MajorKey

Building Digital Trust: How IDProof+ Secures Remote Hiring, Contractor Access, and Call Centers

Identity assurance is no longer optional.

IN PARTNERSHIP WITH authID

INTRODUCTION

The way we work has changed forever.

Remote work, global hiring, and third-party partnerships have unlocked new opportunities, but also new vulnerabilities. Deepfake technology, proxy interviews, and social engineering attacks are no longer fringe threats; they're mainstream tactics costing businesses millions.

This eBook explores:

- Why identity assurance is now a frontline defense
- The risks organizations face across three critical use cases
- How IDProof+, developed by MajorKey in collaboration with authID and integrated with Microsoft Entra Verified ID, delivers the trust your business needs

Table of Contents

Copyright © 2025, MajorKey Technologies. All rights reserved.

PART ONE: THE NEW REALITY

A Diverse, Global, Remote Workforce

Today's workforce is digital-first, distributed, and increasingly reliant on external talent.

38% of the workforce consists of contractors, vendors, and external workers.[1]

Nearly 50% of organizations have experienced a breach involving third-party access, with an average cost of **$4.88 million per incident – a 10% YoY increase.**[2]

Deepfake fraud attempts surged 3,000% in 2023 and continue doubling every few months.[3]

Businesses lost an **average of $500K per deepfake-related fraud** incident in 2024.[3]

5% of all initial security breaches in 2024 were perpetrated by fraudulent employees, not hackers or malware.[4]

Remote work and contractor reliance have created a perfect storm – and attackers know it.

[1] Navigating the Complexities of Global Contingent Worker Management, Papaya Global
[2] Cost of a Data Breach Report 2025, IBM
[3] Deepfake Statistics 2025: AI Fraud Data & Trends, Deepstrike
[4] M-Trends 2025 Report, Mandiant

PART TWO: EVOLVING THREATS

How Attackers Exploit the Modern Workforce

Cybercriminals are adapting faster than ever, leveraging technology and human vulnerabilities to infiltrate organizations.

Key tactics include:

Proxy Interviews

One person applies, another shows up - often with malicious intent

Off-Screen Coaching

Candidates receive real-time answers during interviews via hidden earpieces or messaging apps

Deepfake Identities

AI-generated avatars and synthetic voices convincingly pose as legitimate candidates

Social Engineering

Attackers impersonate employees, vendors, or customers to gain unauthorized access

These methods allow imposters to bypass traditional screening measures, creating significant risk for sensitive systems and organizational security.

PART THREE: REAL-WORLD EXAMPLES

Remote Hiring: A Growing Identity Risk

HOW IDPROOF+ STOPS THIS THREAT

Every remote candidate would have been required to undergo live government ID validation and biometric verification before onboarding, effectively blocking imposters from using stolen identities or deepfake avatars to secure employment.

Arizona Scheme — $17M Funneled Overseas via Fake Hires[5]

A woman enabled North Korean nationals to pose as U.S. citizens, securing remote IT jobs at **309 U.S. companies**, including Fortune 500 firms and government agencies. The FBI, IRS-CI, and DOJ called this one of the largest schemes of its kind, stressing the urgent need for **stronger identity verification and due diligence** when hiring remote workers to prevent exploitation by foreign adversaries.

MECHANICS: Operated a "**laptop farm**" from her home, hosting or shipping over **90 laptops** to North Korea-linked locations via China. These devices allowed imposters to perform remote work under stolen identities.

IMPACT: The operation generated **over $17 million in illicit revenue** for both the perpetrator and the North Korean regime and involved **68 stolen American identities** which were used to forge payroll checks, file fraudulent tax returns, and deposit wages into U.S. accounts.

LEGAL CONSEQUENCES: The woman received a **102-month prison sentence**, three years of supervised release, **forfeiture of $284,555.92**, and **restitution of $176,850**.

KEY TAKEAWAY: Stricter vetting of virtual employees and robust identity verification are essential to prevent insider threats and foreign adversary infiltration.

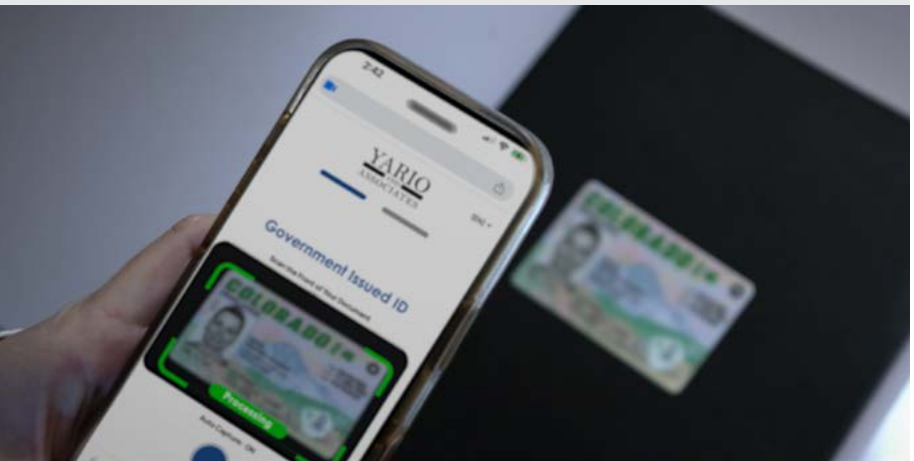
[5] Arizona Woman Sentenced for $17M Information Technology Worker Fraud Scheme that Generated Revenue for North Korea, U.S. Department of Justice

PART THREE: REAL-WORLD EXAMPLES

Securing Contractor Access: Closing the Identity Gap

HOW IDPROOF+ STOPS THIS THREAT

Every third-party contractor would have been mandated to complete live government ID validation and biometric verification before being granted access, ensuring only legitimate individuals receive privileged credentials. This dramatically reduces the risk of nation-state infiltration risk and supply chain compromise.



Russian Hackers Infiltrate Sensitive Systems for Years[6]

Between **January 2020 to February 2022**, Russian state-sponsored hackers infiltrated **U.S. cleared defense contractors** (CDCs) in one of the most persistent espionage campaigns on record, according to a joint alert from the **FBI, NSA, and CISA**.

MECHANICS

- **Phishing and Credential Harvesting:** Spear phishing campaigns, brute-force login attempts, and password spraying
- **Stealthy Persistence**: No malware, just legitimate credentials, enabling undetected access for years

By exploiting weak identity verification during contractor onboarding, attackers gained privileged access without raising alarms.

IMPACT: The attackers gained access to highly sensitive defense data, including:

- **Weapons development plans**, export-controlled technologies, **communications infrastructure**, and proprietary software designs
- **Internal documents** covering product specs, analytics, personnel data, legal matters, and international partnerships

This intelligence allowed Russia to accelerate military modernization, shape strategic planning, and identify systemic vulnerabilities within U.S. defense networks.

THE RISKS: Third-party contractors often require **high-level system access**, making them prime targets. Without **rigorous identity checks**, organizations risk catastrophic breaches and compliance failures.

KEY TAKEAWAY: Adopt **Zero Trust principles**, enforce **multi-layered authentication**, and deploy solutions to protect against persistent nation-state threats.

[6] Joint Alert Says Russian Hackers Compromised Defense Contractors and Accessed Sensitive Information for Years, CPO Magazine

PART THREE: REAL-WORLD EXAMPLES

Call Centers & Help Desk: The Frontline of Social Engineering Risk

HOW IDPROOF+ STOPS THIS THREAT

Every caller requesting sensitive actions would have needed to pass live biometric authentication or credential validation, making it virtually impossible for attackers to impersonate employees and gain unauthorized access through social engineering.

MGM Resorts Cyberattack: Social Engineering at Scale[7]

In **September 2023**, MGM Resorts suffered a **major cyberattack** orchestrated by the **Scattered Spider** hacking group, linked to the ALPHV ransomware collective. The attackers exploited human vulnerabilities through sophisticated social engineering tactics, targeting MGM's internal IT help desk to gain unauthorized access.

MECHANICS

- **Help Desk Exploitation**: Attackers impersonated employees and convinced IT staff to reset credentials.
- **Social Engineering Mastery**: Scattered Spider leveraged phone-based tactics and identity spoofing to bypass security protocols.
- **Operational Paralysis**: Core systems were shut down, affecting guest services, loyalty programs, and payment processing.

IMPACT: The breach caused widespread disruption across MGM's hospitality and gaming operations, including:

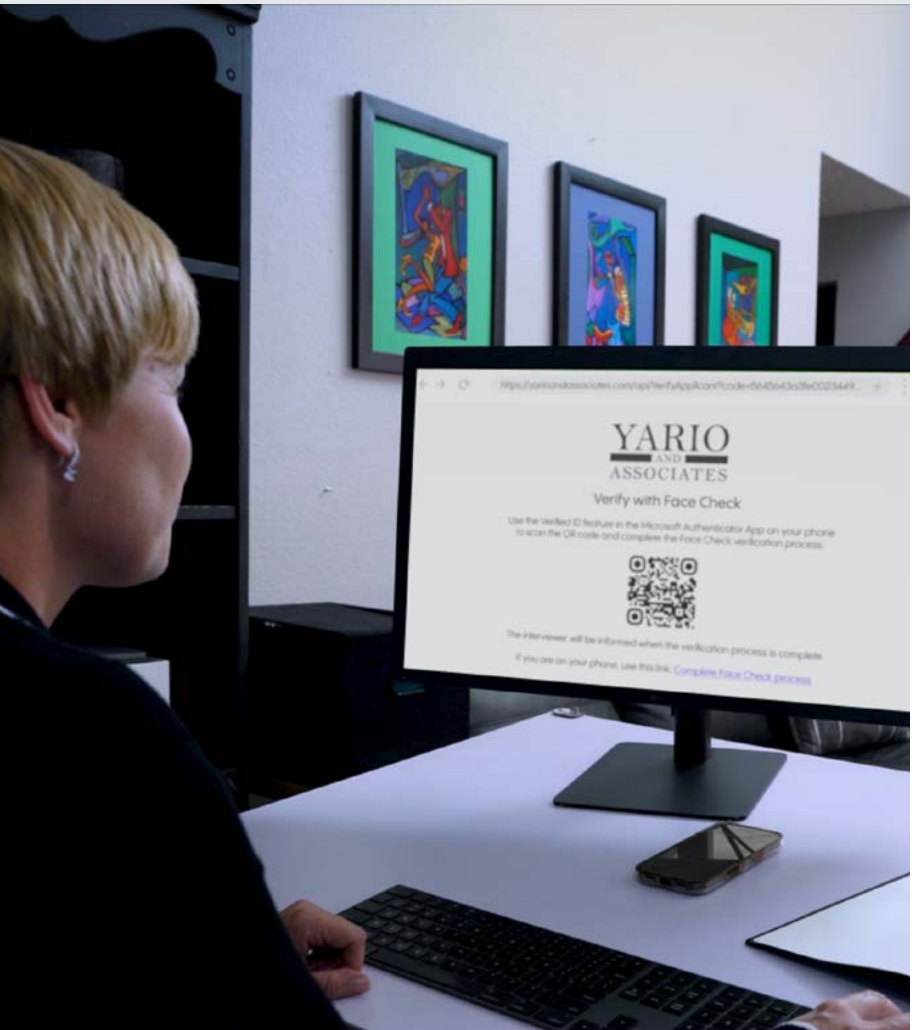
- **Tens of millions in lost revenue** due to system outages
- **Extended downtime** for hotel check-ins, reservations, and casino systems
- **Significant reputational damage**, amplified by global media coverage
- **Data compromise**, as sensitive customer data was also exposed, raising concerns about privacy and compliance obligations

KEY TAKEAWAY: **Robust identity verification**, **multi-layered security controls**, and **employee training** are required to defend against social engineering attacks that can cripple enterprise operations.

[7] The MGM Resorts Attack: Initial Analysis, CyberArk

PART FOUR: THE SOLUTION

IDProof+ Delivers High-Assurance Identity Verification



IDProof+ Stops Identity Fraud Before it Starts

Whether verifying an identity remotely before an interview, during account login, or at a help desk password reset, **IDProof+, in collaboration with authID ensures organizations "Know Who's Behind the Device"™ every time.**

CORE CAPABILITIES

- **Secure**: Government ID validation and biometric verification
- **Global Coverage**: 14,000+ document types from 194 countries
- **Fast**: authID Proof™ delivers sub-700ms identity verification response times
- **Zero Trust Alignment**: Time-limited, scoped access credentials

BENEFITS

- **Blocks deepfakes and synthetic identities** before onboarding
- **Ensures secure, compliant access** across the hybrid workforce
- **Reduces fraud** and manual verification costs

WHY CHOOSE IDPROOF+

Biometric Precision
Selfie and document liveness detection to block spoofing and deepfakes

Global Reach
Multilingual OCR and document verification

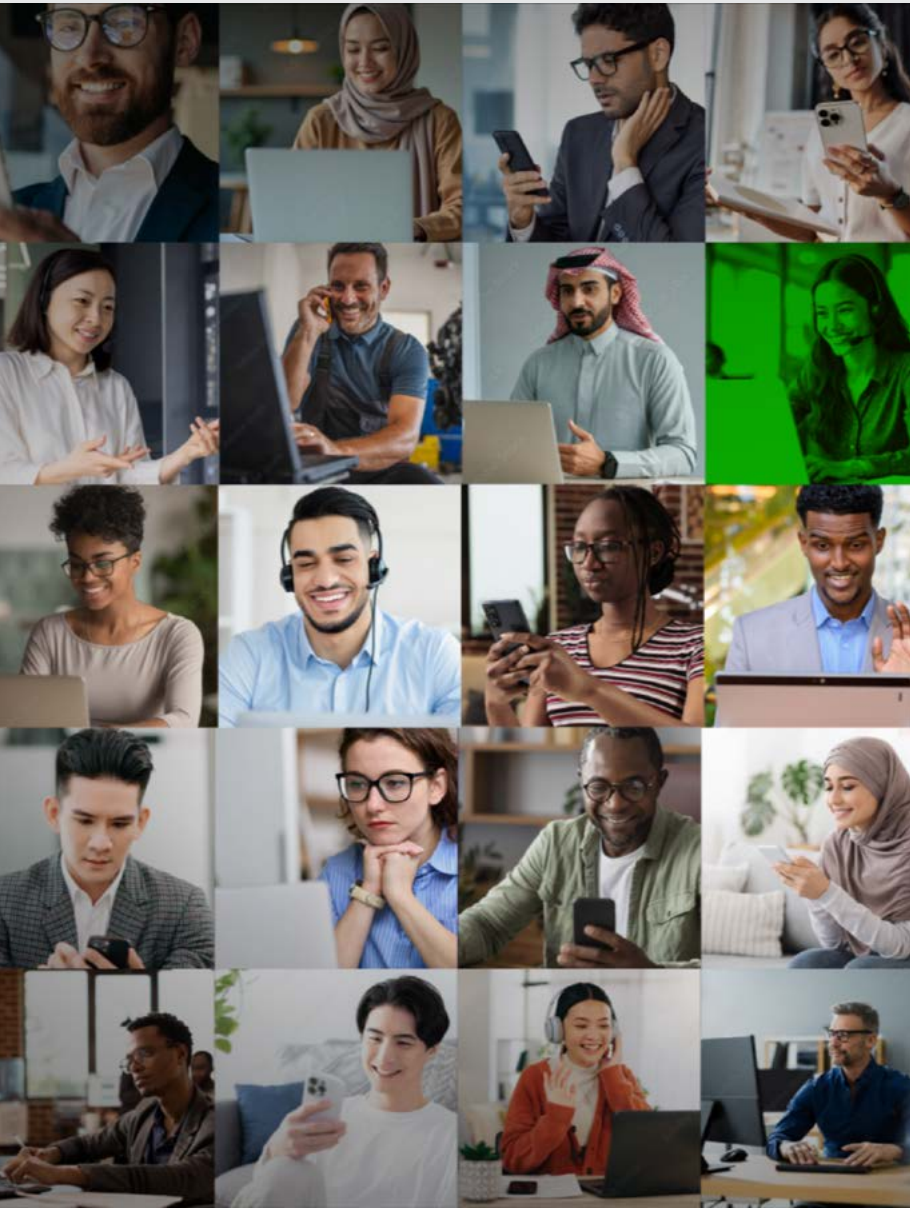
Fast Deployment
Built on Microsoft technologies for quick rollout with minimal disruption

Regulatory Compliance
Meets high-assurance standards for finance, healthcare, and government

"Know Who's Behind the Device" is a registered trademark of authID.

PART FIVE

How IDProof+ Works



The Step-by-Step Verification Flow

Candidate Applies

Candidate initiates application for a remote role.

Enrollment

Candidate is prompted to enroll and provide consent for identity verification.

Digital Credential

Candidate completes a few simple steps (e.g. submitting ID, biometric check) and receives a verified digital credential stored securely in their digital wallet.

Identity Verification

At interview time, candidate performs live verification to confirm identity and liveness in real-time. Verification is completed in seconds, ensuring high assurance.

Ongoing Trust

The process can be repeated whenever trust needs to reestablished, taking only seconds to re-verify and restore trust.

CONCLUSION

Build Digital Trust at Every Touchpoint

Identity assurance is no longer optional – it's essential.

From onboarding remote employees to granting contractor access or verifying help desk callers, IDProof+ provides secure, fast, and frictionless identity verification, ensuring trust at every interaction.

Ready to strengthen your identity strategy?

Click here to learn more about IDProof+ or contact us directly at idproofplus@majorkeytech.com.

MajorKey

IN PARTNERSHIP WITH authID

See IDProof+ in Action

Schedule a Live Demo

Scan the QR code or click here.

Watch a Recorded Demo

Scan the QR code or click here.

Copyright © 2025, MajorKey Technologies. All rights reserved.