MENA FINTECH AWARDS 2024
BEST REGTECH OF THE YEAR

IDENFO

Authenticating Identity Card Documents in an Age of AI and Deepfake Spoofing

Force for good.

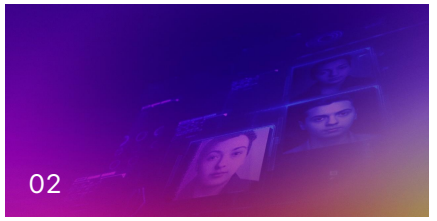
www.idenfo.com

Author

Antony Bellingall

Co-Founder, Idenfo

Challenges Faced by KYC Providers in an AI-Driven Fraud Landscape



Summary of Fraud Vector Findings

Identity Verification: Focus on Passports

Idenfo’s NFC Chip Reading Solution: Transforming Document Authentication

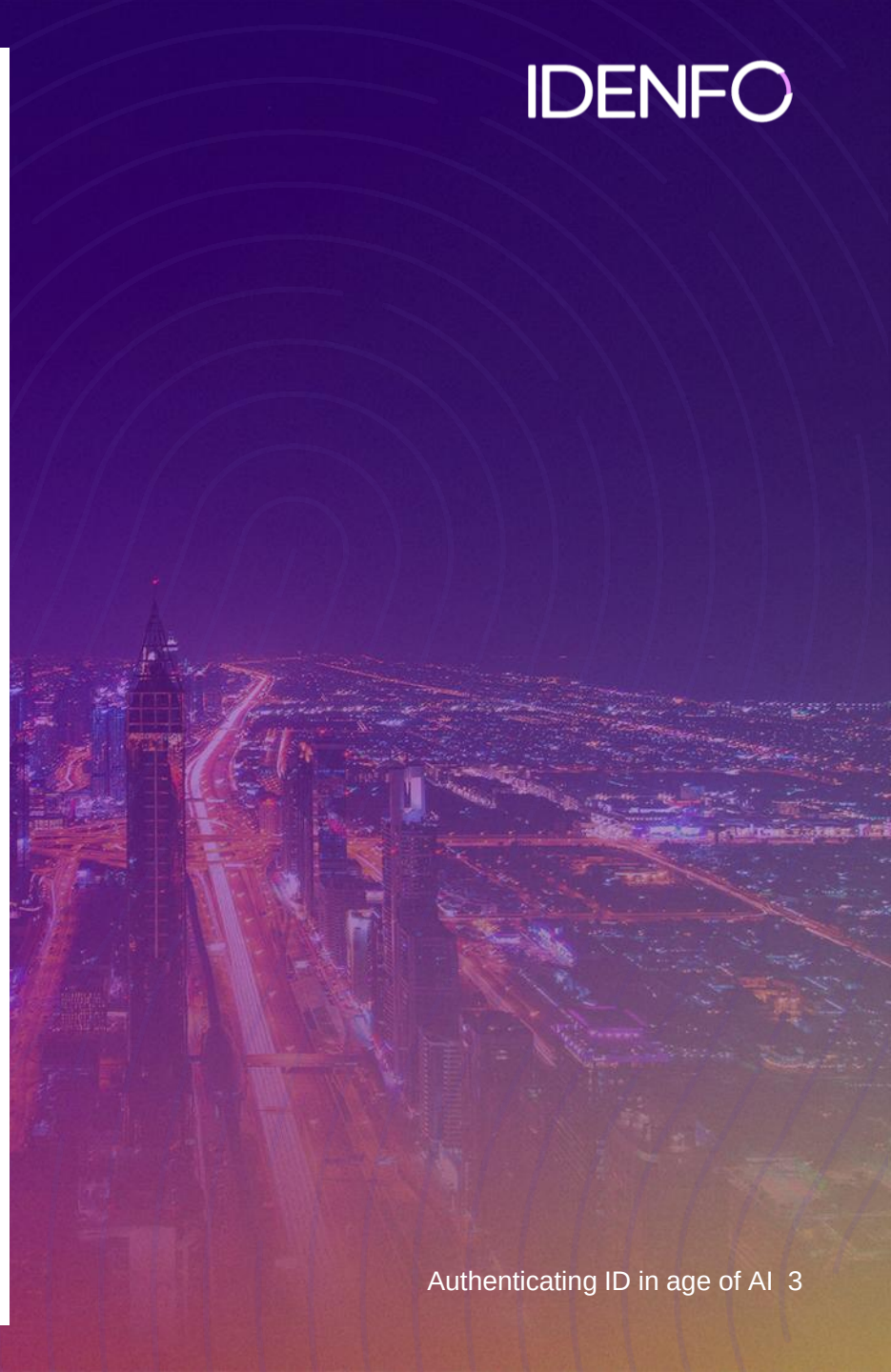
Legal Statement

This document contains proprietary information belonging to Idenfo Ltd.

No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic or mechanical, without the express prior written permission of Idenfo Ltd, excepting a demand by an appropriate Regulatory authority.

The text, graphics and examples included herein are for the purpose of illustration and reference only. No legal or accounting advice is provided hereunder. To the extent that this document provides suggestions for efficient compliance processing, such advice does not constitute legal advice and in no way assumes on Idenfo a responsibility for compliance obligations.

Corporate and individual names and data used in examples herein are fictitious unless otherwise noted. Idenfo reserves the right to revise this document or any part thereof at any time.



Executive Summary

In today's digitally driven world, financial institutions and regulated businesses face unprecedented challenges authenticating identity documents amid rapid advances in artificial intelligence (AI) and the rise of sophisticated deepfake spoofing techniques.

Traditional Know Your Customer (KYC) procedures, reliant on visual inspection and biometric checks, are increasingly vulnerable to AI-generated fake documents, synthetic identities and manipulated live video feeds.

Fraudsters exploit generative AI to create near-perfect replicas of passports, driving licences, and other identity cards that can easily bypass conventional safeguards, putting firms at heightened risk of money laundering, financial fraud and reputational damage.

This white paper explores the evolving threat landscape for KYC providers managing these new attack vectors, focusing on industry research and emerging technology solutions.

It reviews major studies on the effectiveness and limitations of biometric liveness detection, advanced document forensics, synthetic media analysis and the importance of multi-layered, AI-enhanced cross-database verification strategies.

A concise overview of international identity cards, notably passports and their embedded NFC chips, provides context for novel approaches.

Central to the discussion is Idenfo's innovative solution, which leverages NFC chip reading capability integrated with secure digital signature verification.

By enabling a seamless phone-based read of the encrypted chip data within passports and similar IDs, Idenfo's technology authenticates personal details and photographic identity directly against digitally signed chip records.

This method mitigates risks from doctored images and deepfake videos by relying on the secure physical token and cryptographic verification, thereby dramatically enhancing KYC integrity.

The conclusion outlines why Idenfo's technology represents a transformational leap forward in identity verification - balancing enhanced fraud resistance with a frictionless user experience - to meet the demands of AI-driven identity threats and regulatory compliance in the financial sector.

Challenges Faced by KYC Providers in an AI-Driven Fraud Landscape

The Expanding Threat of AI-Powered Identity Fraud:

Data, Trends, and Expert Commentary

The identity verification landscape is under immense pressure from the rapid rise of fraud enabled by advances in generative AI and deepfake technologies.

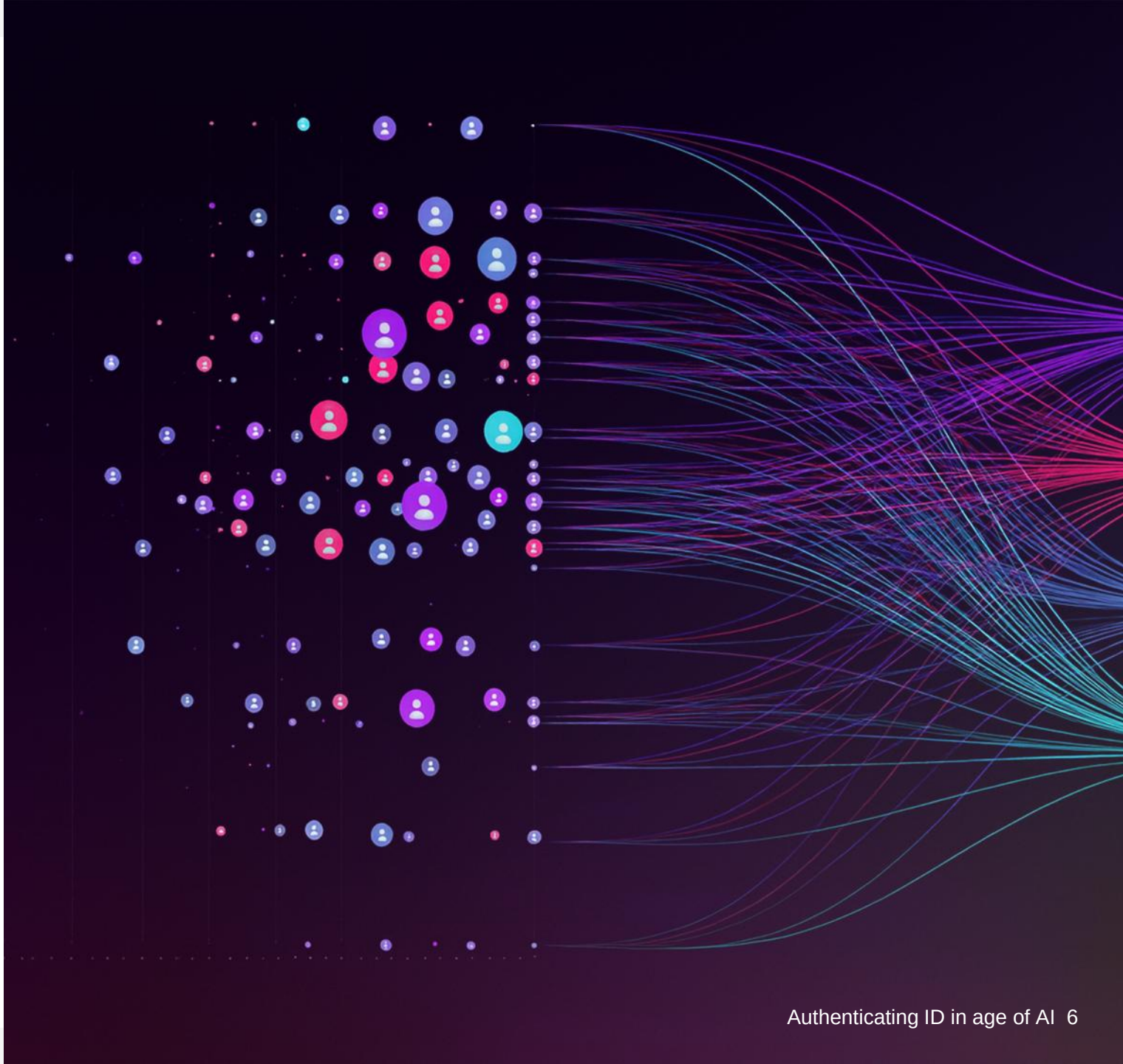
Fraud attempts leveraging AI-generated synthetic media have increased exponentially: deepfake fraud attempts surged by 3,000% in 2023 alone, with an estimated 8 million deepfake files projected to circulate in 2025 compared to 500,000 in 2023. By 2025, roughly 5% (1 in 20) of identity verification failures are now attributable to deepfake attack vectors.

Globally, AI-driven fraud is projected to cost organisations upwards of $40 billion by 2027, demonstrating the enormous financial risk posed to enterprises worldwide. [1]

In the United Kingdom, identity fraud accounted for 59% of all fraud cases in 2024. Account takeovers increased by 76%, and SIM swap scams - often facilitated by AI-aided social engineering - increased over 1,000%, illustrating the intensifying scope and scale of this threat in regulated industries. [2]

1 https://deepstrike.io/blog/deepfake-statistics-2025

2 https://www.mishcon.com/news/fraud-trends-in-2025-the-ai-paradox



Industry experts have sounded alarms about the gravity of these developments.

The Financial Times notes that, "the rise of generative AI in fraud attacks is a watershed moment for identity security - traditional verification is no longer enough," while a BBC technology correspondent highlighted that, "With deepfakes becoming increasingly indistinguishable from real humans, financial institutions must rethink authentication entirely."

Such insights reflect recognition within the media that AI's rapid sophistication outpaces legacy KYC safeguards, compelling a shift towards innovative, layered verification approaches. [3] This is borne out by the emerging attack vectors shown in the table on the right.

3. https://startupsmagazine.co.uk/article-vanta-state-trust-2025-ai-threats-outpace-security-expertise
4. https://deepstrike.io/blog/deepfake-statistics-2025
5. https://authbridge.com/blog/kyc-challenges-today-and-future/
6. https://deepstrike.io/blog/deepfake-statistics-2025
7. https://startupsmagazine.co.uk/article-vanta-state-trust-2025-ai-threats-outpace-security-expertise
8. https://kyc-chain.com/ai-identity-fraud-2025/

Emerging AI-Driven Fraud Vectors and Notable Metrics (2025)

Attack Vector	Description	Notable Metrics
Deepfake Video/Image Spoofing	AI-generated synthetic video and facial images fooling biometric systems	+3,000% increase since 2023; $40B projected losses by 2027 [4]
Synthetic Identity Creation	Hybrid identities blending real and fabricated data evade databases	18% annual growth rate[5]
Video Injection Attacks	Replacement of live biometric feed with pre-recorded or synthetic video	Deepfake video fraud every [5] minutes globally [6]
AI-Powered Phishing & PhaaS	AI-enhanced spear phishing using conversational bots	43% increase in AI-based phishing attacks [7]
Document Forgery	Physical and digital document forgery augmented by AI image synthesis	244% rise in document forgery attempts [8]

Summary of Fraud Vector Findings

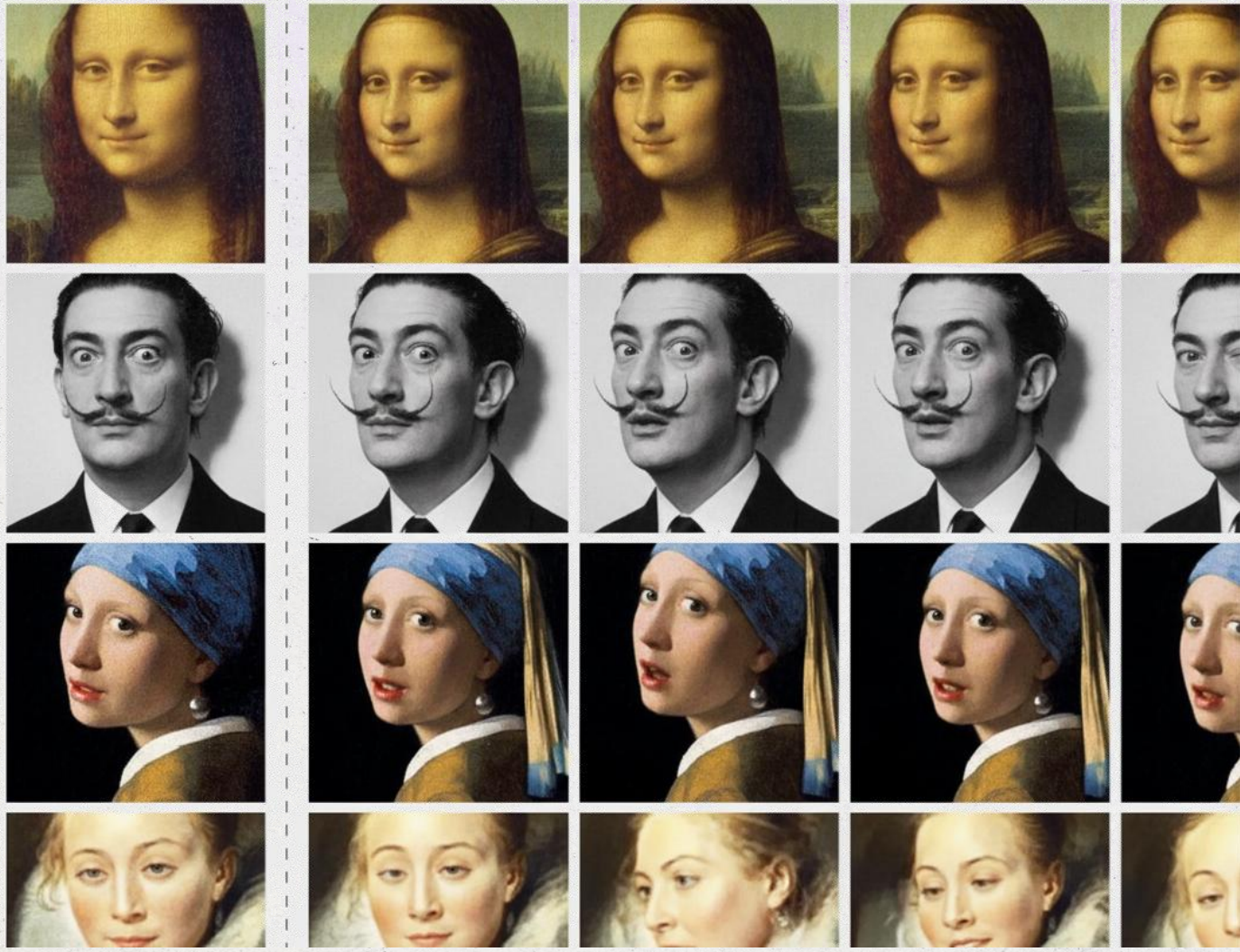
This data underscores the scale and complexity of AI-facilitated identity fraud plaguing KYC systems today.

Deepfake technology is no longer fringe but a mainstream tool utilised to spoof facial biometrics and manipulate identity documents with terrifying accuracy.

Traditional KYC verification systems, often reliant on human document checks and singular biometric scans, are increasingly inadequate.

Fraudsters leverage AI for synthetic identities, deepfake videos, document forgery and social engineering attacks that evade conventional detection.

The convergence of expert opinion and data calls for multi-layered solutions that integrate AI-based analytics, cryptographic physical document verification, biometric and behavioural checks - enabling robust, scalable defences suitable for this rapidly evolving threat landscape.



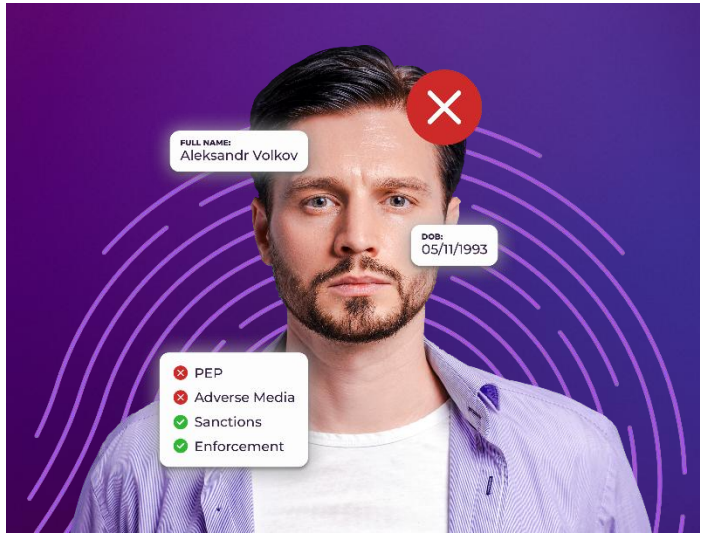
Know Your Customer (KYC) Process in the Post-Pandemic Digital Era

Let’s take a step back though and remind ourselves the key purposes for performing KYC in the first place. Essentially KYC constitutes a series of essential processes financial institutions and regulated entities use to verify client identities, assess associated risks, and ensure regulatory compliance, primarily to prevent fraud, money laundering and terrorism financing.

Traditionally, KYC involved face-to-face interactions where clients presented physical documents for verification. However, the post-pandemic “new normal” shifted KYC predominantly to non-face-to-face digital environments, leveraging online platforms and mobile devices.

Components of Modern KYC

KYC typically covers the following three key mutually dependent functions:



Identity Verification

Confirming the customer's identity by validating government-issued documents (such as passports and driver's licences) and utilising biometric checks like facial recognition.

Name Screening

Comparing customer-identifying information against various global sanctions lists, politically exposed persons (PEP) registers and watchlists to identify potential risks.

Risk Rating

Assigning risk profiles based on customer attributes, behaviours and contextual factors to determine the level of initial and ongoing due diligence.

Digital KYC seeks to enhance these three key components with a combination of automated document verification technologies, AI-enhanced biometric authentication, data aggregation and risk modelling to enable an efficient and secure customer onboarding without physical presence. But is this enough in the age of the deepfake?

Identity Verification: Focus on Passports

When performing the identity verification part of KYC, a typical and critical starting point for financial institutions is the verification of passports, as these documents provide a recognised government-issued proof of identity with established international standards and security features.

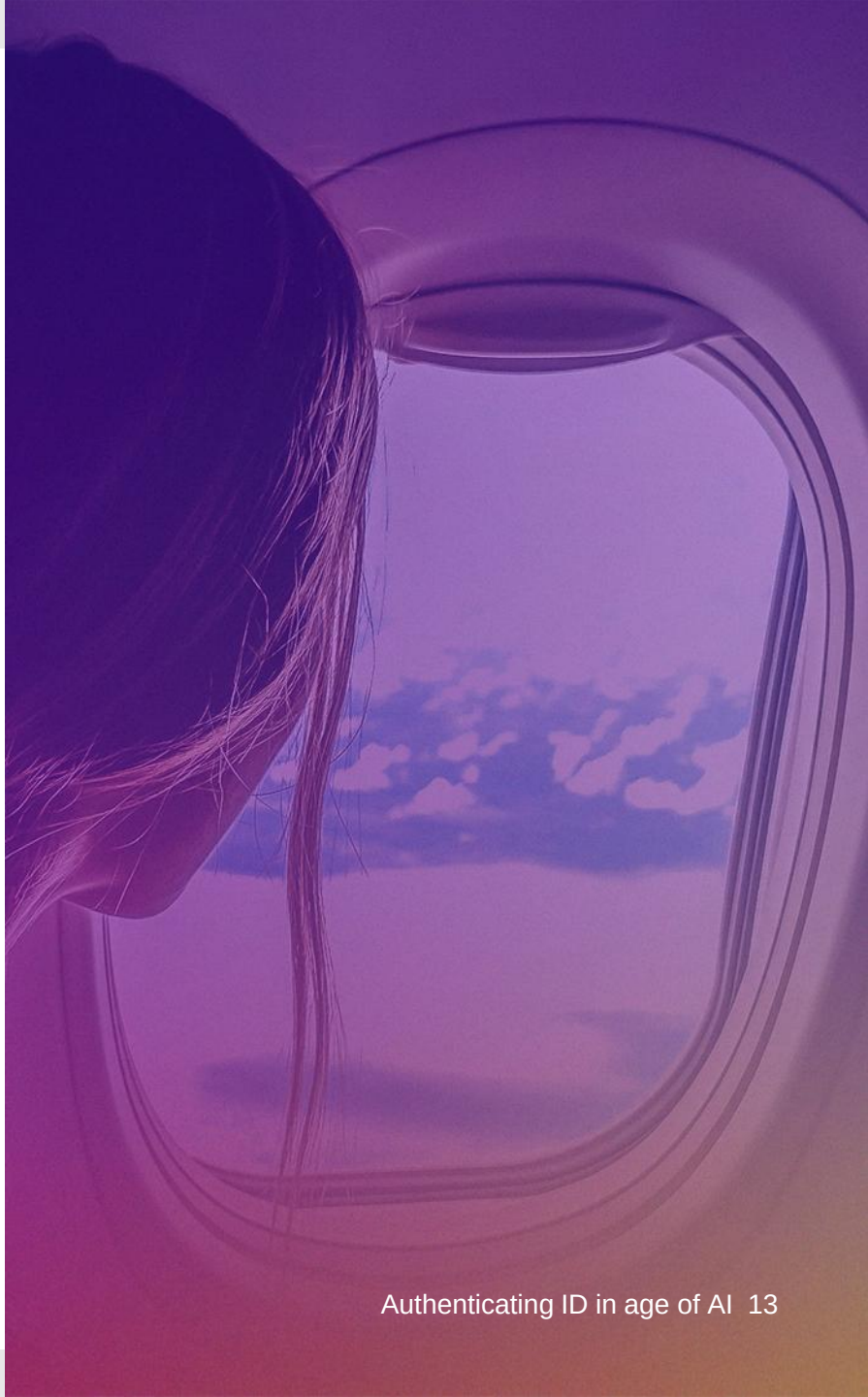
The International Civil Aviation Organisation (ICAO), a specialised United Nations agency established in 1947, has been instrumental in global standardisation of travel documents since 1944. ICAO's remit includes global cooperation to ensure seamless and secure international civil aviation, with one of its key mandates being the creation and maintenance of passport and travel document standards ensuring consistent and verifiable identity validation across borders.

ICAO started standardising machine-readable travel documents in the late 1960s and published the initial specifications for Machine Readable Passports (MRP) in 1980 under Document 9303, introducing uniformity in passport design, functionality, and security elements. Since then, these standards have evolved extensively to incorporate biometric data and harmonised digital signatures, now collectively referred to as ePassports.

These have been adopted globally by over 100 countries. By 2010, ICAO mandated all member states to issue ePassports, phasing out handwritten passports and significantly raising security and verification reliability.

ICAO's global database and standards enable countries to authenticate travel documents worldwide quickly and securely, reducing processing times at border controls and mitigating identity fraud risks during international movement of persons.

Its standards underpin many national and border control systems that intersect with KYC verification, making ICAO compliance a critical feature for any international identity document used in financial services.



How NFC Chip Technology Works in Identity Documents

Embedded NFC chips, integral to ePassports and many modern ID cards, store encrypted biometric and biographic data which can be read contactlessly by compatible NFC-enabled devices (e.g., smartphones, border control readers). The chip contains:

Personal Data
Name, date of birth, nationality, document number and other biographical information.

Biometric Data
A digital facial image often supplemented by fingerprints or iris scans.

Digital Signatures
Cryptographic data (using Public Key Infrastructure) issued by the governmental certificate authority to assure data integrity and authenticity.

When an NFC-enabled reader accesses the chip, it performs a secure handshake and verifies the digital certificates ensuring that the data has not been tampered with or cloned.

This process authenticates the document at the data level rather than relying solely on physical surface features.

The data read can then be cross-checked against the scanned MRZ (machine readable zone) and visually inspected document data, as well as live biometrics, providing multi-factor validation.

This layering significantly enhances trust and fraud resistance, creating a secure digital identity tethered to government-verified physical credentials.

Idenfo’s NFC Chip Reading Solution: Transforming Document Authentication

Idenfo has created a new NFC chip reading capability. This capability revolutionises identity verification by allowing secure, cryptographically validated reads of passports and chip-based IDs via commonplace NFC-enabled smartphones.

This in turn enables:

- Secure extraction of encrypted personal data and biometric images from the NFC chip.

  Rather than risking errors and fraud from visual data, Idenfo’s system reads data straight from the embedded chip, ensuring 100% accuracy and authenticity by accessing the original, government-authenticated record. For example, this eliminates discrepancies caused by damaged or altered physical document surfaces during manual or camera-based reading.

- Verification of the digital certificate signature issued by trusted government authorities, confirming document integrity.

  Idenfo employs Public Key Infrastructure (PKI) to authenticate the cryptographic signature, guaranteeing the document has not been altered or cloned—a critical defence against forgery and chip manipulation. This process includes dynamic validation against certificate revocation lists, ensuring real-time document status verification.

- Multi-factor cross-validation by comparing chip data with physical document details and live biometric facial capture.

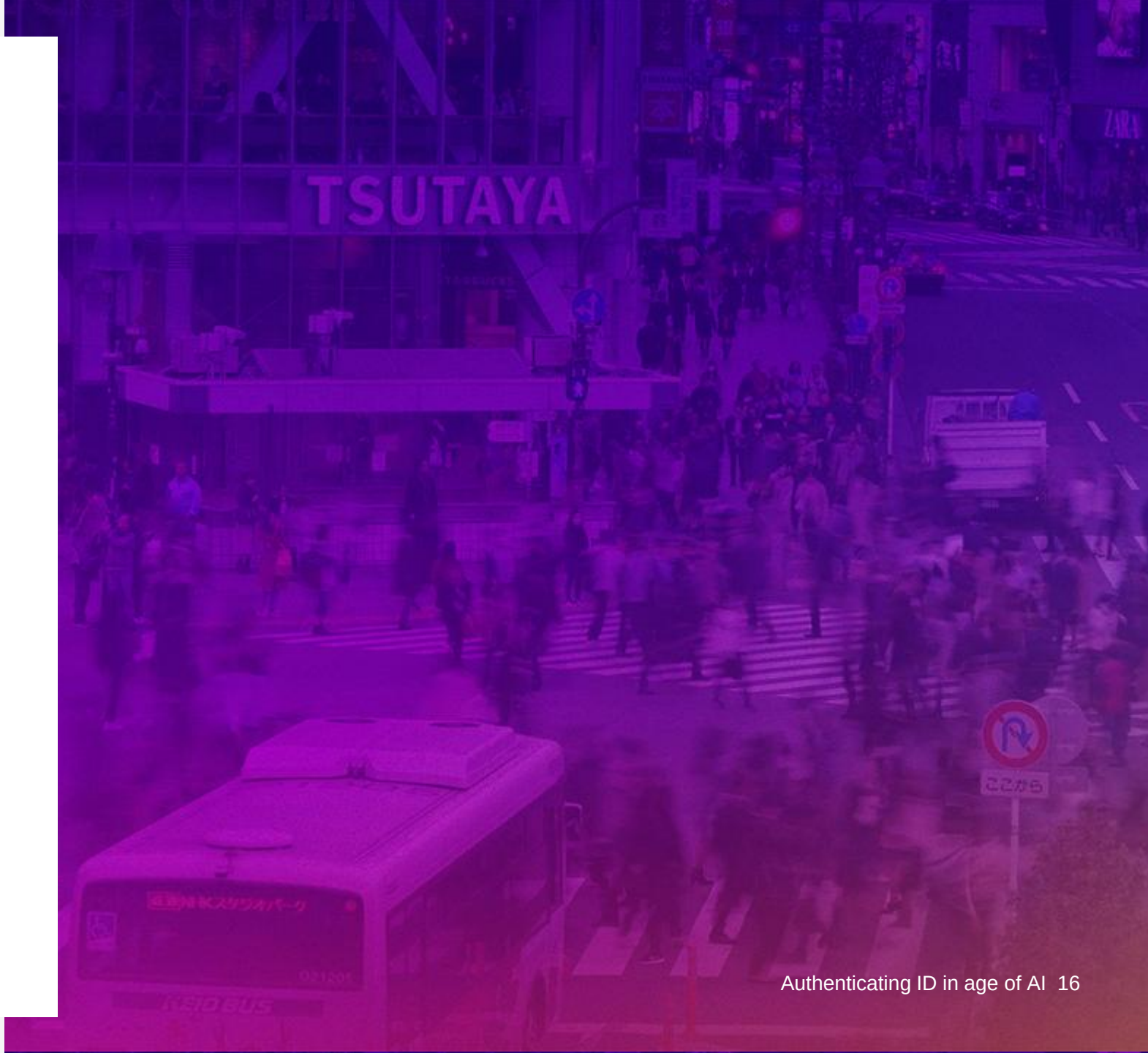
  This layered process ensures the presented physical document matches its secure internal chip data and that the ID holder’s live biometric matches the stored facial template, effectively stopping deepfake, synthetic identity, or stolen document attacks.

- Accelerated, user-friendly onboarding by eliminating manual data entry and reducing friction.

  Users simply hold their phone to the document, allowing instant chip read and validation. This significantly reduces onboarding times from tens of minutes to under two minutes in some cases, enhancing customer satisfaction and decreasing abandonment rates.

- Regulatory compliance adherence meeting ICAO and global AML/KYC standards.

  Idenfo’s solution includes comprehensive audit trails and secure data handling protocols aligned with GDPR, FATF, and regional regulators, providing institutions with confidence in their compliance posture.



Complementary Document Forensic Techniques Strengthen Verification

Idenfo’s NFC solution is further bolstered by an array of forensic document checks that evaluate secondary security features:

Hologram Verification

Idenfo's system analyses the holographic features present on passports and ID cards, which display iridescent and dynamic colour shifting when viewed from different angles. Genuine holograms include micro-text, 3D effects, and laser images that defy replication by simple reproduction techniques. For example, counterfeit holograms tend to show flat or static reflections easily detected by optical sensors.

Moiré Pattern Detection

When images of ID documents are scanned or captured from digital displays, interference patterns known as moiré arise due to pixel grid interactions. Idenfo’s AI-based imaging algorithms detect these tell-tale patterns, exposing attempts to bypass document authenticity by using photographs or screen snapshots instead of original documents.

Watermark Validation

Watermarks, often only visible at certain angles or with transmitted light, are security features embedded during printing. Idenfo’s scanners inspect for the presence, authenticity, and placement of watermarks, essential in verifying documents that lack electronic chips or holograms, such as older ID formats or birth certificates.

Textual Appearance Checks

Using advanced optical character recognition (OCR), Idenfo examines the document's font types, character spacing, alignment, and consistency with official document templates. Any deviation outside accepted parameters or presence of typographic anomalies signals possible tampering or counterfeit attempts.

Checksum Validation

Many official documents incorporate checksums—calculated numerical values that verify the integrity of data fields like ID numbers or dates. Idenfo calculates these checksum digits and compares them to those in the document, confirming that data has not been altered or corrupted.

Biometric Verification

Models created for biometric verification liveness checks provide protection against a range of impersonation attacks from simple 2D masks to sophisticated deepfake videos.

These collective forensic measures complement the cryptographic security offered by NFC chip reading, forming a resilient, multi-angle defence against complex, AI-assisted fraud schemes.

Why Idenfo Is a Game Changer for KYC

Idenfo's integrated hardware-rooted cryptographic chip reading combined with forensic verification offers a multi-dimensional identity assurance platform providing:

- Superior fraud resistance, blocking AI-driven synthetic, deepfake, and forgery attack vectors.

  By leveraging the foundational security of cryptographically signed NFC chip data and layering it with forensic and biometric validations, Idenfo raises the bar well beyond typical one-factor KYC checks, substantially reducing identity fraud risk.

- Regulatory peace of mind through alignment with international AML/KYC mandates and privacy laws.

  Idenfo's solution supports detailed audit trails, data encryption, and controls that ensure compliance with FATF principles, GDPR requirements, and jurisdiction-specific rules. This reduces the risk of costly regulatory penalties.

- Seamless, accelerated customer onboarding with reduced abandonment and operational overhead.

  By leveraging the foundational security of cryptographically signed NFC chip data and layering it with forensic and biometric validations, Idenfo raises the bar well beyond typical one-factor KYC checks, substantially reducing identity fraud risk.

- Scalable automation to meet rising fraud volumes without proportional increases in manual reviews.

  Automation of chip extraction, signature verification, biometric matching, and forensic checks reduces human intervention, enabling operational teams to focus on high-risk cases and lowering verification costs dramatically.

- Future-proof architecture supporting incorporation of behavioural biometrics and AI analytics as threat landscapes evolve

  Idenfo's platform is designed for modular integration, allowing continuous improvement and adaptation to new fraud vectors, ensuring sustainable identity protection.

Critically, Idenfo's offering also encompasses name screening and risk rating services in its global application. The detailed, authenticated data extracted securely via NFC chip reading - including comprehensive data points such as full name, date of birth, nationality, and ID number - enhance the accuracy and reliability of name screening processes against global watchlists and sanction databases, directly contributing to more precise risk rating and compliance adherence.

This robust end-to-end KYC and AML ecosystem positions Idenfo uniquely in the marketplace.

Conclusion

AI and deepfake technologies have irreversibly transformed the identity fraud landscape.

The sophistication and volume of AI-powered fraud schemes severely challenge conventional KYC and document verification methods, exposing institutions to heightened financial crime, compliance risk and reputational damage.

Idenfo's NFC chip reading technology, reinforced by multi-layered forensic checks and biometric validation, represents a transformative leap forward in identity verification. It harnesses the immutable security of government-issued cryptographic identity tokens and augments them with rigorous physical and digital document assessments to effectively combat increasingly nuanced fraud attacks.

Moreover, by integrating name screening and risk rating capabilities powered by the highly accurate data extracted through NFC chip reading, Idenfo delivers a comprehensive KYC and AML solution that enhances regulatory compliance and operational confidence.

Adopting this integrated solution delivers superior fraud mitigation, operational efficiency, and enhanced customer experience - all while ensuring regulatory compliance and privacy preservation.

As fraudsters escalate their capabilities through AI, Idenfo equips financial institutions and regulated entities with an indispensable, future-proof weapon to protect trust, streamline onboarding and safeguard the digital economy.

About IDENFO

At Idenfo, we want to be ‘culturally remarkable’. We want to stand out from the crowd of FinTech startups and be known for the value we add not just to our businesses, but to our communities and the lives of the people we associate with.

We are driven by a desire to shape a better, safer world through technology.

We are driven by a desire to produce a net positive change in our societies. We understand that the work we do helps strengthen communities and make them safer and more stable, and this devotion to goodness is what makes our work meaningful. This is our societal purpose.

As a tech company, our purpose is to change the way digital financial technologies function in order to make them more secure. We aim to cause disruption and revolutionise the tech sphere with radical and original responses to improve digital security.

For more information, visit www.idenfo.com

Connect with us

facebook.com/IdenfoAML

linkedin.com/company/idenfo

instagram.com/idenfoaml

IDENFO

Bankside 300 Peachman Way,
Broadland Business Park, Norwich, Norfolk,
United Kingdom, NR7 0LB