Jobma

MARKET RESEARCH

PART 3 OF 5

2027 Interview Fraud Prevention Report

Securing Interviews, Assessments & Credentials

Part 3 of a 5-part series on AI, candidate fraud & trust in recruitment

Table of Contents

Part 3 of 5: Securing Interviews, Assessments & Credentials

Introduction	1
Interview Fraud Detection and Authentication	2
AI-Powered Fraud Detection and Proctoring	3
Assessment Validation and Integrity Monitoring	4
Employment Verification	5
Credential Verification	5
Conclusion	6
Jobma: Enabling Secure and Authentic Hiring	6
Continue the Series	7

Introduction

Much of hiring fraud surfaces at the moment a candidate is evaluated. A proxy can sit an interview, an AI tool can feed answers in real time, and a second screen can quietly turn a skills test into an open-book exercise. Controls applied during interviews and assessments are where many organizations have their biggest gaps.

This is Part 3 of Jobma's five-part 2027 Interview Fraud Prevention Report. It continues the layered detection framework introduced in Part 2, covering layers four through eight: the technologies that protect live and recorded interviews, online assessments, and the employment and credential claims candidates make.

Interview Fraud Detection and Authentication

Technologies that verify candidate authenticity and preserve interview integrity throughout the evaluation process include:

Technology/Method	How it works
Identity Continuity Verification	Helps ensure the individual participating in the interview is the same person who completed earlier verification steps and submitted the original application
Liveness Detection	Confirms that a real person is physically present during the interview rather than a static image, prerecorded video, virtual camera feed, or synthetic media presentation
Proxy Interview Detection	Identifies indicators that another individual may be participating in or completing the interview on behalf of the applicant
Mobile Device Detection	Flags the presence of smartphones, tablets, secondary screens, notes, or other materials that may facilitate unauthorized support during interviews
Browser & Desktop Activity Monitoring	Tracks activities like tab switching, application switching, copy-and-paste activity, and repeated access to external resources during interviews

These technologies help strengthen confidence that interview performance reflects the candidate's own knowledge, communication skills, and professional capabilities.

37.5% of respondents identified candidate impersonation and proxy interviews as a concern, while 50% cited AI-assisted cheating in remote interviews. At the same time, none of the respondents reported using candidate monitoring and proctoring tools, suggesting a gap between the risks teams recognize and the integrity-specific controls represented in their current toolsets.

This may be one of the clearest readiness gaps.

AI-Powered Fraud Detection and Proctoring

In addition to point-in-time verification technologies, use AI-powered fraud detection systems to monitor suspicious activities.

Technology	How it works
Automated Interview Proctoring	Monitors interview sessions for suspicious activity, such as the presence of additional individuals, off-screen glances, unauthorized device usage, and records potential integrity concerns for later review
Risk Scoring & Fraud Flagging	Aggregates indicators like identity verification results, liveness checks, proxy interview alerts, and browser activity patterns into an overall fraud risk assessment that recruiters can use to prioritize reviews
Response Pattern Analysis	Identifies factors, like answer timing and identity inconsistencies, that may suggest real-time AI assistance or externally generated responses
Audit Trailing	Creates detailed records of suspicious events, verification activities, and candidate performance throughout the interview process

Jobma provides hiring teams with additional visibility into candidate authenticity while maintaining human oversight in interviews.

Assessment Validation and Integrity Monitoring

As online assessments become a standard part of hiring, the following technologies help ensure assessment results accurately reflect a candidate's own skills and knowledge:

Technology/Method	How it works
Plagiarism Detection	Compares responses against internet sources, previous submissions, and proprietary databases to identify copied content
AI-generated Content Detection	analyzes responses for patterns that may indicate the use of generative AI tools like ChatGPT, Claude, Gemini, etc.
Unauthorized Assistance Detection	Identifies indicators of external help through collaboration tools, screen sharing, or off-camera support
Browser Lockdown	Restricts access to external websites, applications, and copy-and-paste functionality during assessments
Multi-device Detection	Flags the use of secondary devices that may be used to access unauthorized resources
Assessment Proctoring & Activity Monitoring	Tracks candidate device usage, navigation patterns, and suspicious activity throughout the assessment

These capabilities help organizations preserve assessment integrity and ensure hiring decisions are based on authentic candidate performance.

Employment Verification

Employment verification technologies confirm whether a candidate's work history accurately reflects their actual employment experience. These systems typically validate:

- Previous employers, by confirming that the mentioned organizations employed the candidate during the claimed time period.
- Job titles, by verifying whether the candidate held the position indicated on their resume or application.
- Employment dates, by validating start dates, end dates, and duration of employment.
- Professional references by collecting and verifying information from former managers, supervisors, or colleagues.
- Work history claims, by comparing the candidate-provided information against employer records to identify discrepancies or inaccuracies.

Automated employment verification helps recruiters validate career histories more efficiently while reducing the risk of hiring candidates based on fabricated experience.

Credential Verification

Checkr, Reveal, VerifiedFirst, etc., help confirm that candidates possess the qualifications, certifications, and licenses they claim. It validates:

- Educational qualifications by verifying degrees, diplomas, graduation dates, and academic records directly with educational institutions or trusted verification networks.
- Professional certifications by confirming certification status, issuing authority, expiration dates, and current standing.
- Occupational licenses by checking whether licenses remain active, valid, and in good standing with relevant regulatory bodies.
- Training credentials by validating completion of specialized training programs, industry courses, or professional development requirements.
- Memberships in professional organizations by confirming active membership status and participation in recognized industry associations.

Automated credential verification reduces reliance on manual checks and helps organizations identify fabricated, altered, or expired qualifications before hiring decisions are finalized.

Conclusion

Interviews and assessments are where hiring decisions are made, which makes them the point where fraud does the most damage. Identity continuity checks, liveness detection, proctoring, and activity monitoring help confirm that the person being evaluated is the person who applied, and that their performance is their own.

Employment and credential verification complete the picture by confirming that the experience and qualifications behind a candidacy are real. Together with the early-funnel checks covered in Part 2, these layers create a continuous chain of trust from application to offer.

Yet the technology that makes these safeguards possible also makes fraud easier. Part 4 examines AI's dual role in hiring fraud, and how to balance stronger safeguards with a fair, compliant candidate experience.

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 3 of 5. Explore the rest of the 2027 Interview Fraud Prevention Report:

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

Part 2 Detecting Fraud Before the Interview — Read Part 2 →

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