IIA NISQUALLY CHAPTER

Combating Fraud in Hiring

OSINT-Enhanced Verification & Document Authentication for HR and Fraud Examiners



Captain Ryan Durbin, D.B.A., CFE

YOUR PRESENTER

Ryan Durbin

CURRENT ROLE



HR Director
Washington State Patrol
Captain

CREDENTIALS



Doctor of Business Administration
Certified Fraud Examiner

SERVICE



21+ Years with WSP

- Criminal Investigation
- Training Division
- Special Operations
- Field Operations

ROADMAP

What We'll Cover

01 **The Threat Landscape**
Why hiring fraud now threatens public-safety agencies

02 **Fraud Typology & CFE Lens**
Risk tiers and the fraud triangle applied to recruitment

03 **Fortune 500 & Scale Cases**
Yahoo, RadioShack, Walmart, Nightingale, DPRK IT workers

04 **OSINT Verification Playbook**
Profiles, photo metadata, document authentication

05 **Red Flags, Guardrails & Rollout**
Escalation matrix, legal limits, takeaways

THE STAKES

Why Hiring Fraud Matters to Public Safety

When a credential is fabricated, the breach is not only financial — it is a breach of public trust.

Access & Authority

Public Servants and staff gain critical access to systems, accounts, and the public's personal data. A fraudulent hire is an insider threat from day one.

Public Trust Eroded

A bad hire who causes harm exposes the agency to liability and reputational damage no insurance fully covers.

AI Lowered the Barrier

Deepfake interviews, AI-generated resumes, and synthetic identities make fabrication cheap, fast, and scalable.

Background Checks Alone

Standard vendor checks verify the obvious. OSINT triangulation catches what a database lookup cannot.

DEFINITIONS

Hiring Fraud Risk Spectrum

LOW

Application / Resume

EXAMPLES

Exaggerated skills, padded dates

IMPACT

Mismatched hires, retraining cost

MED

Document

EXAMPLES

Fake diplomas, altered transcripts, bogus certifications

IMPACT

Compliance violations, liability

HIGH

Identity

EXAMPLES

Stolen PII, synthetic identities, criminal intent

IMPACT

Data breaches, insider threat

CRITICAL

Organized / State

EXAMPLES

Proxy interviews, deepfakes, laptop farms, cyber terrorism

IMPACT

National-security risk

LIVE AUDIENCE POLL

How confident are you that you could recognize potential fraud indicators during a hiring process?

- Not confident at all
- Not very confident
- Somewhat confident
- Very confident

SCAN TO VOTE

Use your phone camera to open Microsoft Forms or
Click Here to Vote

POLL SUMMARY

How confident are you that you could recognize potential fraud indicators during a hiring process?

- Only 31% of HR leaders say they have strong fraud-prevention controls
- 58–61% of organizations encountered hiring fraud in the past year
- 59% of managers suspected AI misuse
- 62% believe candidates are better at faking than teams are at detecting

VIEW LIVE RESULTS



See your results

THE CFE LENS

The Fraud Triangle Applied to Hiring

PRESSURE



Financial strain, desperation for a job, or coercion by an organized ring.

OPPORTUNITY



Weak verification — no degree check, no live video, no metadata review, ease of AI tools.

RATIONALIZATION



“Everyone pads their resume.” “The system is unfair.” Self-justification.

Examiner’s takeaway: We cannot eliminate pressure or rationalization — but we can close opportunity through layered, auditable verification.

LOW RISK, REAL COST

Meet Greg — The “Excel Wizard”

WHAT THE RESUME CLAIMED

- Advanced Excel — pivot tables, macros, VBA
- Enterprise forecasting systems
- 10+ years strategic reporting leadership
- MBA, top-tier business school

Hired into a $120K+ IT project-manager role.

A 5-minute degree verification could have stopped this.

POST-HIRE REALITY

- Week 1: “Where’s the Start menu in Excel?”
- Called pivot tables “those spinny chart things”
- Q2 forecast: Alabama $48 billion, California –$12
- Top region = “Test”
- School: no MBA record
- References: fabricated

LOW RISK, REAL COST

Meet Greg — The “Excel Wizard”



A 5-minute degree verification could have stopped this.

POST-HIRE REALITY



CASE STUDY 1 · FORTUNE 500

Yahoo — CEO Scott Thompson (2012)

4 mo	~$20M	0
Tenure before exit	Compensation forfeited	Independent credential checks

THE SCHEME

Official bio and SEC filings listed Computer Science (CS) degrees in accounting and computer science from Stonehill College.

- The CS degree did not exist
- Stonehill did not offer it until years after he graduated
- Exposed by an activist shareholder, not the board or search firm.

HOW OSINT WOULD HAVE CAUGHT IT

- Registrar call: only accounting degree confirmed
- SEC vs. earlier proxies: only accounting listed before
- Wayback Machine: false claim lived across prior employer bios
- One journalist's query to the registrar exposed the gap

CASE STUDY 2 · FORTUNE 500

RadioShack — CEO David Edmondson (2006)

Claimed theology and psychology degrees from a university he only briefly attended.

- The school had no record of either degree and never offered psychology
- Resigned within days; pled to a misdemeanor; 30 days jail
- Became a governance case study

CONTROL GAP → OSINT FIXES

Gap	Relied on self-reported education; no primary-source check.
Fix 1	Direct registrar verification — school confirmed no degrees.
Fix 2	National Student Clearinghouse degree-verify for every candidate.
Fix 3	Course-catalog archive: did the claimed program even exist then?

CASE STUDY 3 · FORTUNE 500

Walmart — VP David Tovar (2014)

Listed a bachelor's from the University of Delaware

- Post-hire review found a single-credit gap — the degree was never conferred
- Resigned from the world's largest retailer over an incomplete credential.

KEY LESSONS FOR EXAMINERS

1 Completion is binary

Enrollment ≠ degree. Verify conferral date.

2 Primary source before offer

Self-reported education triggers a check — always.

3 Trust roles need rigor

Communications & public-facing posts same standard as finance.

4 Document everything

Source, reviewer, date — auditable by design.

5 Consistent standard

Same process for every hire at a level = EEOC defense.

PATTERN ANALYSIS

What the Three Cases Share

Different companies, different decades — same root cause: reliance on self-attested credentials with no independent primary-source verification.

1 **No registrar / degree-verify**

Every case would have been caught by a 5-minute call or Clearinghouse query.

2 **Bio carried forward unchecked**

False claims lived across employers and SEC filings for years.

3 **Discovery came from outside**

Activist, journalist, newspaper — not the hiring organization.

4 **Vetting scaled to title, not risk**

C-suite sometimes skipped controls applied to entry-level staff.

CASE STUDY 4 · CREDENTIAL FRAUD AT SCALE

Operation Nightingale — Nursing Diploma Fraud

7,600+
Fake diplomas & transcripts

25
Individuals charged federally

5
States impacted

THE FRAUD CHAIN

1. Recruiters supplied bogus diplomas from real-sounding FL nursing schools
2. Holders sat for NCLEX using the fake credentials
3. Passing exam → state licensure that looked legitimate
4. Licensed “nurses” hired into direct patient-care roles
5. Break: coordinated HHS-OIG action across 5 states (Jan 2023)

CASE STUDY 5 · STATE-SPONSORED

North Korean IT-Worker Infiltration

DPRK operatives used forged/stolen U.S. IDs, proxy computers, and U.S.-based “laptop farms” to win remote IT jobs

- Wages funneled to Pyongyang in violation of sanctions
- One DOJ indictment: work from ≥64 U.S. companies
- Experts: hard to find a Fortune 500 that has not been hit.

Stolen IDs + forged docs	Verify against issuing authority; inspect metadata for tampering.
Laptop farms	Company laptops only via corporate VPN; flag remote-access tools.
Proxy interviews	Live video + random movement prompts; compare to gov ID photo.
IP / timezone anomalies	Log working hours & connection origins; investigate outliers.
Extortion after hire	Least privilege onboarding; monitor for data exfiltration.

CASE STUDY 6 · ORGANIZED

Job Impersonation Schemes

Scammers impersonate legitimate employers, collect SSNs, IDs, and financial data from applicants, then commit identity fraud

- USPS targeted at scale since 2019
- Average victim loss ~$3,000
- Additional attack: spoofed USPS payroll site stole credentials and redirected paychecks (460+ employees, >$1M).

CONTROL GAPS

- No training on official payroll access paths
- Weak screening for impersonation attempts
- Insufficient IT safeguards on employee portals

FIXES

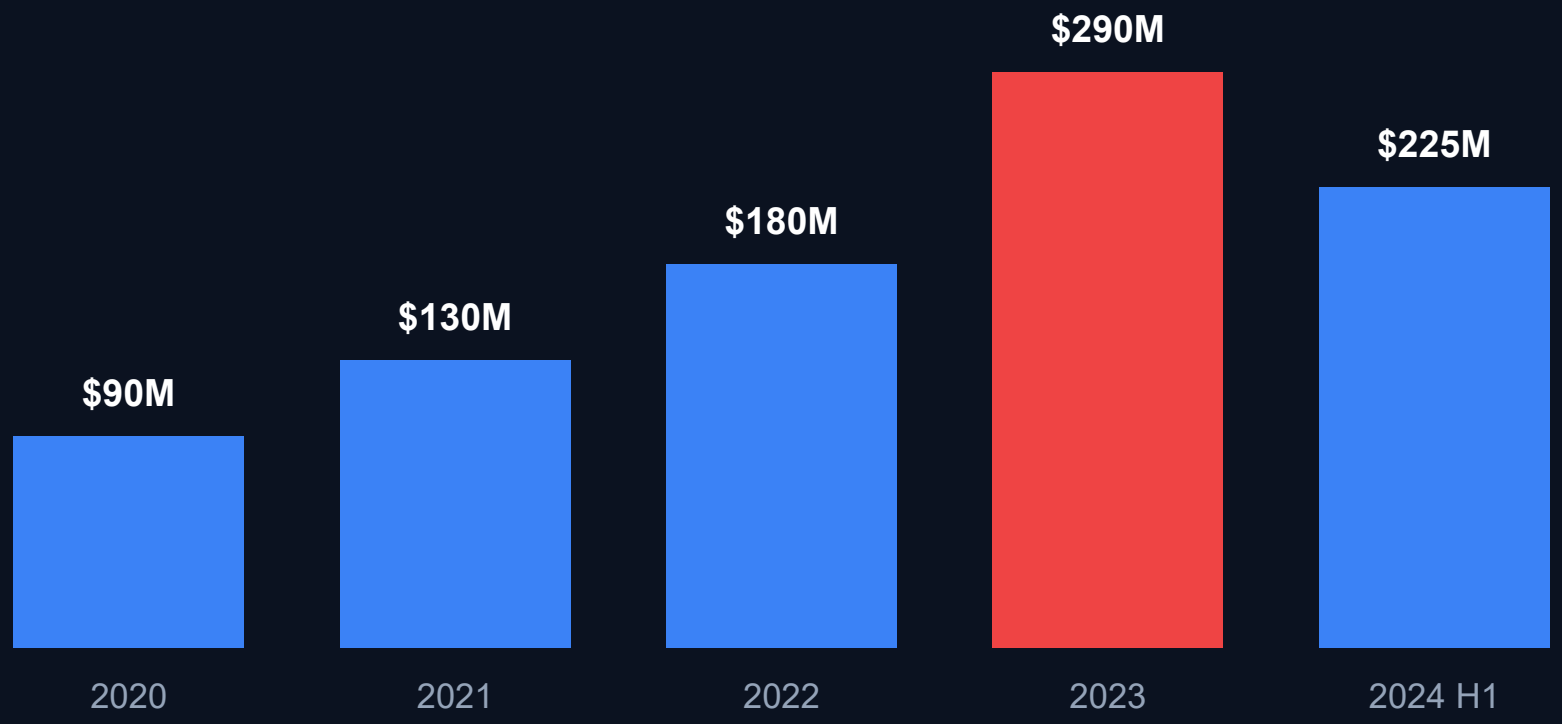
- Continuous search for impersonation domains/sites
- MFA on all payroll and sensitive employee resources
- Clear internal communication of official channels only





THE TREND LINE

Job-Scam Losses Are Climbing — AI Is Accelerating Them



AI MULTIPLIER

- AI resumes tuned to beat ATS filters
- Deepfake video for remote interviews
- Synthetic identities from stolen PII
- Automated parallel applications
- Lower cost = industrial scale

LIVE AUDIENCE POLL

Which part of the hiring process is most vulnerable to fraud?

- **A** Application screening
- **B** Reference checks
- **C** Background investigations
- **D** Interview panel decisions
- **E** Credential verification

SCAN TO VOTE

forms.cloud.microsoft/r/NADwbx5yM3

Use your phone camera to open Microsoft Forms

LIVE AUDIENCE POLL

Which part of the hiring process is most vulnerable to fraud?

- Background checks are the most common stage where fraud is detected
- Many fabrications are only found after hire or by outside parties
- Many Background checks fail to detect fraud
- Resume/credential fabrication ~36% of staffing organizations
- Document fraud ~32%.

View Results Here



TACTICS & DETECTION

Advanced AI & Deepfakes

Verify the camera

Virtual cameras often lack real EXIF (aperture, shutter, ISO, lens).

Restrict VPNs

Unexpected VPN/IP during interview is a red flag.

IP / timezone anomalies

Working hours and connection origin must match claim.

Use proctors

Trusted remote sites or live proctors for high-risk roles.



BEYOND THE BACKGROUND CHECK

The OSINT Verification Workflow

1 Capture

Save application, resume, IDs, docs as submitted — before any edits. Gather IP addresses from candidates

2 Verify Credentials

Registrar / Clearinghouse + license board + cert body.

3 Triangulate Identity

Name, photo, history across public profiles & records, metadata and geolocation.

4 Authenticate Docs

Metadata, EXIF, fonts, layers, template consistency.

5 Assess

Trained reviewer; HR sees only decision-relevant findings.

6 Decide & Log

Outcome, evidence, retention — fully auditable.

OSINT TECHNIQUE 1

Online Profile Triangulation

One profile is a claim. Three independent profiles that agree is evidence.

Professional profiles

LinkedIn tenure/titles vs. employer sites & Wayback Machine. Live bio vs. archived form = red flag.

Licensing & court records

State boards, UCC filings, court dockets — credentials, ownership, undisclosed litigation.

Publications & patents

Google Scholar, USPTO — claimed papers, patents, talks… or fabrications.

Employer corroboration

Press releases, staff directories, archived org charts — title and dates, not just company.

OSINT TECHNIQUE 2

Image & Document Authentication

Photo EXIF

GPS, timestamps, device, software. “Seattle” photo tagged overseas or edited in Photoshop = flag.

Reverse image search

Headshot on stock sites or dozens of fake accounts → synthetic identity.

PDF / doc metadata

Author, creation tool, edit history. “Scanned” diploma created in Word = fabrication.

Font & layer analysis

Mismatched fonts, raster text over vector, misaligned boxes = alteration.

Template consistency

Compare to known-good template for that institution and year.

Geolocation cross-check

EXIF GPS + landmarks + time zone vs. claimed residence and work history.

DECISION FRAMEWORK

Red Flags & Escalation Matrix

RED FLAG	ACTION	OWNER
Degree from unaccredited / closed school	Degree-verify + accreditation check	Background investigator
Photo on stock sites / many accounts	Reverse-image + ID comparison	OSINT reviewer
EXIF GPS/timezone contradicts claim	Request fresh geo-tagged photo	OSINT reviewer
Refuses live video / evades camera	Random movement prompts	Hiring mgr + security
Laptop routes via unexpected IP/VPN	Lock to corporate VPN; alert security	IT security
Doc metadata shows wrong authoring tool	Request certified official copy	Background investigator

NON-NEGOTIABLE

Legal & Ethical Guardrails

OSINT is powerful. Used carelessly, it creates legal exposure and harms candidates. These rules are absolute.

Consent & disclosure (FCRA)

Where OSINT feeds a decision, follow FCRA disclosure and consent for consumer reports.

Firewall protected-class data

Reviewers never surface race, religion, age, disability, family status. HR sees only job-relevant findings.

No pretexting or fake accounts

No impersonation, false profiles, or befriending under false pretenses. Public info only.

No standalone reliance on metadata

Metadata is a lead, not a verdict. Corroborate with primary sources before adverse action.

EEOC consistency

Same verification standard for every candidate at a given level.

Data minimization & retention

Collect only decision-relevant data. Retain per schedule, then dispose. Log access.

ACTION PLAN

How to Build a Stronger Process

CRAWL

Foundation



- Adopt verification checklist as policy
- Designate & train OSINT reviewers
- Stand up evidence-retention process
- Validate and Train processes

WALK

Build



- Integrate checks into ATS / onboarding
- Live-video protocol for remote hires
- Pilot on sample of recent hires
- Conduct adverse impact analysis

RUN

Scale & Audit



- Agency-wide rollout
- First quarterly audit of logged decisions
- Tune red-flag thresholds from real cases
- Set future review/revision dates

AUDIENCE POLL

After today’s session, how prepared do you feel to prevent, detect, and report hiring-related fraud?

- Still unsure
- Somewhat prepared
- Mostly prepared
- Fully prepared

CLOSING

Trust, but verify — consistently, legally, and auditable.



MY CONTACT CARD

The Fortune 500 cases prove that credentials unchecked will be credentials faked.
Layer OSINT on every background investigation, log every step, and protect both the agency and the candidate.

Captain Ryan Durbin, D.B.A., CFE · Washington State Patrol

Questions & discussion welcome