Combating Fake Resumes and Interview Fraud

A Strategic White Paper for Employers and Hiring Managers
January 2026

EliteTechnical®
Innovation, Technology and Talented People.
CELEBRATING 33 YEARS IN BUSINESS

Executive Summary

The rise of digital hiring platforms, remote interviewing, and flexible workplaces has opened the door to a growing problem: fake resumes and fraudulent interviews. Using exaggerated credentials and fabricated work histories, a plethora of candidates now engage in résumé fraud – which undermines hiring integrity, damages organizational trust, and increases the likelihood and cost of employee turnover.

This white paper explores the scope and implications of the fake resume problem, while presenting actionable strategies employers can adopt to detect and prevent fraud-related hiring mistakes.

Introduction

Résumé fraud is the intentional misrepresentation of one's qualifications, experience, or credentials on a job application. The rise of remote hiring practices, digital tools, and competitive job environments have brewed a perfect storm in which fraud activities amplify business risks for employers. This pervasive and detrimental crime may result in substantial, measurable business losses, legal risks, and damage to business reputations and organizational cultures.

Résumé and Interview Fraud

Instances of résumé fraud may incorporate embellished skills and exaggerated responsibilities; falsified employment history; fabricated references, academic credentials, altered transcripts, and forged documents; AI-generated or plagiarized content.

Further, the proliferation of online interviews and artificial intelligence enables unethical individuals to utilize a "deepfake" proxy – another person or AI-generated avatar posing as the candidate during interviews and tests. Deepfakes typically blend lies with generative AI to provide simulated images, videos and/or code that makes it more difficult for recruiters to discern inconsistencies.

Serious consequences of résumé and interview fraud may include unintended hiring of unqualified, unethical candidates, potential data breaches, and security threats in the event that fraudsters gain access to sensitive systems. In addition, when bad hires become public knowledge, organizations may suffer public scandal, loss of shareholder trust, and reputational damage.

Case in Point

Take for instance, the case of Dr. Michael Swango. Beginning as early as 1984, Dr. Swango repeatedly falsified credentials to conceal a checkered academic past, a fraudulent employment history, and criminal convictions. His ability to scam the system enabled him to secure a series of positions in university settings, laboratories, emergency medical services, and hospitals in the United States and Africa.

In 1993, using forged credentials, the fraudster secured a position with the Stony Brook University Hospital Department of Psychiatry, and rotated at the Veterans Affairs Medical Center in Northport, NY, before coming under investigation for a series of patient murders – then escaping prosecution until 2000.

This disastrous hiring scenario resulted not only in multiple patient and colleague deaths, but also led to adverse business and professional consequences: amid the clamor, both the dean of medicine and director of psychiatry at Stony Brook submitted their resignations; University Hospital also suffered a hotbed of negative press that required rapid and intense crisis communication as well as changes to hiring policy and procedure.

Reportedly, the FBI believes that Dr. Swango may have been "responsible for as many as 60 deaths, which would have made him one of the most prolific killers in American history," all while defrauding numerous well-respected institutions.[1] While this true example is extreme, it delineates the serious potential and consequences of overlooking résumé fraud.

Problem Scope

- 44% of job seekers admitted to lying during the hiring process, with 24% specifically falsifying their résumés.[2]
- 85% of hiring managers report catching lies on résumés**,** yet résumé fraud still costs U.S. businesses an estimated and staggering $600 billion annually**.** [3]
- 59% of hiring managers suspect candidates of using AI tools, such as résumé generators or interview assistants, to misrepresent themselves.[4]
- 60% of managers uncovered candidates who misrepresented their experience or qualifications**,** while another 13% suspected deception but couldn't prove it.
- 35% of managers say someone other than the applicant participated in a virtual interview, indicating identity fraud. [5]

At left: **Manager Reports of AI-Driven Resume Fraud in Technical Hiring (2020–2025),** especially in software engineering and remote-first roles. *Source: Checkr*

Industry	% Of Hiring Managers Reporting Résumé Fraud
Software Engineering	68% (npaworldwide.com)
Cybersecurity	64% (npaworldwide.com)
Data Science / AI	59% (checkr.com)
IT Support / DevOps	52% (checkr.com)
Product Management	47% (checkr.com)

And it gets worse from there: Gartner, a leading research firm, predicts that by 2028, one in four global job candidates could be fake, driven by the accessibility of generative AI.

Résumé Fraud: A Growing Business Epidemic

The following statistics reveal the expansion of résumé fraud and its changing impact on business today.

- In 2020/2021, résumé fraud mostly involved exaggerated skills or experience.
- By 2022, AI-generated résumés and cover letters began to surface.
- In 2023, deepfake interviews and voice manipulation emerged.
- The problem of identify fraud surged in 2024, with 31% of managers reporting fake candidates were identified in tech interviews.[6]

Of note, 62% of hiring professionals believe job seekers are now better at faking their identities with the help of AI than HR teams are at detecting deceptions.

Risks and Financial Implications

The cost of résumé fraud is staggering. A survey of more than 3,000 hiring managers conducted by Checkr, indicated that: "Nearly one in four respondents (23%) estimate their company lost more than $50,000 to hiring fraud in the past year while another 18% believe the annual cost ranged between $10,000 and $50,000. An additional 10% reported losses exceeding $100,000. The actual costs are likely even higher when factoring in lost productivity, delayed projects, and the cost of rehiring."

Organizational Risks and Challenges

Plagued by Intentional misrepresentation of skills and qualifications, fabricated credentials and work experience and fake references – in addition to "deepfake" interviews hiring managers are increasingly challenged to discern unethical and unqualified candidates**.**

Risking bad hires opens employers to potential legal, security and reputational nightmares, such as:

- Productivity losses, low team morale, and costly turnover.
- Security risks when unqualified individuals are placed in sensitive roles.
- Legal liability when misrepresentation leads to business and/or personal harm.
- Reputational damage when hiring failures and subsequent mishaps are publicized.

A report by CrossHQ indicates that, "The real crisis isn't just the prevalence of deception—it's the fundamental inadequacy of our verification systems in an era where AI can generate convincing falsifications in minutes." Think avatars, photo cloning and/or voice cloning.

Countering this problem is critical!

Résumé fraud prevention is an evolving discipline that requires continuous investment in tools, training, and talent. Reducing opportunities for candidates to scam employers is the first line of defense. Thus, watching for overly polished résumés, inconsistencies, and/or unexplained gaps in employment history, and vagueness is a logical first step when screening candidates, but way more is needed in today's digital hiring environment.

Current best fraud-prevention practices combine training in anti-fraud measures across all departments and hiring levels with standardized, consistent, and thorough screening processes

Current Fraud Prevention Tools

Adoption of specific AI tools designed to help qualify candidates and detect potential fraud can mitigate employer risk by spotting fake credentials, fabricated work histories, and AI-generated résumés – faster and more effectively. Tools, such as *Tofu AI Résumé and Fraud Detection*, help flag suspicious profiles using data-driven techniques that validate applicants along billions of data points that help detect the hidden patterns revealing fake résumés.[7]

Other fraud detection tools include: Voice stress analyzers and AI interview monitoring platforms that track eye movement and hesitation, and flag suspicious behavior. In addition, new block-chain based credentialing programs, such as Ethereum and HyperLedger, can help prevent credential tampering. Platforms such as Truework and Learning Machine allow institutions to issue verified digital credentials that employers can instantly validate.

Current AI-powered résumé screening tools utilize machine learning and Natural Language Processing models to detect

patterns of deception and inconsistencies by identifying exaggerated language, suspicious phrasing, or overuse of buzzwords. In addition, AI tools also can provide cross-evidence verification by comparing résumé claims against public records, social media, and professional databases. These tools also offer deepfake detection by flagging facial movements and voice patterns indicative of impersonation. Specific AI firms, such as Strider Intel, also screen for falsified résumés linked to insider threats and potential existential threats posed by nation-state actors.

In addition to use of AI tools, detailed video interviews by savvy recruiters and hiring managers can detect proxy candidates – sometimes by noticing unnatural blinking or lip-sync mismatches during video calls and by asking highly specific questions to uncover résumé distortions. *When in doubt, opt out!* Further skill analysis may be conducted by an outsource team, such as e-Teki, which offers consultant interviewers skilled in technical skill evaluation.

Regardless of which AI models and interview strategies organizations employ to guard against fraud, employers must prioritize background and verification checks in order to flag inconsistencies and confirm claims and details, such as whether a candidate actually held a specific position with a particular employer. They also must carefully scrutinize and compare identification, such as driver's licenses, passports, visas, and other documentation.

Further, implementing a zero-tolerance policy for unethical behavior is essential! Today's companies must consistently communicate expectations regarding candidate integrity. It is essential to clearly articulate potential legal and reputational consequences – not only to hiring teams but to candidates themselves.

"Incorporating identity verification into early-stage workflows (such as applicant tracking and scheduling software) can reduce the risk of deception before interviews even begin. Above all, building institutional confidence requires aligning people, policies, and technology toward a common fraud-prevention strategy."[8]

Elite Technical's Strategic Approach to Fraud Prevention

Elite Technical is a staffing and recruiting firm with a 33-year history of rigorous compliance and accountability across its organization. The firm's proactive Fraud Risk Management and Anti-Corruption Policy focuses on the obligations of company principals and employees to consciously avoid and notice signs of actual or potential fraud, misconduct, noncompliance, malpractice, and corruption across all business areas. In addition, interdisciplinary team training - particularly for recruiters and account managers - also focuses on résumé and interview fraud prevention.

Communicating high expectations for ethical behavior and rigid compliance across organizations is essential.

Elite Technical requires all employees to guard against fraud. Employees are urged to conduct open and transparent communication regarding any suspicion or proof of fraud without fear of reprisal. Employees also are expected to report any apparent discrepancies in time, accounting, and financial reports.

The firm prioritizes honesty, integrity, and compliance as central to reputation management, and its fraud management and corruption mitigation program starts before hiring. Elite Technical's policy is to hire only individuals who demonstrate targeted ethical characteristics and reliability – and who have been rigorously vetted as a trustworthy fit for the corporate culture.

The firm fosters an organizational culture with zero tolerance for fraudulent behavior and/or transactions. Thus, hiring protocols require exacting precision during skill-based and behavioral interviews, as well as background and reference checks. The firm also procures security clearances when appropriate. Only individuals who meet Elite Technical's high standards are submitted, along with a detailed candidate summary, for client consideration. Elite Technical also uses e-Verify to validate each candidate's eligibility for employment in the United States and provides each client with the candidate's Right-to-Represent agreement, utilizing Elite Technical's proprietary SubmittalCheckTM platform.

Further, Elite Technical requires all employees to adhere to company policy and procedures, process management, and to produce accurate reporting across their business area.

Having provided carefully vetted technical professionals to more than 400 leading companies across the United States, the firm's recruiters go beyond evaluating education backgrounds and certifications. They also engage candidates in multiple detailed interviews to assess how well the individual articulates specific examples of actual skill and workplace experience.

All candidates undergo video screening with deep drilldowns on skills and specific questions that elucidate the candidate's ability to explain relevant information.

The Importance of Subject Matter Experts

Elite Technical ensures that interviews are conducted by subject matter experts (SME) in a team environment that includes recruiters with prior in-the-trenches technology experience. SME input enables recruiters to better detect exaggerated claims. In addition, video screening provides visual cues that allow recruiters to judge whether people really know their job, *(Are they googling for answers while on the call?!)* and to determine whether candidates circle around prepared talking points rather than provide direct answers.

To separate pretenders from qualified candidates, Elite Technical recruiters evaluate how well candidates explain themselves and demonstrate real experiences**.** *Can they appropriately detail exact features and actual responsibilities? Can they explain their levels of involvement on different projects, or do they end up going round and round without demonstrating evidence?*
Recruiters also utilize screen sharing to verify the candidate's location during video interviews with Google Maps. In addition to background / verification checks, they also research LinkedIn and other social media profiles - comparing résumés received to the candidate's online presence. In addition, **the firm requires government-issued photo ID** to validate candidate identity by matching the person interviewed to their ID during the live interview.

Reiterating concerns about candidate fraud, Jeff Keller, Elite Technical's Director of IT Staff Augmentation Programs, revealed that approximately 40% of driver's licenses submitted with candidate applications show signs of possible falsification. This further demonstrates the need for scrupulous attention to detail and uncompromising efforts to detect fraud at every touch point.

Recommendations and Conclusions

Résumé and interview fraud have reached epidemic proportion, and it is time for society to acknowledge the practice as criminal, rather than simply a nuisance.

To combat the growing incidence of résumé fraud and deceptive interview practices, organizations must:

- Employ structured best practices that blend advanced technology, including proven AI tools, with human oversight.
- Institute consistent training on the most current tools for résumé and interview fraud detection.
- Demand high standards of excellence and integrity throughout the hiring process.
- Implement careful detail-driven assessments and interview protocols for evaluating, skill, predicting behavior, and unmasking unscrupulous candidates.
- Adopt a zero-tolerance policy for individuals who perpetrate or facilitate candidate misrepresentation.
- Work together to develop legal and social sanctions capable of discouraging fraud.
- Develop and participate in an industry-wide clearinghouse of candidates who commit resume fraud.

Without rigorous anti-fraud efforts, organizations will increasingly risk financial losses, legal liability, and reputational damage. Robust interviewing and verification strategies shall remain increasingly important for ensuring ethical hires, cultural integrity, and organizational security. Thus, when hiring, follow the rigorous anti-fraud practices adopted by Elite Technical and remain hypervigilant with resume review and interview protocols. Finally, Organizations that invest wisely in fraud prevention will ultimately save money, ensure stronger teams, and enhance brand integrity.

References

Disclaimer: *This report is provided for informational purposes only, and while it may reveal the author's opinion, it should not be construed as legal advice. Elite Technical assumes no liability, legal or otherwise, for information within. When implementing policies and procedures for your own organization, be sure to seek professional legal and business counsel. Data presented in this report was compiled, in part, with AI assistance from Microsoft® Copilot and other Internet tools.*

1. **Wiki.** "*Michael Swango."* Wikipedia. https://en.wikipedia.org/wiki/Michael_Swango

2. **Resume Builder.** (January 28, 2025) *"1 in 4 Americans Have Lied on their Resume and Many Say It Helped their Careers."* Resume Builder. https://www.resumebuilder.com/resume-examples/1-4-americans-have-lied-on-their-resume/

3. **Ko, Mark.** *"Résumé Fraud: The $600 Billion Crisis Transforming How Organizations Verify Talent in 2025."* Crosschq. https://www.crosschq.com/blog/resume-fraud-the-600-billion-crisis-transforming-how-organizations-verify-talent-in-2025

4. **Patterson, David.** *"The Hiring Hoax: What 3000 Managers Revealed about AI & Identify Fraud in 2025.* Checkr Resources. https://checkr.com/resources/articles/hiring-hoax-manager-survey-2025 (September 16, 2025)

5. **Patterson, David.** *"The Hiring Hoax: What 3000 Managers Revealed about AI & Identify Fraud in 2025.* Checkr Resources. https://checkr.com/resources/articles/hiring-hoax-manager-survey-2025 (September 16, 2025)

6. **Patterson, David.** *"The Hiring Hoax: What 3000 Managers Revealed about AI & Identify Fraud in 2025.* Checkr Resources. https://checkr.com/resources/articles/hiring-hoax-manager-survey-2025 (September 16, 2025)

7. **Tofu AI Fraud Detection.** HireTofu.com https://hiretofu.com/resume-fraud-detection

8. **Patterson, David.** *"The Hiring Hoax: What 3000 Managers Revealed about AI & Identify Fraud in 2025.* Checkr Resources. https://checkr.com/resources/articles/hiring-hoax-manager-survey-2025 (September 16, 2025)