Jobma

MARKET RESEARCH

PART 2 OF 5

2027 Interview Fraud Prevention Report

Detecting Fraud Before the Interview

Part 2 of a 5-part series on AI, candidate fraud & trust in recruitment

Table of Contents

Part 2 of 5: Detecting Fraud Before the Interview

Introduction 1

Technologies That Detect and Prevent Hiring Fraud 1

Resume and Application Fraud Detection 2

Bot and Automated Submission Detection 3

Identity Verification 4

Conclusion 5

Jobma: Enabling Secure and Authentic Hiring 5

Continue the Series 6

Introduction

Understanding how hiring fraud works is only useful if you can catch it. Many of the tools to do so already exist. The challenge is applying them at the right points in the hiring process without slowing down genuine candidates.

This is Part 2 of Jobma's five-part 2027 Interview Fraud Prevention Report. It introduces the layered approach to fraud detection and covers the first three layers: the checks that happen early in the funnel, before a candidate is interviewed.

Technologies That Detect and Prevent Hiring Fraud

As AI's footprint becomes more prominent, a single verification method can't eliminate the vulnerability. Traditional hiring controls such as resume reviews, interviews, and reference checks remain important, but they were not designed to detect AI-generated applications, proxy interviews, identity manipulation, or real-time assessment assistance.

Modern hiring requires a layered approach that combines technology, process controls, and human oversight throughout the hiring lifecycle.

There's a need to implement verification checkpoints at multiple stages of recruitment, creating a continuous chain of trust from application submission through candidate onboarding. This approach not only improves candidate validation and evaluation consistency but also strengthens compliance, hiring quality, and confidence in hiring decisions.

To some extent, organizations already have parts of this infrastructure in place: 87.5% of our survey respondents reported using an ATS, 62.5% use background verification platforms, and 50% use skill assessment software or asynchronous or AI video interviewing platforms. Yet the tool stack does not necessarily translate into fraud readiness, particularly where controls need to operate during candidate evaluation.

Resume and Application Fraud Detection

Application verification tools analyze resumes, application forms, and candidate-submitted information for inconsistencies, anomalies, and indicators of potential misrepresentation. Rather than relying solely on manual recruiter review, these technologies use rules-based logic and AI-powered analysis to identify patterns that may warrant additional verification.

Technology/Method	How it works
Employment Timeline Inconsistencies	Detects overlapping positions, unexplained employment gaps, unrealistic career progression, or conflicting dates across resumes, applications, and external records.
Suspicious Career Progression Patterns	Flags unusually rapid promotions, role transitions that do not align with industry norms, or experience claims that appear disproportionate to a candidate's career history
Duplicate Application Detection	Compares resumes and application materials against previous submissions to identify reused content, duplicated profiles, or multiple applications originating from the same source.
AI-generated Applications Detection	Analyzes language patterns, formatting consistency, repetitive phrasing, and other indicators commonly associated with AI-generated content.
Qualification Verification	Identifies discrepancies between information provided across resumes, application forms, social profiles, certifications, or supporting documentation.

Rather than replacing recruiter judgment, platforms like Gem and Tofu provide risk indicators that help hiring teams prioritize reviews and focus verification efforts where concerns exist.

Bot and Automated Submission Detection

To address the challenges of high-volume, low-quality job applications, deploy technologies designed to identify automated application activity.

These systems may monitor:

Submission Velocity	Identifying candidates who submit unusually high numbers of applications within short periods of time, often indicating automated behavior
IP Address Patterns	Detecting multiple applications originating from the same network, geographic anomalies, or suspicious routing activity
Browser Fingerprints	Creating unique identifiers based on browser configurations, plugins, and device attributes to identify repeat activity across multiple applications
Repeated Applications	Identifying identical navigation patterns, form completion methods, or submission sequences commonly associated with bots and automation tools

Sardine and SEON include such controls to help organizations maintain application quality, reduce recruiter workload, and prevent automated activity from overwhelming recruitment systems.

Identity Verification

Identity verification technologies compare candidate-provided information against trusted documentation and verification sources to establish confidence that an applicant is who they claim to be.

Method	How it works
Government-issued ID Verification	It requires candidates to submit a photograph of an official identity document, such as a passport, national identity card, or driver's license.
Selfie-based Identity Verification	It requires candidates to capture a live selfie in real time that is compared against the photograph on the submitted identity document to confirm that the individual presenting the document is the legitimate owner of the credential.
Liveness Detection	It analyzes facial movements, expressions, and real-time interactions during the selfie capture process to verify that a real person is present and to reduce the risk of spoofing attempts using photographs, prerecorded videos, or synthetic media.

Identity verification helps organizations reduce the risk of impersonation, synthetic identities, and fraudulent candidate profiles progressing throughout the recruitment lifecycle. Jobma, Veriff, Entrust, Persona, etc., may provide combinations of document verification, biometric matching, and liveness detection capabilities.

Conclusion

Early-funnel checks set the tone for the rest of the hiring process. Application analysis surfaces inconsistent or AI-generated materials, bot detection keeps automated submissions from overwhelming recruiters, and identity verification confirms that applicants are who they claim to be.

None of these controls replaces recruiter judgment. They give hiring teams risk signals that help them prioritize their attention, so genuine candidates move forward quickly and questionable ones get a closer look.

But verifying an applicant at the start does not guarantee that the same person shows up to the interview, or that their answers are their own. Part 3 covers the controls that protect interviews, assessments, and credential checks.

Jobma: Enabling Secure and Authentic Hiring

Jobma's Layered Controls

Jobma helps enterprise organizations protect interview integrity, reduce candidate fraud risk, and create a more consistent, auditable hiring process across full-time and contingent labor - while seamlessly integrating with existing HCM, ATS, VMS, and enterprise workflows.

Verify

- Identity verification before the interview
- Secure candidate authentication
- Document and face matching with a selfie
- Liveness detection to confirm real-time presence

Proctor

- Proctoring and fraud deterrence during interviews
- Suspicious activity flags
- Multiple faces and environment indicators
- Tab or browser activity signals where applicable
- Candidate absence or unusual activity alerts

Evaluate

- Structured interview questions
- Scorecards and summarization
- AI-assisted scoring based on pre-set criteria
- Candidate comparison and stack ranking
- Reviewer notes and assessment results

Integrate

- Enterprise workflow integrations
- ATS, HCM, VMS, calendar, and collaboration tools
- Integration readiness with Oracle HCM, Beeline, and other enterprise hiring systems

Continue the Series

You've just read Part 2 of 5. Explore the rest of the 2027 Interview Fraud Prevention Report:

Part 1 The Growing Challenge of Hiring Fraud — Read Part 1 →

Part 3 Securing Interviews, Assessments & Credentials — Read Part 3 →

Part 4 AI, Candidate Experience & Real-World Impact — Read Part 4 →

Part 5 Survey Results: What Hiring Leaders Are Seeing — Read Part 5 →

About Jobma

Jobma is an intelligent, human-first hiring system. The platform promises innovative, compliant hiring solutions built to scale and deliver ROI through AI video interviewing, pre-hire skill assessments and candidate fraud prevention. Jobma is SOC 2 Type II and ISO/IEC 27001 certified, compliant with GDPR and CCPA, and aligned with the EU AI Act.

For more information about Jobma, visit www.jobma.com

Get in Touch

Sales Inquiries
sales@jobma.com

Customer Support
support@jobma.com

Phone
1-800-986-5620