Securitas

WHITE PAPER

# Mistaking manufactured **credibility for genuine trust:**

## AI, Synthetic Identities & the Future of Risk Mitigation through Background Verification

2026-2027

WALSONS
BUILDING FAITH

# Executive Summary

What was once viewed as a routine verification process has become a strategic safeguard against hiring fraud, compliance and reputational risks. From foundational verification checks to comprehensive verification risk intelligence, background screening has undergone a significant transformation.


From AI-generated employment histories and deepfake interview candidates to proxy job applicants, synthetic professional identities, credential laundering networks, and manipulated digital footprints, hiring fraud has evolved faster than verification ecosystems themselves.

**While AI has strengthened recruitment efficiency and accelerated screening processes, it has simultaneously empowered fraudsters with tools capable of bypassing automated checks at scale. As organisations compete aggressively for talent in a borderless workforce economy, the ability to distinguish authentic professionals from digitally manufactured identities is becoming a critical business risk, not merely an HR concern.**

## This white paper explores:

# When Digital Credibility Becomes Easy To Manufacture

The hiring ecosystem has transformed dramatically over the past few years. Remote hiring, global talent mobility, AI-generated content, and digital onboarding have made recruitment faster and more scalable than ever before.

> However, the same technological advancements enabling efficient hiring have also enabled sophisticated fraud. Traditional fraud indicators such as forged educational certificates or fabricated references have evolved into complex deception models that mimic legitimate candidate behavior with alarming precision.
>
> **Diving in the core factors**


## 1. Deepfakes & Impersonation

A 2025 enterprise hiring survey found that

**31%** of hiring managers encountered fake candidates during recruitment cycles.

One of the fastest-growing threats in remote recruitment is deepfake-assisted interviewing.

- Live deepfake interview overlays
- AI voice modulation
- Proxy interview impersonation
- Post onboarding identity swaps

**The threat vector is especially severe across GCC ecosystems, technology staffing, offshore workforce deployment and privileged-access roles. Most facial recognition systems validate identity snapshots, not real-time behavioural authenticity. Sophisticated deepfakes can now replicate facial movement patterns convincingly enough to bypass standard detection thresholds.**

## 2. Synthetic Professional Identities

Synthetic identity fraud is no longer limited to financial ecosystems. It has entered recruitment aggressively. Fraudsters now combine.

| | | |
|---|---|---|
| Real government IDs | Fabricated employment histories | AI-generated references |
| Fake payroll records | Artificial LinkedIn engagement | Purchased endorsements & recommendations |

**The result is a candidate profile that appears digitally authentic and professionally credible across multiple verification systems. Because each data point appears legitimate in isolation, these synthetic identities often bypass automated screening frameworks undetected. The deception does not lie within isolated records; it exists in the carefully engineered narrative connecting them.**

## 3. AI Is Rewriting Professional Credibility

**59% of hiring managers suspected candidates of using AI tools to misrepresent skills, experience, or identity during hiring processes.**

Generative AI tools now allow candidates to create.

- Hyper-optimised resumes
- Technically convincing project descriptions
- Fabricated managerial experience
- Artificial career progression stories

Many candidates are also using AI tools during interviews to generate real-time responses. This makes traditional experience validation increasingly unreliable unless supported by deeper verification frameworks.

## 4. The Hidden Employee Behind The Hired Identity

Organisations are witnessing a sharp rise in proxy working fraud, where:

- One individual clears the interview while another joins the organisation
- Actual work is outsourced anonymously post-hiring
- Shared or manipulated identities operate across multiple employers simultaneously
- Candidates misrepresent real-time skills, location, or employment ownership

**This is increasingly prevalent across:**

| | |
|---|---|
| **Remote technology hiring** | **Contract & contingent staffing** |
| **Cross-border gig ecosystems** | **High-volume project-based deployments** |

Such fraud frequently remains undetected for extended periods, exposing organisations to operational, security, and compliance risks.

## 5. Credential Laundering Ecosystems

According to Gartner, by 2028, nearly **25%** of job applicants globally may have synthetically engineered or entirely fabricated identities. This fundamentally changes the role of modern verification.

> **Fraud is no longer opportunistic. It is operationalised.**

**Underground ecosystems now offer:**

- Hyper-optimised resumes
- Technically convincing project descriptions
- Fabricated managerial experience
- Artificial career progression stories

**In effect, fraudulent employability has become a service economy. In many cases, candidates now successfully pass automated screening tools, interview rounds, and onboarding stages and inconsistencies emerge months later, often after operational, financial, or reputational damage has already occurred.**

# Why Hiring Fraud Is Now An Enterprise Risk

**41%** of enterprises surveyed admitted to hiring and onboarding fraudulent candidates without realizing it.

## Operational Risk

Unqualified hires can disrupt productivity, execution quality, & business continuity.

## Cybersecurity & Insider Threats

Fraudulent identities may gain unauthorised access to sensitive systems, data, and financial infrastructure.

## Compliance & Regulatory Exposure

Weak due diligence can result in compliance breaches, contractual liabilities, and client trust erosion.

## Brand & Reputation Impact

Even a single fraudulent hire can damage organisational credibility, stakeholder confidence & market trust.

> Because in the age of artificial intelligence, the biggest hiring risk is no longer missing talent, **it is mistaking manufactured credibility for genuine trust.**

# The Trust Gap Inside Virtual Recruitment

## 62% of hiring managers believe candidates are now better at using AI to fake identities than organisations are at detecting them.

Remote hiring has fundamentally altered the modern risk environment. Traditional hiring naturally validated certain behavioural and identity markers through physical interaction. In digital-first hiring, authenticity has become significantly harder to assess than it was in the past.

| | | | |
|---|---|---|---|
| Identity is **virtual** | Communication is **curated** | Presence is **controlled** | Authenticity is **questionable** |

**Generative AI Tools Now Allow Candidates To Create:**

- Cross-border data limitations
- Inconsistent regulatory frameworks
- Varying documentation standards
- Fragmented identity databases

"Modern hiring fraud no longer exploits missing data alone; it exploits disconnected verification ecosystems."

# The Securitas Verification Risk Framework

At Securitas India, employee verification is approached as a strategic enterprise risk function rather than a transactional pre-employment process. Our approach is designed to help organisations build resilient employee ecosystems through:

Trust intelligence

Privacy-first verification frameworks

Compliance centric governance

Technology enabled due diligence

Further strengthening this commitment, Securitas India is registered as an Offline **Verification Seeking Entity (OVSE) with UIDAI, reinforcing our ability to support organisations with:**

- Enhanced identity assurance
- Faster verification outcomes
- Improved audit readiness
- Reduced operational complexity
- Stronger compliance and risk management

The following framework outlines key employee risk areas, and the measures organisations can adopt to strengthen trust across the employee lifecycle.

## ☑ Mitigating Identity Fraud & Synthetic Candidate Risks

### Risk Exposure

AI-generated profiles, synthetic identities, impersonation attempts, forged documents, and deepfake-enabled hiring fraud are making candidate authentication increasingly challenging.

### How Securitas India safeguards

By combining identity verification, document authentication, address validation, database screening, and digital authenticity assessments, organisations can establish stronger identity assurance at the point of hire.

### Business Impact

- Reduced onboarding of fraudulent candidates
- Stronger candidate authenticity validation
- Improved compliance and audit readiness
- Increased trust in workforce onboarding decisions

## ☑ Addressing Credential Manipulation & Misrepresentation

### Risk Exposure

Fabricated employment histories, inflated experience claims, falsified educational credentials, and undisclosed adverse records continue to create significant hiring risks.

## How Securitas India safeguards

Securitas India validates professional credibility through a source-led verification methodology that prioritises evidence over declarations. In addition to traditional verification checks, we leverage technology-driven intelligence to identify inconsistencies that may otherwise go unnoticed.

> As generative AI makes it easier to fabricate resumes, embellish experiences, and construct convincing professional narratives, **Securitas India** harnesses AI-driven intelligence to detect anomalies hidden within those same narratives. By analysing declared information for inconsistencies in skills, experience, timelines, and career trajectories, we help organizations distinguish genuine capability from manufactured credibility.

**The same technology that enables deception can also be used to expose it.**

Comprehensive employment, education, criminality, and professional reference verifications help validate candidate claims through trusted source-based verification methodologies.

## Business Impact

- Improved hiring accuracy
- Reduced risk of negligent hiring
- Enhanced workforce quality and reliability
- Better protection of organisational reputation

# ☑ Strengthening Trust in High-Risk Business-Critical Roles

## Risk Exposure

Not all positions present the same level of risk. Securitas India tailors' verification depth to the sensitivity, access, and potential impact of each role, helping organisations strengthen trust where it matters most.

### How Securitas India safeguards

Enhanced due diligence, integrity assessments, investigative research, adverse media intelligence, reputation risk analysis, and risk-based screening frameworks provide deeper visibility into potential exposure areas.

### Business Impact

- Stronger governance and control frameworks
- Reduced insider threat exposure
- Better protection of critical business assets
- Increased confidence in strategic hiring decisions

## ☑ Managing Verification Risk Beyond Onboarding

### Risk Exposure

Employee-related risks do not end after hiring. Compliance violations, identity anomalies, misconduct indicators, and emerging risk events can arise throughout the employee lifecycle.

### How Securitas India safeguards

Periodic screening programmes, continuous monitoring frameworks, and ongoing workforce risk assessments help organisations maintain trust long after onboarding.

### Business Impact

- Early identification of emerging risks
- Improved regulatory compliance
- Stronger workforce governance
- Sustained organisational trust

## ☑ Enhancing Digital Trust and Reputation Intelligence

### Risk Exposure

Today's workforce leaves a digital footprint that can reveal inconsistencies, undisclosed risks, or indicators of professional misrepresentation.

### How Securitas India safeguards

Digital footprint intelligence, adverse media screening, public domain reviews, and cross-platform identity assessments provide additional context beyond traditional verification checks.

## ☑ Enabling Faster, Smarter, & More Scalable Verification

### Risk Exposure

Global hiring demands faster turnaround times without compromising verification quality, compliance, or candidate experience

### How Securitas India safeguards

Technology-enabled verification workflows, automated case management, digital verification capabilities, and global screening expertise help streamline verification operations at scale.

### Business Impact

- Faster turnaround times (TATs)
- Reduced manual effort and operational friction
- Improved candidate experience
- Consistent, high-quality verification outcomes across geographies

Because in the era of synthetic employability, enterprises do not simply seek verification partners. **They need risk mitigation & intelligence partners.**

## The Securitas Advantage: Workforce risk intelligence in the AI Era

the future of verification is not choosing between speed and trust. It is achieving both through intelligent orchestration.

**While many providers verify records, Securitas help organizations verify trust!**

Securitas

**With Securitas India**
stay ahead of risks that
try to pass the test of scrutiny.

# Contact Us

For Domestic:

ev.screen@securitas-india.com

+91 9978 990 585

For International:

verify.global@securitas.in

+91 9319 585 385

WALSONS
BUILDING FAITH