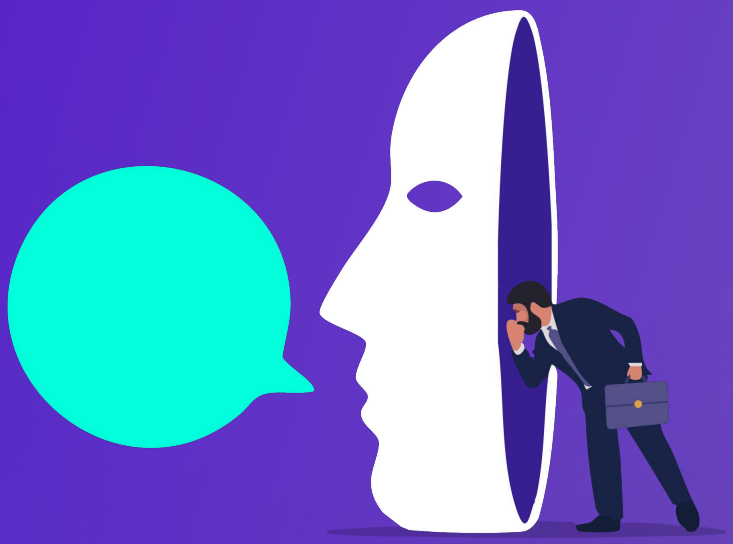
BrightHire

Candidate Fraud:

Your complete guide to detecting and safeguarding against fake candidates.

"The hiring process is an inherently human process with many hand-offs and many different people involved. It's become a weak point that folks are trying to expose."

Benjamin Sesser
CEO of BrightHire



Candidate fraud is on the rise. Take action to protect your hiring process today.

Candidate fraud is escalating due to remote work and AI, forcing TA teams to defend against threats from sophisticated fraudsters to state-sponsored attacks.

This comprehensive guide outlines everything you need to know about the more severe types of fraud: the risks, real examples, and most importantly, actionable steps to protect your company.

> **By 2028, 1 in 4 candidates could be fake, according to Gartner**

The Chapters

Understanding Candidate Fraud

Candidate fraud is exploding—AI, remote work, and deception are reshaping hiring.

Types of Candidate Fraud

From bots to deepfakes, candidate fraud is evolving fast—learn the risks hiding in plain sight.

Spot the Lie: 14 Red Flags Every Hiring Pro Should Know

Learn how to detect fake candidates with subtle signs across resumes, interviews, and online profiles.

Building Your Defenses: Proactive Steps to Stay Safe Against Candidate Fraud

Proactive hiring tips to detect and prevent candidate fraud early.

Real-Life Examples: True Cases of Fake Candidates

Fraud is happening, it's sophisticated, and even vigilant companies can be targeted.

Candidate Fraud Exposed: Understanding the Threat, Factors Fueling the Rise & Risks

What is Candidate Fraud?

Candidate fraud refers to any instance where an applicant intentionally misrepresents themselves during the hiring process. The spectrum of this deception is wide, ranging from minor infractions to highly organized criminal activity.

In this guide, we'll deep dive into the more severe types of fraud, highlighting signs to look for and how to protect your organization.

A Rapidly Growing Threat

- Gartner predicts that by 2028, globally **1 in 4 job candidates will be fake**. This is largely due to the proliferation of AI-generated profiles and application tactics.
- Beyond individual attempts, **organized schemes** are also generating significant revenue. For instance, the UN estimates that North Korean IT worker scams alone have funneled **$250MM - $600MM annually** to the regime since 2018, often funding sanctioned activities like weapons programs.
- Since 2022, the FBI has warned of increased fraud using deepfakes and stolen personally identifiable information (PII) to apply for remote jobs.

> **"Talent teams and hiring managers are responsible for talent strategy and other important things, but being on the front lines of security has historically not been one of them. Folks may think they're not experiencing candidate fraud, but it's probably more likely that they're just not realizing that it's going on."**
>
> 
>
> **Benjamin Sesser**
> CEO of BrightHire

What's Driving the Rise in Fraud?

- **Remote Work & Global Hiring:** Remote work and virtual interviewing makes it easier for fraudsters to hide their true identity, location, and even the fact that someone else might be involved in the interview process.
- **Generative AI:** AI tools make it trivially easy to create fake profiles and perfectly tailored resumes, generate plausible answers in real-time, cheat on assessments, and even power deepfakes.
- **Job Market Imbalances:** High demand for certain skillsets, combined with economic pressures can lead some individuals or groups to resort to deceptive tactics to secure employment.
- **Sophistication of Bad Actors:** Organized crime and state-sponsored groups are becoming increasingly adept at exploiting the hiring process, using tactics like identity theft and coordinated efforts to bypass security measures.

The Real Costs of Hiring a Fake

Hiring a fraudulent candidate goes far beyond the frustration of a bad hire. The consequences can ripple throughout an organization, impacting finances, security, and reputation, and can be magnified particularly for organizations handling highly sensitive data (e.g. healthcare, financial institutions) or critical infrastructure (e.g. utilities, military, etc).

- **Wasted Time and Resources:** Countless hours spent screening fake applications, interviewing unqualified or deceptive individuals, and onboarding someone who can't perform the job or has malicious intent.
- **Direct Financial Loss:** Salaries paid to underperformers or fraudsters, costs associated with re-hiring, potential ransom demands, and direct theft if financial systems are compromised.
- **Security Breaches & IP Theft:** Fraudulent hires, especially those placed by sophisticated actors, may aim to exfiltrate sensitive company data, customer information, proprietary code, or trade secrets.
- **Malware and System Damage:** There have been recorded incidents where fraudulent hires installed malware on company systems upon receiving their equipment.
- **Negative Team Impact:** Any mishire hurts productivity and morale, but fraud-related hires are significantly more disruptive.
- **Reputational Harm:** Fraudulent hires can devastate brand trust, especially when linked to data breaches or public incidents, affecting all stakeholders.

Types of Candidate Fraud from Low to High Risk

Low Risk

Mass Applications

Using AI to generate and submit thousands of tailored resumes and cover letters. While often driven by desperation rather than malice, this floods systems, wastes recruiter time, and can obscure genuinely qualified candidates.

Medium Risk

Candidate Cheating

Leveraging AI for assessments, coding tests, or real-time answer generation during interviews. This misrepresents a candidate's true abilities, potentially leading to costly mishires and performance issues.

High Risk

Fake Candidates / Impersonation

Having someone else (an impersonator) conduct interviews OR using sophisticated "deepfake" technology where the person on screen appears to be talking, but their words are generated by AI or spoken by someone else off-camera.

Highest Risk

Organized / State-Sponsored Fraud

Placing individuals within companies with specific, malicious intent to steal data, intellectual property, or funds, or to install malware. These complex operations are often run by criminal organizations or malicious governments like North Korea.

Spot the Lie: 14 Red Flags Every Hiring Pro Should Know

Developing a "spidey sense" for potential fraud is crucial. While many of these signs could have innocent explanations (beware of false positives!), they warrant further investigation.
Train your team to watch for:

- [ ] **LinkedIn Profile Watchouts:** Profiles that were recently created, missing basic information (like a Master's listed without an undergrad degree), few LinkedIn connections.
- [ ] **Questionable Profile Pictures:** Use of stock photos or pictures associated with other individuals when doing a reverse image search.
- [ ] **"Too Good to be True" Career Paths:** Illogical career paths (e.g., elite degrees/jobs with no grounding) or experience that lines up *too* perfectly to the job description.
- [ ] **Suspicious Interview Behavior:** Answers that don't match the resume, sound heavily scripted, are identical to AI-generated responses, or lacking credible answers when probed.
- [ ] **Face/Appearance Mismatches:** The person looks noticeably different across multiple interview stages or doesn't resemble the person who shows up for work (check interview recordings!).
- [ ] **Voice Mismatches or Oddities:** Does the voice sound different across calls? Are there unusual speech patterns or indications of voice-changing technology?
- [ ] **Potential Deepfake Signs:** Unnatural facial movements, poor lip-syncing, flickering around the edges of the face, lack of normal blinking or emotional expression.
- [ ] **Excessive or Unusual Background Noise:** Does it sound like a noisy call center with multiple people talking in the background? Anything inconsistent with a typical home office environment should put you on alert.
- [ ] **Unnatural Pauses & Delays:** Frequent long pauses, looking away, or audible typing can signal the candidate is receiving external help or looking up answers online.
- [ ] **Inconsistent Answers:** Contradictions within a single interview or across different stages of the process such as with years of experience or inability to give a consistent chronological overview of their work history.
- [ ] **Reluctance for Video or On-Site Interaction:** Resistance to turning on the camera (especially without a good reason), blurring backgrounds excessively, or finding constant excuses to avoid meeting in person if required.
- [ ] **Unusual Requests:** Asking for sensitive company information early in the process or making peculiar payment requests.
- [ ] **Identity Theft Indicators:** Using a known stolen identity, potentially even one belonging to someone deceased. Check for inconsistencies in names and background details.
- [ ] **Location & IP Address Mismatches:** IP address doesn't match the location stated on the resume or profile. Signing documents (like NDAs) or logging in from geographically diverse IPs in a short time. If you have a security team, you might also seek to track latency or VPNs from your video conferencing provider for the candidates interviews as a signal for where they are located.

Building Your Defenses: Proactive Steps to Safeguard Your Hiring Process

Awareness is the first step, but proactive measures across the hiring lifecycle are essential. Here's a step-by-step approach:

A. Building a Culture of Fraud Awareness:

- **Raise Awareness & Train Your Team:** Ensure everyone involved in hiring (recruiters, HR, hiring managers) understands the types of fraud, the red flags, and the importance of vigilance. Awareness is the #1 priority because bad actors target low suspicion.
- **Foster a Vigilant Culture:** Encourage your team to trust their gut and speak up about suspicions without fear. Make sure everyone knows the clear, safe way to report concerns internally.
- **Hold Third Parties Accountable:** Ensure your staffing agencies, RPOs, headhunters, and contingent work platforms are aware of these threats and implement equally rigorous fraud prevention measures. Bad actors will probe for the weakest link.

B. Pre-Interview / Screening Stage:

- **Scrutinize LinkedIn Profiles:** Check LinkedIn profiles for date created, number of connections, activity, and consistency.
- **Use reverse image search:** See if the individual's profile picture is being used by others or if it is a stock photo.
- **Verify Contact Information:** Be clear on where the individual is based so you can identify signs if they are not using that same location during interviews, or in future. Use tools to identify Voice over IP (VoIP) numbers or VPNs. Use public records to verify addresses for suspicious candidates.
- **Implement Robust Identity Verification:** Consider using identity verification providers that offer a higher level of scrutiny, similar to airport security checks, especially for sensitive roles.

C. Interview Stage:

- **Train Your Hiring Panel to Look for Signs:** Train all your interviewers to probe for and flag suspicious candidate behavior.
- **Require Cameras On:** Mandate cameras during video interviews. Ask candidates to briefly turn off background blur if suspicion arises to see the environment.
- **Ask Probing Questions:** Ask specific questions related to their claimed location ("What's your favorite local coffee shop?") or delve deeper into project details mentioned on their resume. Note evasiveness or vague responses.
- **Observe Behavior Closely:** Pay attention to pauses, eye contact (or lack thereof), background noise, and signs of reading or being coached.
- **Record Interviews (with consent):** Use tools like BrightHire to record interviews. This provides an objective record to review if suspicions arise later and helps verify consistency in appearance and answers.

D. Verification & Offer Stage:

- **Mandatory Phone References:** Require phone calls for reference checks, not just email.
- **Use Savvy Background Check Vendors:** Don't rely on basic checks. Partner with providers skilled in fraud detection who verify employment history and income records (e.g., via Social Security number verification where permissible) to confirm claimed roles and timelines. They should rigorously verify references, not just call potentially fake numbers provided by the applicant.
- **Carefully Examine Payment Requests:** Scrutinize where new hires request payments to be sent, looking for unusual locations or intermediaries.
- **Revisit Interview Recordings:** Use previously recorded interviews to verify the same person was present across all interview interactions and examine for any other flags.

E. Onboarding & Post-Hire:

- **Secure Equipment Shipping:** Only ship company laptops and equipment to verified residential addresses listed on the application or background check, or use secure pick-up locations requiring ID (like a UPS Store). Avoid shipping to mail forwarders or unknown business centers.
- **Require in-person onboarding (where possible):** If feasible, request employees to be in-person for new hire training.
- **Require Periodic Camera Use:** For remote employees, require cameras to be on during certain meetings or check-ins to ensure the person working is the person hired. New hire training is a good opportunity to do this.

Special measures for high-risk roles

- **Consider Fingerprinting:** Some financial institutions are now using fingerprinting during onboarding as an added layer of identity verification.
- **Practice "Principle of Least Privilege":** Limit new hires' access to systems and data to only what is strictly necessary for their job function, especially initially. Monitor for unusual software installations or remote access tools.

Real-Life Examples: True Cases of Fake Candidates

These stories underscore the reality: fraud is happening, it's sophisticated, and even vigilant companies can be targeted.

The Large-Scale Operation

The U.S. Justice Department uncovered a scheme affecting over 300 companies, including major retail and tech firms, generating nearly $7 million for fake IT workers, likely linked to North Korea.

A Cybersecurity Firm Falls Victim

KnowBe4, a company specializing in security awareness training, unknowingly hired a North Korean IT worker using a stolen American identity. They sent him a workstation, which he immediately began loading with malware. Luckily, he was caught before major damage occurred.

Ransom Demands

A company hired a fraudulent North Korean employee who infiltrated systems and downloaded information. After being caught and fired, the individual demanded a ransom payment to prevent the release of the data.

> **"No longer are they just after a steady pay check, they are looking for higher sums, more quickly, through data theft and extortion, from inside the company defenses."**
>
> **Rafe Pilling,** Director of Threat Intelligence at Secureworks

Experiences from BrightHire Customers

- One customer discovered an applicant was using the identity of someone who had died.
- Another found a candidate could speak at length about their last two jobs but was completely stumped when asked about earlier roles – they hadn't rehearsed those lies.
- A candidate aced initial interviews but refused to be on camera for the deep-dive technical interview with the hiring manager – they likely weren't the one with the skills.
- A healthcare company hired someone, only for the recruiter to notice the new hire's Slack photo didn't match the person interviewed. Reviewing interview recordings confirmed the discrepancy, leading to termination. Records showed the individual logging in from various global locations.
- Recruiters reported seeing applicants pause unnaturally after questions, looking aside as if being fed answers, and even spotting extra limbs (belonging to someone off-camera) during video calls.

BrightHire's Own Encounter

Even we at BrightHire encountered a suspicious candidate for a back-end engineer role. The applicant had an unusual name for his accent, gave a lengthy, overly rehearsed background story, but then became stumped and audibly seemed to be searching for an answer when asked a simple follow-up question ("Where were you before Amazon?"). Throughout the interview, pauses, keyboard noises, and increasingly evasive responses raised major red flags.

Conclusion: Staying Vigilant in the New Era of Hiring

Candidate fraud is no longer a niche problem; it's a significant and growing threat impacting organizations of all sizes, globally. From AI-powered cheating to sophisticated state-sponsored infiltration, the methods are evolving, and the potential damage is substantial.

Talent Acquisition teams are now guardians at the gate, playing a critical role in protecting their organizations. By fostering awareness, training teams to spot red flags, implementing robust verification processes throughout the hiring lifecycle, and leveraging technology thoughtfully, companies can significantly mitigate their risk.

Don't let your organization become the next victim. Stay informed, stay vigilant, and build strong defenses against the rising tide of candidate fraud.

Report suspicious activity: If you suspect you've encountered fraud, especially involving potential North Korean actors, report it to the FBI's Internet Crime Complaint Center (IC3) at www.IC3.gov.

BrightHire

The AI copilot for exceptional hiring

BrightHire is the leader in Interview Intelligence, trusted by 300+ clients to transform how they hire - delivering substantial hiring efficiency and consistently raising the bar on the quality.

TRUSTED BY HUNDREDS OF GAME-CHANGING COMPANIES

toast Canva ramp Vercel onetrust klaviyo
attentive Talentful greenhouse NAVAN zapier

G2 ★★★★★ 4.9 rating

Curious to learn more?

Contact sales@brighthire.ai to experience the ease, breadth and depth of BrightHire's interview intelligence platform firsthand.