Jobma

MARKET RESEARCH

PART 1 OF 5

2027 Interview Fraud Prevention Report

The Growing Challenge of Hiring Fraud

Part 1 of a 5-part series on AI, candidate fraud & trust in recruitment

Table of Contents

Part 1 of 5: The Growing Challenge of Hiring Fraud

Introduction 1

Executive Summary 2

The Growing Challenge of Hiring Fraud 3

Emerging Types of Hiring Fraud 5

Conclusion 7

Jobma: Enabling Secure and Authentic Hiring 7

Continue the Series 8

Introduction

Hiring fraud used to mean an inflated job title or a degree nobody checked. Today it can mean an AI-written resume, a stand-in who sits the interview, or a cloned voice on a video call. Remote hiring, global talent sourcing, and widely available generative AI have changed what employers need to verify, and how quickly.

This is Part 1 of Jobma's five-part 2027 Interview Fraud Prevention Report. It sets the stage for the rest of the series: why hiring integrity has moved from a background HR concern to a business risk, what is driving the rise in candidate misrepresentation, and which types of fraud hiring teams are encountering most often.

Executive Summary

Over the last decade, hiring has evolved both in scale and structure, with teams growing globally. Organizations are sourcing talent across borders, conducting interviews asynchronously, and embedding AI into nearly every stage of the hiring lifecycle. These changes have expanded access to talent and improved efficiency, but they have also redefined how employers evaluate and validate candidates.

As hiring becomes increasingly digital, many of the traditional signals used to assess credibility, like face-to-face interaction, physical documentation, and direct verification, are no longer consistently available. In their place, organizations increasingly rely on digital channels, remote interactions, and automated systems to make hiring decisions. This shift requires a more deliberate approach to ensuring that candidate identity, experience, and demonstrated capabilities align with the role being filled.

Hiring integrity is no longer a peripheral concern. The impact of onboarding a candidate whose qualifications, identity, or capabilities cannot be fully validated can extend far beyond a hiring mismatch. It may affect workforce quality, operational performance, cyber security, regulatory compliance, customer trust, and employer brand credibility.

A Checkr survey found that 23% of organizations reported annual losses exceeding $50,000 due to hiring or identity fraud incidents, while approximately 10% reported losses above $100,000. As hiring workflows change, verifying candidate authenticity has become a non-negotiable.

Structural shifts that may be changing the hiring landscape:

- Remote and distributed hiring may reduce opportunities for direct identity verification and in-person validation.
- Generative AI can be used to produce highly convincing resumes, applications, portfolios, interview responses, and professional profiles.
- Deepfakes, voice cloning, and synthetic identity technologies are growing increasingly sophisticated and accessible.
- Automated application tools may enable candidates to target large numbers of employers simultaneously, overwhelming traditional screening processes.
- Global talent sourcing has expanded access to talent but may also pose greater complexity in verifying identities, credentials, employment histories, and qualifications across jurisdictions.

This report aims to equip HR leaders with a clear-eyed understanding of how hiring fraud is evolving and the strategies to navigate it so the hiring function stands strong. Our survey responses from hiring leaders and HR professionals reinforce that this is already tied to broader hiring outcomes: improving quality of hire was selected by all respondents as an on-going priority, while improving candidate experience and preventing interview and hiring fraud were each selected by 75%. Reducing time-to-hire was selected by 50%, suggesting that fraud prevention is increasingly being considered alongside quality, experience, and efficiency rather than as a separate security concern.

A Checkr survey found that 23% of organizations reported annual losses exceeding $50,000 due to hiring or identity fraud incidents, while approximately 10% reported losses above $100,000.

What this report covers:

- The structural forces driving the rise in hiring fraud
- Emerging fraud types - from AI-generated resumes and proxy interviews to deepfake impersonation
- Detection technologies deployed across the hiring funnel
- AI's dual role as both fraud enabler and line of defense
- Frameworks for secure, compliant, and equitable hiring

The Growing Challenge of Hiring Fraud

Historically, organizations were primarily concerned with resume inflation, inaccurate employment histories, or overstated qualifications. Today, hiring teams face a broader set of challenges driven by remote hiring, global talent acquisition, and the rapid adoption of artificial intelligence.

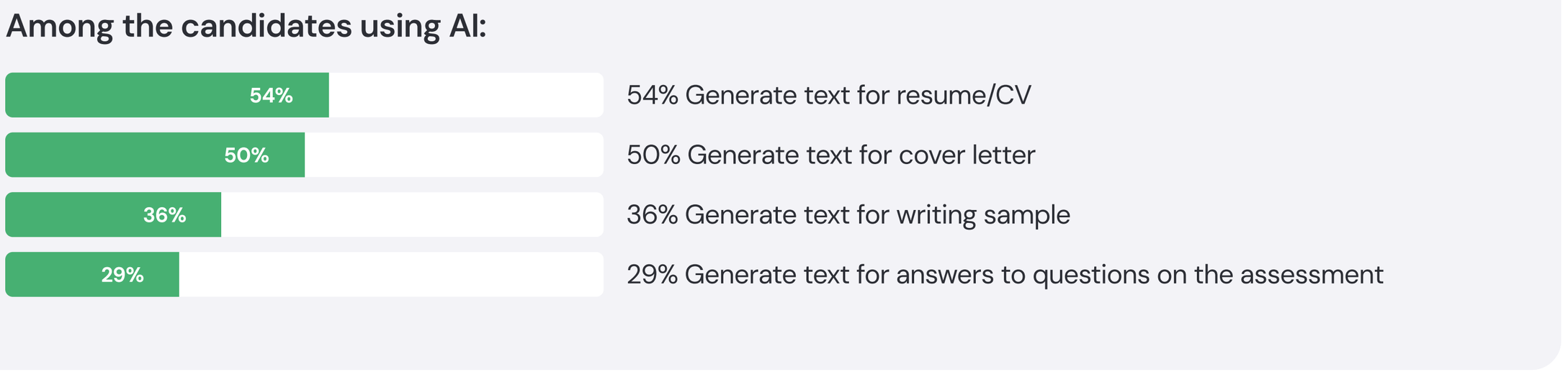
1. The Shift to Remote Hiring

Hiring has always involved a degree of uncertainty. Candidates naturally seek to present themselves in the strongest possible light, while employers make decisions based on the information available to them at a given moment. That dynamic is as old as the interview process itself. What has changed - rapidly and significantly - is the sophistication, scale, and ease with which candidate information and interview performance can now be enhanced, influenced, or misrepresented using emerging technologies.

As video interviews, asynchronous assessments, and distributed onboarding become standard practice, organizations gain access to a wider talent pool. While, by nature, remote hiring brings efficiency, it may also remove some of the in-person validation signals that hiring teams traditionally relied upon.

2. AI as an Accelerant

The growing accessibility of AI is also changing how candidates prepare for and participate in the hiring process. Tools that once required technical expertise are now available to anyone with an internet connection. Candidates can generate highly polished resumes in minutes, refine application materials, receive real-time interview assistance from AI, or, in more sophisticated cases, use synthetic methods to overstate their skills. 39% of candidates (roughly 4 in 10) have reported using AI during the application process. What was once relatively uncommon is becoming increasingly accessible, creating new challenges for hiring teams.



Source: Gartner

3. The Business Cost of Fraudulent Hires

SHRM places the cost of a bad hire at anywhere from 30% to over 200% of the role's annual salary, depending on seniority and function. When misrepresentation is the root cause, the costs compound further: potential legal exposure, data security risks, and the operational burden of restarting the search for the right candidate.

SHRM places the cost of a bad hire at anywhere from 30% to over 200% of the role's annual salary, depending on seniority and function.

4. Compliance and Regulatory Exposure

The compliance dimension adds another layer of urgency. In regulated industries – healthcare, finance, legal, and others – a misrepresented credential is not merely an HR problem. It can create liability that extends to clients, patients, and regulators. Organizations operating across multiple jurisdictions face the additional challenge of navigating inconsistent verification standards, creating gaps in visibility that can make applicant validation more difficult.

5. Traditional Hiring Methods Need New Layers of Validation

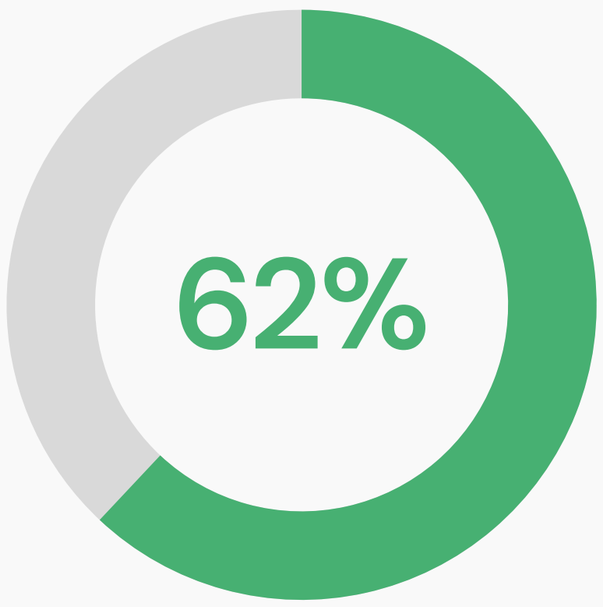
The methods candidates use to present information, complete assessments, and participate in interviews are evolving faster than conventional hiring processes were designed to handle. Resume review, panel interviews, and reference calls remain valuable components of hiring, but they were built for a different hiring environment. Organizations that rely solely on traditional hiring practices are, in many cases, operating without the visibility they need to make confident decisions.

The question for HR leaders and executive teams is not whether candidate authenticity and hiring integrity are concerns worth addressing. The more pressing question is whether the current hiring infrastructure is equipped to detect and deter fraud at the pace and scale that modern recruitment demands. In the survey, more than half of the respondents said they are more concerned about hiring fraud now than they were two years ago. More notably, 62.5% reported suspected incidents and another 12.5% reported at least one confirmed incident within the past 12 months, meaning 75% reported some level of recent fraud exposure.

Emerging Types of Hiring Fraud

According to Checkr's 2025 Hiring Hoax Survey of 3,000 hiring managers, 59% suspected candidates had used AI to misrepresent themselves during the hiring process, while 62% believed job seekers had become better at using AI to fake identities than employers were at detecting such deception.

Who is winning the AI fraud race—job seekers or employers?



Percentage of managers who say job seekers are now better at faking their identities using AI than employers are at detecting them.

Data from Checkr's proprietary survey of 3,000 American managers.

What once meant an inflated job title or an unverified degree now encompasses a far broader range of deceptive practices, many of them enabled by technology, and several that are difficult to detect through conventional hiring methods.

Skillfishing	Misrepresenting qualifications, experience, certifications, or skills through exaggerated, fabricated, or AI-generated applications and resumes.
Identity Fraud	Using altered, borrowed, or synthetic identities to participate in the hiring process or secure employment.
Proxy Interviews	Having another individual participate in or complete interviews and assessments on behalf of the actual candidate.
AI-Assisted Candidate Fraud	Using AI tools to generate interview responses, complete assessments, provide real-time coaching, or alter appearance and voice during hiring interactions.
External Assistance During Assessments	Receiving unauthorized support from third parties, secondary devices, hidden collaborators, or external resources during interviews and evaluations.

While these tactics differ in execution, they share a common characteristic: they reduce the reliability of the signals organizations use to assess candidate capability, authenticity, and fit. The survey reflects this across both familiar and emerging risks. Respondents selected resume misrepresentation as one of the top concerns (87.5%), followed by AI-assisted cheating in remote interviews at 50%. False credentials or certifications, candidate impersonation and proxy interviews, were cited each by 37.5%, while identity fraud and deepfakes were selected by 12.5%. The results suggest that hiring teams are not concerned only about sophisticated synthetic threats, but traditional forms of misrepresentation also remain prominent concerns.

According to CareerBuilder research, 74% of employers report having hired the wrong person for a position, with a single bad hire often costing thousands of dollars in recruiting expenses, onboarding investments, lost productivity, and replacement costs. As hiring becomes increasingly digital, identifying and mitigating these risks has become a critical component of hiring integrity.

According to CareerBuilder research, 74% of employers report having hired the wrong person for a position.

Conclusion

Hiring fraud is not a new problem, but the conditions around it have changed. Remote and asynchronous hiring removed many of the in-person signals employers once relied on, while generative AI made it faster and cheaper to produce convincing resumes, answers, and even identities.

The result is a broader set of risks, from familiar resume misrepresentation to proxy interviews and deepfake impersonation. Each one weakens the signals hiring teams use to judge capability and authenticity, and the cost of getting it wrong now reaches well beyond a single bad hire.

Recognizing the threat is the first step. Part 2 looks at what organizations can do about it, starting with the technologies that detect fraud before a candidate ever reaches the interview.

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

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

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