interview process. Scammers use voice spoofing or voice deepfakes during online interviews. Oftentimes, the actions and lip movement of the person being interviewed do not completely coordinate with the audio of the person speaking. At times, actions such as coughing, sneezing, or other auditory actions are not aligned with what is visually presented. The MIT Media Lab has created a website and its own checklist of video elements you should be attuned to in order to avoid getting tricked.

_____ Consider the feasibility of conducting in-person interviews, even for remote positions. If the position is important enough to the organization, you should find a way to fit it into your budget and your calendar to pay for their travel to your office. In fact, even mentioning that the process includes an in-person interview may dissuade scammers from continuing with the interview process.

_____ Don't skimp when it comes to the employee verification process. You could have the best processes in place but feel pressured to skip some steps if you are under the gun

to onboard new hires as rapidly as possible. Make sure you run through your normal background check process.

_____ Include clear notice in your policies – and in the information shared with applicants – that you expect full-time workers to have only one full-time job at a time. While it is up to you whether you want to restrict outside part-time work that does not interfere with their job – to the extent permitted within the jurisdiction in which the employee will be working – you do not want your employees to be overemployed.

_____ Also, make sure your conflict-of-interest policies are up to date, ensuring workers understand that they are not to conduct work that directly conflicts with your organization's business.

_____ Make sure your managers are not tolerating substandard work. They should be performing regular check-ins and 1:1 meetings, and holding all of their team members to the same standards. This will make it harder for remote work scammers to slide through unnoticed and collect paychecks for not working.

_____ To the extent you intend to employ tracking tools to monitor remote employees' productivity, ensure you are consulting with counsel to comply with applicable laws in terms of notification and consent requirements.

Conclusion

We will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information. For further information, contact the author of this Insight, your Fisher Phillips attorney, or any attorney in our Privacy and Cyber Practice Group.

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email

Service Focus

Privacy and Cyber