CONFIDENTIAL

Resume Screening Report

REPORT ID	DATE	CANDIDATE
RSA-A083ADDA	April 28, 2026	N/A

HIGH RISK FLAG

Recommended Action: Escalate - Multiple fraud signals detected

Resume Screening Report

Automated analysis and verification of candidate resume

REPORT ID	DATE	CLASSIFICATION	CANDIDATE
RSA-A083ADDA	April 28, 2026	CONFIDENTIAL	N/A

100
RISK SCORE

HIGH RISK FLAG

If this candidate is fraudulent, the estimated cost to your organization is $14,900 (based on role level and industry averages).
AI Probability: Medium | Confidence: Medium | Consistency: 15/100

Limited web presence for claimed employers

This resume contains multiple critical technology timeline fabrications that are factually impossible. Istio deployment in June 2015 predates the project's May 2017 public announcement by 2 years - Istio did not exist in 2015. Kubernetes rollout in 2011 predates the June 2014 open-source release by 3 years. BGP-EVPN deployment in 2003 predates RFC 7432 ratification in 2015 by 12 years. These are not estimation errors - they represent claims of deploying technologies before they existed. The metadata shows creator=Microsoft Word but producer=ReportLab (Python PDF library), indicating programmatic generation inconsistent with stated authorship. Claims 22 peer-reviewed papers but lists only 3. Pattern of extreme superlatives (industry-first, world's first) and round-number metrics ($47M, $23.4M) across all roles suggests template-based fabrication.

RECOMMENDED ACTION

Escalate

Multiple fraud signals detected

Summary: 5 CRITICAL 4 HIGH 3 MODERATE - 3 consistency flags, 1/6 checks passed

Score Pipeline: Raw 73 | Adjusted 100 | Final 100

HIGH RISK FLAG

Confidence: 69%

- Five or more fabricated claims detected.
- Composite risk score is at or above 71 (high-risk band).
- Some claims could not be found in the resume text.
- At least one critical flag raised by the LLM analysis.
- A single risk dimension scored high while employment links remained unverified.
- PDF metadata indicates an automated resume builder or headless browser export.
- Resume claims experience with a tool before it was publicly released (see anachronisms list).

If flagged claims are resolved, projected risk score drops to **80** (removes: 5 hallucinated claim(s))

```
Rules triggered: many_hallucinated_claims, critical_risk_score, moderate_hallucination, critical_flag_present,
dimension_peak_unverified, metadata_programmatic, technology_anachronism
```

Risk Dimensions

Claims reducing mean time to detect security incidents from 197 days to 0.8 seconds. 197 days is the industry average breach discovery time (not MTTR), and 0.8 seconds is physically implausible for human incident response workflows. Consider asking: How did you measure the 197-day baseline and 0.8-second detection time for security incidents?

Language 99 13%

Professional summary contains verbatim phrases from experience bullets: 'quantum-resistant zero-trust', 'self-healing infrastructure', '99.9999% availability'. Summary should synthesize experience, not copy-paste exact terminology. Consider asking: Can you describe your quantum-resistant architecture work in your own words?

Authorship 70 13%

Career Logic 65 18%

Professional summary claims 22 peer-reviewed papers but Patents & Publications section lists only 3 papers. Discrepancy of 19 publications unexplained. Consider asking: Can you provide a complete list of your 22 peer-reviewed publications with DOI links or DBLP profile?

Metadata 60 15%

PDF creator field shows 'Microsoft Word' but producer field shows 'ReportLab PDF Library (opensource)' - a Python PDF generation library. This metadata mismatch indicates programmatic PDF generation, not manual Word authorship. Consider asking: How did you create this PDF resume, and why does the metadata show ReportLab rather than Word's native PDF export?

Timeline 50 18%

Claims Istio service mesh deployment in June 2015, nearly 2 years before Istio was publicly announced (May 2017). Istio did not exist in 2015. This is factually impossible. Consider asking: Can you provide documentation or architecture diagrams from your June 2015 Istio deployment?

CONFIRMED (SKILLS + EXPERIENCE)	UNCONFIRMED (SKILLS ONLY)	EXPERIENCE ONLY
AWS, Azure, GCP, Go, Python, C++, Java, TypeScript, PyTorch, TensorFlow, Kubernetes, Docker, Terraform, Vault, Istio, Cilium, eBPF, SOC 2, PCI DSS, HIPAA, ISO 27001, FedRAMP, GDPR	OCI, Alibaba Cloud, IBM Cloud, Tencent Cloud, Huawei Cloud, Yandex Cloud, Rust, Kotlin, Scala, Haskell, Erlang, Elixir, Zig, OCaml, Assembly, JAX, custom transformer architectures, RLHF pipelines, LLM alignment, mechanistic interpretability, TLA+, Coq, adversarial ML red-teaming, NIST 800-53 Rev5, SAMA CSF, CBUAE, SOX, HITRUST CSF, FISMA, ISO 27701	ML-based autoscaling, FinOps automation, disaster recovery architectures, quantum-resistant consensus protocols, autonomous SRE agents, formal verification pipelines

Key Findings 12

CRITICAL FAB TIMELINE CONSISTENCY

Timeline Consistency

> *"Engineered the first enterprise production deployment of Istio service mesh in June 2015, predating"*

Claims Istio service mesh deployment in June 2015, nearly 2 years before Istio was publicly announced (May 2017). Istio did not exist in 2015. This is factually impossible. Consider asking: Can you provide documentation or architecture diagrams from your June 2015 Istio deployment?

CRITICAL FAB TIMELINE CONSISTENCY

Timeline Consistency

> *"Led Fortune 100 cloud transformations including a full Kubernetes rollout for a major global bank in 2011"*

Claims Kubernetes rollout for Fortune 100 bank in 2011, three years before Kubernetes was open-sourced (June 2014). Kubernetes did not exist outside Google in 2011. Consider asking: Which Fortune 100 bank deployed Kubernetes in 2011, and can you provide project documentation?

CRITICAL FAB TIMELINE CONSISTENCY

Timeline Consistency

> *"Led the transition from OSPF to BGP-EVPN fabric in 2003, 11 years before the RFC was ratified"*

Claims BGP-EVPN fabric transition in 2003, 12 years before RFC 7432 (BGP MPLS-Based Ethernet VPN) was ratified in 2015. Technology did not exist in standardized form in 2003. Consider asking: Can you describe the BGP-EVPN implementation you deployed in 2003, given that RFC 7432 was published in 2015?

CRITICAL EMB METRICS CREDIBILITY

Metrics Credibility

> *"reducing mean time to detect security incidents from 197 days to 0.8 seconds"*

Claims reducing mean time to detect security incidents from 197 days to 0.8 seconds. 197 days is the industry average breach discovery time (not MTTR), and 0.8 seconds is physically implausible for human incident response workflows. Consider asking: How did you measure the 197-day baseline and 0.8-second detection time for security incidents?

CRITICAL EMB METRICS CREDIBILITY

Metrics Credibility

> *"Saved $47,000,000 annually in cloud spend through proprietary ML-based autoscaling, while simultaneo"*

$47M annual savings claim at a 4-year-old company is extremely high and lacks baseline context. Claim is compounded by simultaneous 340% feature expansion. Consider asking: What was the baseline cloud spend before optimization, and how was the $47M savings calculated and verified?

HIGH FAB METADATA SIGNALS

Metadata Signals

> *"N/A - metadata discrepancy"*

PDF creator field shows 'Microsoft Word' but producer field shows 'ReportLab PDF Library (opensource)' - a Python PDF generation library. This metadata mismatch indicates programmatic PDF generation, not manual Word authorship. Consider asking: How did you create this PDF resume, and why does the metadata show ReportLab rather than Word's native PDF export?

HIGH EMB CAREER LOGIC

Career Logic

> *"Published researcher with 22 peer-reviewed papers"*

Professional summary claims 22 peer-reviewed papers but Patents & Publications section lists only 3 papers. Discrepancy of 19 publications unexplained. Consider asking: Can you provide a complete list of your 22 peer-reviewed publications with DOI links or DBLP profile?

HIGH EMB CAREER LOGIC

Career Logic

> *"AWS (all 400+ services), Azure, GCP, OCI, Alibaba Cloud, IBM Cloud, Tencent Cloud, Huawei Cloud"*

Skills section lists 87 technologies including claims of knowing 'all 400+ AWS services' and 9 cloud platforms. Skills breadth is implausibly comprehensive. 30+ skills listed but never demonstrated in experience bullets. Consider asking: Can you demonstrate working knowledge of Yandex Cloud, Huawei Cloud, and Alibaba Cloud services you've listed?

HIGH EMB METRICS CREDIBILITY

Metrics Credibility

> *"achieving 99.9999% availability (six nines) with sub-millisecond failover"*

Claims 99.9999% (six nines) availability - a reliability level typically achieved only by hyperscale cloud providers with massive redundancy. Most enterprise systems achieve 99.9-99.99%. Consider asking: Can you provide monitoring dashboards or SLA reports documenting 99.9999% availability over a sustained period?

MEDIUM EMB LANGUAGE PATTERNS

Language Patterns

> *"Architected quantum-resistant zero-trust frameworks... self-healing infrastructure achieving 99.9999%"*

Professional summary contains verbatim phrases from experience bullets: 'quantum-resistant zero-trust', 'self-healing infrastructure', '99.9999% availability'. Summary should synthesize experience, not copy-paste exact terminology. Consider asking: Can you describe your quantum-resistant architecture work in your own words?

MEDIUM EMB LANGUAGE PATTERNS

Language Patterns

> *"industry-first self-healing... world's first production deployment... Pioneered the world's first"*

Excessive use of superlatives across all roles: 'industry-first', 'world's first', 'pioneering', 'visionary', 'transformative'. Every role claims groundbreaking achievements. Pattern suggests template-based inflation. Consider asking: Can you describe a project where you were NOT the first or pioneering, and what you learned from it?

MEDIUM EMB METRICS CREDIBILITY

Metrics Credibility

> *"Reduced P1 incident rate by 99.4% (from 820 per year to 5 per year) while growing the platform from"*

Reduced P1 incidents by exactly 99.4% (from 820 to 5 per year) - suspiciously precise percentage while simultaneously growing from 120 to 1,400 services. 11x service growth typically increases incidents. Consider asking: What specific architectural changes enabled 99.4% incident reduction during 11x service growth?

Internal Consistency Checks

Check	Status	Finding
Dates vs Technology	FLAG	Three critical technology timeline impossibilities: Istio 2015 (public 2017), Kubernetes 2011 (OSS 2014), BGP-EVPN 2003 (RFC 2015). These technologies did not exist at claimed dates.
Metrics vs Role Scope	FLAG	Multiple extreme claims: $47M annual savings, 99.9999% availability, 0.8-second incident detection. Values exceed typical enterprise scale and lack proportional context.
Skills vs Experience	FLAG	87 technologies listed. Claims 'all 400+ AWS services' knowledge - implausible comprehensiveness. 30+ skills (Yandex Cloud, Huawei Cloud, Scala, Haskell, SAMA CSF, CBUAE, SOX) never demonstrated in experience bullets.
Titles vs Responsibilities	REVIEW	Progression from Senior Systems Engineer to Chief Technology Architect is logical and spans 24 years. However, responsibilities include multiple 'world's first' and 'industry-first' claims at every role.
Education vs Career	OK	PhD 2004 from ETH Zurich, career start 2001 aligns with graduate timeline. Education credentials match seniority level.
Seniority vs Writing	REVIEW	Writing quality matches executive level but shows template uniformity. Claims 22 peer-reviewed papers but lists only 3. Professional summary copies verbatim phrases from experience section.

Web Verification Results 5

Web verification confirms whether entities (companies, institutions) exist online. It does not confirm whether the candidate actually worked at or attended these organizations. Treat all results as indicators, not proof. Direct verification with employers and institutions is always required.

COMPANIES FOUND ONLINE	EMPLOYMENT LINKS FOUND	INSTITUTIONS FOUND
0 / 3	**0** / 2	**0** / 0

Query	What Was Checked	Status	Details	Source
OmniVantage Cybertech Holdings company official site	Company exists online?	UNVERIFIED	Search results show only similar-named companies in different industries: VantageRisk (insurance), Inovaantage (IT solutions), and Noventiq (IT services). None match 'OmniVantage Cybertech Holdings' exactly. No official website, LinkedIn company page, or Glassdoor presence found for this exact company name.	View
John Doe OmniVantage Cybertech Holdings employee	Person-company link found?	UNVERIFIED	Search results show a generic LinkedIn profile for 'john doe' with company listed as 'zz' in Singapore, not OmniVantage Cybertech Holdings. No connection found between this person and the claimed employer.	View
Helios Quantum Systems AG company official site	Company exists online?	UNVERIFIED	Search results show multiple different companies: Quantinuum (which has a product called 'Helios'), Quantum Systems (drone/robotics company), and Helios Technologies (hydraulics/electronics). None match 'Helios Quantum Systems AG' as a distinct company entity. The exact company name with 'AG' designation was not found.	View
John Doe Helios Quantum Systems AG employee	Person-company link found?	UNVERIFIED	Search results show a John Doe at 'ILB Helios Holding AG' (a solar energy company), not 'Helios Quantum Systems AG'. These are different companies in different industries. No employment connection found to the claimed quantum systems company.	View
Vertex Strategic Consulting company official site	Company exists online?	PARTIAL	Search results show multiple companies with similar names: Vertex Consulting Services (tax software), Vertex Strategy (tech consulting), vertex.consulting (digital transformation). Without additional context about location, industry focus, or founding date from the resume, cannot definitively confirm which entity matches the claimed employer or if 'Vertex Strategic Consulting' is a distinct company.	View

Company Web Presence

OmniVantage Cybertech Holdings - 0 sources searched.

Helios Quantum Systems AG - 10 sources searched.

Vertex Strategic Consulting - 10 sources searched.

Northwind Telecommunications Group - 10 sources searched.

LinkedIn: J. D. at OmniVantage Cybertech Holdings - 0 sources searched. Not found

LinkedIn: J. D. at Helios Quantum Systems AG - 0 sources searched. Not found

Institution Existence Check

ETH Zurich - Exists. ETH Zurich (education, CH) - 236484 publications indexed

Imperial College London - Exists. Imperial College London (education, GB) - 377016 publications indexed

University of Cambridge - Exists. University of Cambridge (education, GB) - 438763 publications indexed

Interview and Screening Guide

Personalized questions generated from this candidate's experience and flagged concerns. Questions are organized by priority and category.

Verification Questions Ask these first to address flagged concerns

P1

`Istio 2015 anachronism`

You claim to have deployed Istio in production in June 2015, nearly 2 years before the project was publicly announced in May 2017. Can you provide architecture diagrams, configuration files, or project documentation from this deployment?

P2

`Kubernetes 2011 anachronism`

Your resume states you led a Kubernetes rollout for a Fortune 100 bank in 2011, three years before Kubernetes was open-sourced. Which bank was this, and can you explain how you accessed Kubernetes before its public release?

P3

`BGP-EVPN 2003 anachronism`

You describe transitioning to BGP-EVPN in 2003, 12 years before RFC 7432 was ratified. Can you describe the BGP-EVPN implementation you used, given that the standard did not exist at that time?

P4

`0.8-second MTTR claim`

How did you measure and verify the reduction in mean time to detect security incidents from 197 days to 0.8 seconds? Can you walk through the detection workflow that achieves sub-second response?

P5

`$47M savings claim`

What was the baseline cloud spend before your $47M annual optimization, and how was this savings calculated and independently verified?

P6

`22 papers vs 3 listed`

Your professional summary claims 22 peer-reviewed papers, but only 3 are listed. Can you provide a complete publication list with DOI links or your DBLP/Google Scholar profile?

P7

`Metadata mismatch`

Can you explain why your PDF metadata shows 'creator: Microsoft Word' but 'producer: ReportLab PDF Library'? ReportLab is a Python PDF generation tool, not Word output.

P8

`Unconfirmed exotic cloud platforms`

You list experience with Yandex Cloud, Huawei Cloud, and Alibaba Cloud. Can you describe a specific project where you used each of these platforms?

P9

`Six nines availability`

Can you provide monitoring dashboards, SLA reports, or incident logs documenting 99.9999% (six nines) availability over a sustained period?

P10

`99.4% incident reduction`

You claim to have reduced P1 incidents by 99.4% while growing from 120 to 1,400 services. What specific architectural patterns enabled incident reduction during 11x service growth?

Role Fit

You mention architecting a self-healing quantum-resilient platform at OmniVantage processing 14.8M events/sec with 99.9999% availability across 47 regions. Walk me through the architecture decisions you made to achieve that level of availability—what were the top 3 failure modes you designed for?

Listen for: Specific technical trade-offs, concrete failure scenarios, evidence of hands-on architecture work vs. high-level oversight. Vague answers suggest the claim may be overstated.

At Helios Quantum Systems, you designed a multi-region Kubernetes platform across AWS, Azure, and GCP serving 2.8M concurrent users. How did you handle data consistency and failover between cloud providers, and what was your actual P99 latency in production?

Listen for: Details on cross-cloud networking, state management, and real observability data. Generic Kubernetes knowledge won't answer this.

You led a globally distributed engineering organization of 280 engineers across 12 time zones at OmniVantage. Describe your approach to on-call rotations, incident command, and knowledge sharing across that many people and time zones.

Listen for: Practical team management experience. Listen for specific tools, processes, and real examples of how they scaled communication and decision-making.

Your resume states you reduced mean time to detect security incidents from 197 days to 0.8 seconds at OmniVantage. What specific detection mechanisms, tools, or processes drove that improvement?

Listen for: Concrete technical implementation (SIEM, threat intel, behavioral analytics, etc.). A 246x improvement is extraordinary—they should be able to explain exactly what changed.

At Vertex Strategic Consulting, you mention orchestrating a full Kubernetes rollout for a major global bank in 2011 with 8,400 containerized workloads. Kubernetes 1.0 wasn't released until July 2015. Can you clarify what container orchestration platform you actually used in 2011?

Listen for: Honest correction or clarification. This is a factual inconsistency that needs resolution—they may mean a different technology or a different date.

Technical Depth

You claim to have pioneered the world's first production deployment of Cilium eBPF service mesh in January 2016, 2+ years before the public 1.0 GA release. What specific production workloads were you running on it, what challenges did you encounter, and how did you handle the lack of public documentation?

Listen for: Specific use cases, real operational challenges (performance, debugging, upgrades), and evidence of deep eBPF knowledge. Generic service mesh knowledge won't suffice.

You list 'custom transformer architectures, RLHF pipelines, LLM alignment, and mechanistic interpretability' under AI/ML skills. Describe a production system where you implemented one of these—what was the business problem, what did you build, and what were the results?

Listen for: Concrete project with measurable outcomes. If they can't name a specific system or only describe theory, this is likely resume padding.

You saved $47M annually in cloud spend at OmniVantage through 'proprietary ML-based autoscaling.' How did you measure that savings? What was your baseline, what metrics did you track, and how did you isolate the impact of autoscaling from other cost reduction efforts?

Listen for: Rigorous measurement methodology. Listen for attribution clarity—did they account for business growth, pricing changes, or other variables?

Your resume mentions formal verification using TLA+ and Coq under security skills. Describe a specific system you formally verified—what properties did you prove, how long did it take, and what bugs did it catch that testing missed?

Listen for: Real experience with formal methods, not just familiarity with the tools. Formal verification is specialized; they should have concrete examples.

You engineered the first enterprise production deployment of Istio service mesh in June 2015, predating the public project announcement by nearly 2 years. Were you working with an internal fork, or can you clarify the timeline? Istio's public announcement was in May 2017.

Listen for: Honest clarification or correction. This is another timeline inconsistency that needs resolution.

Behavioral

At Northwind Telecommunications, you operated a nationwide telco backbone serving 4.2M subscribers with 99.999% uptime. Tell me about a time when you were close to breaching that SLA—what happened, how did you respond, and what did you learn?

Listen for: Humility and learning from failure. Listen for specific incident details, their role in resolution, and systemic improvements made afterward.

You led 280 engineers across 12 time zones at OmniVantage and reduced P1 incidents by 99.4%. Walk me through how you built consensus on a major architectural decision when your team was distributed across multiple continents and potentially had conflicting opinions.

Listen for: Communication strategy, conflict resolution, and evidence of collaborative leadership. Did they listen to dissenting views? How did they handle disagreement?

At Vertex Strategic Consulting, you authored the firm's internal cloud security framework that was adopted across 62 engagements. How did you get buy-in from senior partners and teams who might have preferred their own approaches?

Listen for: Influence without authority, stakeholder management, and change management skills. Listen for evidence of persuasion vs. mandate.

You've held roles at four different companies over 25 years. Tell me about a time when you had to learn a completely new technology or domain quickly because the business needed it—how did you approach it?

Listen for: Growth mindset, learning velocity, and humility. Listen for specific examples and how they stayed current across such a long career.

Delivering simultaneous compliance certifications across SOC 2 Type II, PCI DSS, HIPAA, ISO 27001, FedRAMP High, SAMA CSF, and HITRUST CSF in 6 months is extremely ambitious. Describe a moment when you thought you wouldn't make it—what did you do?

Listen for: Stress management, prioritization under pressure, and team support. Listen for whether they took shortcuts or maintained quality.

Red Flags to Probe

Your resume lists mastery of 'all 400+ AWS services.' In reality, AWS has 200+ services. Can you clarify what you meant, and walk me through the 10 AWS services you use most frequently in your current role?

Listen for: Honest correction or clarification. This suggests either hyperbole or lack of precision. Listen for whether they can name and describe specific services in depth.

You list 14 programming languages and 8 cloud platforms. For each of the top 5 languages you've used, tell me the last production system you built with it and roughly when.

Listen for: Specificity and recency. If they can't name recent projects or if all examples are 10+ years old, this is likely resume padding.

Your education shows a Ph.D. from ETH Zurich in 2004, an M.Sc. from Imperial College in 2000, and a B.Sc. from Cambridge in 1998. That's three degrees in 6 years while working. Can you walk me through your timeline—were you studying full-time or part-time during any of these?

Listen for: Clarification on concurrent work and study. This timeline is tight but possible; listen for whether the explanation is coherent.

You hold 5 US patents, all issued between 2022 and 2024, and you've published 22 peer-reviewed papers. That's an extraordinary publication rate alongside a full-time executive role. How did you manage that workload, and who were your co-authors?

Listen for: Realistic explanation of how this was accomplished. Listen for whether they were primary authors or contributors, and whether they can discuss the research in depth.

Your resume mentions pioneering Cilium eBPF in January 2016 and Istio in June 2015, both predating public releases by 1-2 years. Were you working with pre-release versions, internal forks, or different projects? I want to understand the exact timeline.

Listen for: Honest clarification. These are significant claims that need verification. Listen for whether they can explain the relationship between their work and the public projects.

About This Report

METHODOLOGY

Each resume is analyzed across six weighted dimensions: Timeline Consistency (18%), Career Logic (18%), Metrics Credibility (18%), Language Quality (13%), Authorship Signals (13%), and Metadata Analysis (5%). Raw scores are combined using a weighted sum, then passed through Bayesian adjustment accounting for web verification results.

VERIFICATION

Automated web searches check whether claimed employers and institutions exist online (company websites, LinkedIn, Glassdoor, Crunchbase, academic databases). This confirms entity existence only - it does not confirm the candidate actually worked at or attended these organizations. UNVERIFIED status does not indicate fabrication. Direct contact with employers and institutions is required for definitive verification.

SCORING

Raw composite score passes through Bayesian adjustment. When employer verification fails or metadata signals programmatic generation, the adjustment increases the final score. Risk levels: Low (0-20), Moderate (21-45), Elevated (46-70), High (71-100).

FAIRNESS

Scoring includes bias mitigation for non-native English speakers and industries with limited web presence. This report is a screening aid, not a background check. All concerns should be verified through direct candidate communication.

Score Scale

Score	Risk Level	Interpretation	Recommended Action
0 - 20	Proceed	No significant concerns identified	Proceed with standard hiring process
21 - 45	Verify	Minor inconsistencies worth investigating	Ask targeted questions in the interview
46 - 70	Investigate	Notable concerns requiring direct verification	Contact references and employers directly
71 - 100	**Escalate**	**Serious concerns detected in multiple areas**	**Escalate to hiring manager before proceeding**

Equal Employment Opportunity - This screening tool analyzes resume document content only. It does not consider or evaluate protected characteristics including race, color, religion, sex, national origin, age, disability, or genetic information. Hiring decisions must comply with Title VII of the Civil Rights Act, ADA, ADEA, and applicable state and local laws. Always provide candidates an opportunity to explain flagged items before taking adverse action.

FCRA Notice - GetPruf is not a consumer reporting agency (CRA) as defined under the Fair Credit Reporting Act (FCRA). This report is not a consumer report. GetPruf analyzes resume document content and checks publicly available web sources for consistency verification. It does not provide employment verification, criminal background checks, credit reports, or identity verification services.

Disclaimer - This report is a screening aid, not a background check. Web verification confirms whether entities (companies, institutions) exist online - it does not confirm the candidate's specific claims of employment or enrollment. Social media profiles and education records found online may belong to a different person with the same name. A company not found online does not prove fabrication. Always verify concerns through direct contact with employers, institutions, and the candidate. No hiring decision should be made solely based on this report.

Fairness: Scoring is adjusted to reduce false positives for non-native English speakers and industries where companies typically have limited web presence.

References: Crosschq (2023) Reference Check Analytics; Loconte et al. (2022) Resume Fraud Detection Methods; Gartner (2025) Candidate Profile Fraud Forecast; Henle et al. (2019) Resume Fraud Taxonomy.