Supporting Talent Acquisition Teams During an Epidemic of Hiring Fraud

A Polyguard Whitepaper for IT Departments

May, 2025

Executive Summary

The Challenge of Hiring Fraud

The modern hiring process is under siege. What once relied on in-person interactions and trusted referrals has evolved into a high-velocity, remote-first system — and with that shift has come a surge in deception. Hiring Fraud has emerged as a systemic threat, where candidates misrepresent their identity, outsource interviews to third parties, or leverage AI tools to convincingly impersonate qualified professionals. Proxy candidates and malicious impersonation techniques are now widespread, blurring the lines between legitimate applicants and synthetic fraudsters.

For staffing firms and recruiters, the cost isn't just reputational — it's operational and financial. Time is wasted vetting candidates who don't exist, interviewers are misled, client trust is eroded, and in too many cases, impersonators make it through to placement — triggering contractual penalties, regulatory headaches, and the loss of critical business relationships. These errors aren't just human; they're systemic, exacerbated by brittle verification workflows and an overreliance on screenshots, spreadsheets, and good faith.

Beneath the surface lies a quieter crisis: the normalization of unsafe behaviors. Candidates are routinely asked to share sensitive personal data through insecure channels, often with minimal verification or safeguards. This not only creates risk for the recruiter and the employer — it sets up jobseekers to become victims of fraud themselves. In the rush to screen faster, we're training users to trust blindly — and in doing so, we've opened a new front in the battle for digital identity.

Recruiting fraud is no longer just a Talent Acquisition problem—it's an IT and security risk. Deepfake interviews, fake credentials, and global impersonation schemes expose your company to data breaches, reputational harm, and compliance failures. While your Talent Acquisition (TA) team focuses on hiring, **your infrastructure, policies, and systems are what keep the organization secure**.

Why Polyguard Is the Smart Choice for IT Teams

Every IT department has too much to do, and not enough resources to go around. So addressing new risks isn't just a matter of deploying a quick fix; it's critical to make sure that we don't make things worse while we're trying to make them better.

Polyguard makes that job easier—by embedding identity verification directly into the recruiting workflow, without creating new risk for IT to manage. Let's look at the specific set of approaches that Polyguard uses to minimize new work and reduce both new and existing risks:

- Eliminating accidental capture of candidate PII
- Verifiable location data (mitigating existing tax risks as well as co-employment)
- Hands-free ongoing compliance testing for location and identity
- No change to recruiter workflows - integrated into existing conferencing software
- Bidirectional Identity Verification
- Built-in high-touch support keeps any new tickets out of the IT helpdesk
- Compliance-ready business records affidavits avoids new audit workloads

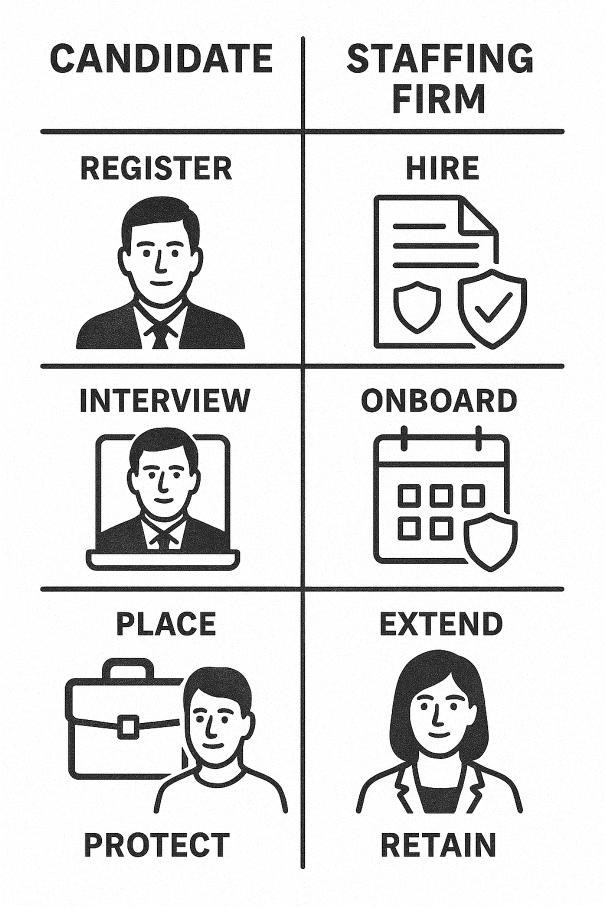
No Sensitive Data Retention = No Extra Liability

Most identity tools dump PII into your environment—creating a compliance nightmare. Polyguard verifies IDs and biometrics in real time, then discards the sensitive data immediately after verification. Nothing is stored. There's nothing for attackers to exfiltrate, and no long-term data retention policies for your team to manage.

This isn't just easier—it's safer.

Location Verification That's Actually Verifiable

Spoofed IP addresses are trivial to fake. Polyguard uses trusted mobile hardware signals like SIM and GPS data to confirm real-world location—critical for proving legal employment jurisdiction, avoiding regulatory fines, and preventing sanctioned individuals from slipping through.



For globally distributed teams, this is the difference between guessing and knowing.

Ongoing Identity and Location Assurance—Without New Tools

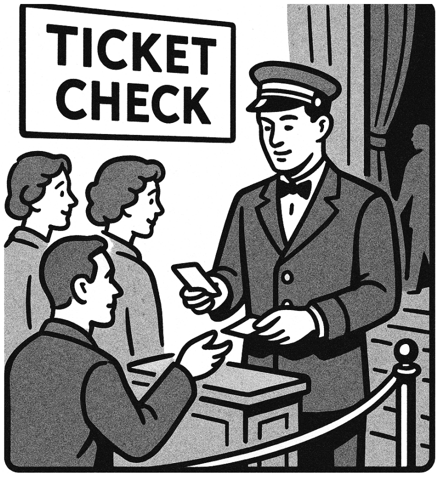
Once a worker is verified, Polyguard keeps verifying—silently, in the background. That means no new tools, no additional steps, and no separate systems to manage. You can confirm that remote workers are still who they say they are, and still where they claim to be.

This persistent validation helps reduce co-employment and misclassification risks—while staying completely invisible to IT.

Seamless Zoom Integration Means Less User Training

Polyguard plugs directly into Zoom. There's no new app for recruiters to learn, no accounts to manage, and no confusion for candidates. Installation is straightforward and IT doesn't need to own the onboarding process.

TA teams stay in their existing tools. You stay out of the support loop.



Bi-Directional Identity Verification: Stop Impersonators on Both Sides

Polyguard doesn't just confirm the identities of job candidates. It also verifies your own recruiters and hiring managers—so fraudsters can't impersonate your company in phishing scams. This protects job seekers from deception and protects your brand from being hijacked by criminals using fake job offers to steal personal data.

It's zero-trust, applied to the hiring process—on both sides of the call.

Built-In Helpdesk Reduces IT Load

Polyguard provides integrated support for both recruiters and applicants, resolving issues before they ever hit your helpdesk. That means fewer tickets, faster resolution, and more bandwidth for your IT team to focus on strategic work.

Business Records Affidavits Make Compliance Audit-Ready

After each verified meeting, Polyguard generates a **cryptographically signed Business Records Affidavit**—an immutable record of who was verified, when, how, and with what level of certainty. These affidavits can be exported for internal compliance, external audits, or legal inquiries.

They serve as real, reviewable evidence—so you're not relying on logs or screenshots to prove that a fraud check was done.

Conclusion: Polyguard Is Security That Starts Before the First Login

Most IT security tools start protecting your company after someone has access. Polyguard protects you **before** they get in the door—by stopping fraud at the interview stage. No backdoors. No gray areas. Just verified identity, right from the start.

Polyguard reduces exposure to impersonation, minimizes PII risk, and provides tools to verify every meeting, every time. It's the simplest way to help your TA teams move fast—**without cutting corners on trust or security.**

Empower hiring. Protect the business. Secure the perimeter where it starts.

Polyguard, the industry's first real-time defense against deepfakes and AI-powered fraud, delivers proactive protection against call spoofing, hijacking, and impersonation for voice, video, and messaging, in the call center and beyond.

Book a Demo

- **Email:** info@polyguard.ai
- **Phone:** (844) 671-0790
- **Web:** www.polyguard.ai