Key Trends and Insights of Identity Fraud Activities

2024 IDENTITY FRAUD REPORT

| AI-Driven Identity Assurance and Fraud Prevention

innov8tif SOLUTIONS

Contents

Foreword

"The strategic investments we've made over the past thirteen years have positioned our technologies to support clients more effectively as they navigate the complexities of a rapidly changing digital environment.

The digital ecosystem continues to evolve at a rapid pace, and with it, the tactics employed by fraudsters. In 2024, we observed a significant shift in fraud patterns, driven largely by advances in AI and the broadening attack surface of online services."

Joe Seah
Chief Operation Officer,
Innov8tif Solutions

This report was compiled to shed light on the growing sophistication of digital fraud, and to share actionable insights derived from Innov8tif's work with clients across sectors including banking, financial services, FinTech, telecommunications, and more. It serves as a guide for businesses, regulators, and the public to better understand and navigate fraud risks in an increasingly digital world.

This report is not only a presentation of statistics, but a reflection of the stories behind the numbers — stories that highlight the evolving challenges faced by institutions across Malaysia and Southeast Asia. As digital onboarding and eKYC become mainstream, the need for robust and intelligent fraud detection mechanisms has never been more critical.

This year's data reaffirms that **ID captured from screen** remains the most prevalent fraud tactic observed across the industries we support. At Innov8tif, our commitment to fraud prevention is anchored in innovation, compliance, and cross-sector collaboration. By sharing these insights, we aim to empower businesses, policymakers, and technologists in the collective pursuit of building digital trust.

> "In 2024, Innov8tif successfully reduced fraud attempts involving ID captured from screen, the most frequent suspicious activity, by over 35%, from 3,150 cases in 2023 to 2,040 in 2024."

We extend our sincere appreciation to our clients, partners, and regulatory bodies for their continued support in fostering a secure digital ecosystem. It is our hope that this report will inspire more organizations to proactively strengthen their fraud resilience and engage in meaningful collaboration.

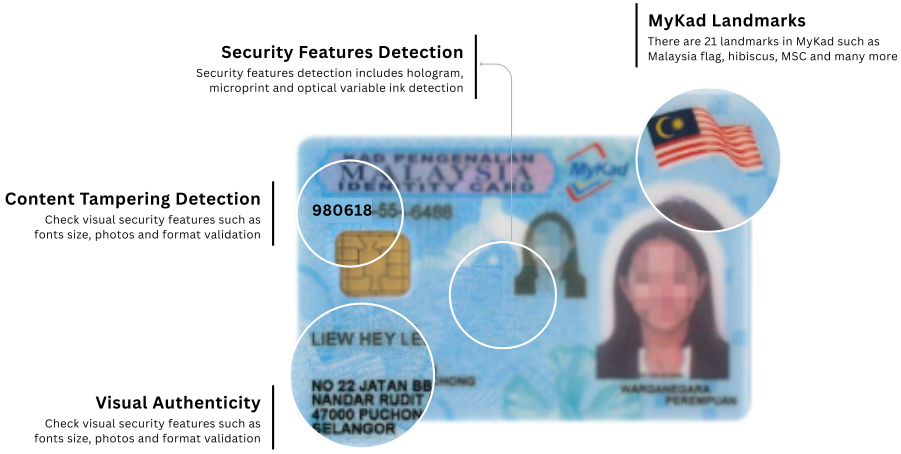
Executive Summary

> In 2024, Innov8tif processed over 23 million ID verifications across its eKYC and digital identity platform, marking a continued surge in digital onboarding activity across Southeast Asia.

The most frequent fraud attempt detected involved ID documents captured from screens, a tactic commonly used to spoof identity proofing systems. Encouragingly, these cases were reduced by over 35% year-on-year, from 3,150 in 2023 to 2,040 in 2024. Other prominent fraud signals included photocopy ID in full color, while the least frequent were faces captured from photos or screens.

Throughout the year, Innov8tif continued to strengthen its fraud prevention capabilities, with the internal development team working on a range of enhancements, including a **new anti-deepfake engine, fraud detection modules, and overall accuracy improvements** across its verification stack.

As fraud tactics evolve in complexity, Innov8tif remains committed to empowering organizations with data-driven insights, adaptive technologies, and secure identity verification solutions. This report shares not only statistics, but a deeper look into fraud patterns and emerging threats — serving as a strategic resource for decision-makers, compliance teams, and fraud prevention units navigating today's digital risk landscape.



Methodology

This report was developed using aggregated and anonymized data derived from Innov8tif's eKYC and fraud detection systems across multiple industries throughout 2024. The data reflects real-world submissions, fraud detection results, and risk scoring generated by our proprietary technology, which supports clients in banking, government services, fintech, insurance, telecommunications, and e-wallet sectors across Southeast Asia.

Scope of Data

The analysis spans **over 23 million ID verification transactions** processed across all client platforms within the calendar year. All data points were collected in compliance with relevant data protection regulations and were anonymized to ensure confidentiality.

Fraud Identification Criteria

The Suspicious cases were categorized based on a combination of automated flags, manual review, and expert investigation. The top fraud triggers in 2024 included:

- ID captured from screens or digital displays
- Photocopies of ID in full color
- Face images presented via photo or screen for spoofing
- Discrepancies between selfie and ID face

Each suspicious case was scored using Innov8tif's internal fraud classification system, which includes real-time decisioning rules, biometric mismatch rates, and image quality analysis.

TRENDS & SHIFTS

FRAUD LANDSCAPE

Overall Trend of Suspicious Activities

As digital services continue to expand across various sectors, fraudsters have grown increasingly adaptive in their methods. Tactics now frequently target vulnerabilities in document capture, liveness detection, and facial verification systems.

Innov8tif's 2024 data reveals several notable shifts in the fraud landscape. The graph presented offers a snapshot of monthly trends in suspicious activities, where the **X-axis represents each month of 2024, and the Y-axis indicates the total number of fraud attempts detected per month.**

The top 3 fraud tactics observed in 2024 were:-
1. **ID captured from screen** — the most frequent method,
2. **Photocopy of ID** (full-color), and
3. **Face captured from photo or screen**, which recorded the lowest volume among the three.

These trends highlight the evolving strategies of fraudsters and reinforce the need for robust, adaptive fraud detection mechanisms across digital onboarding platforms.

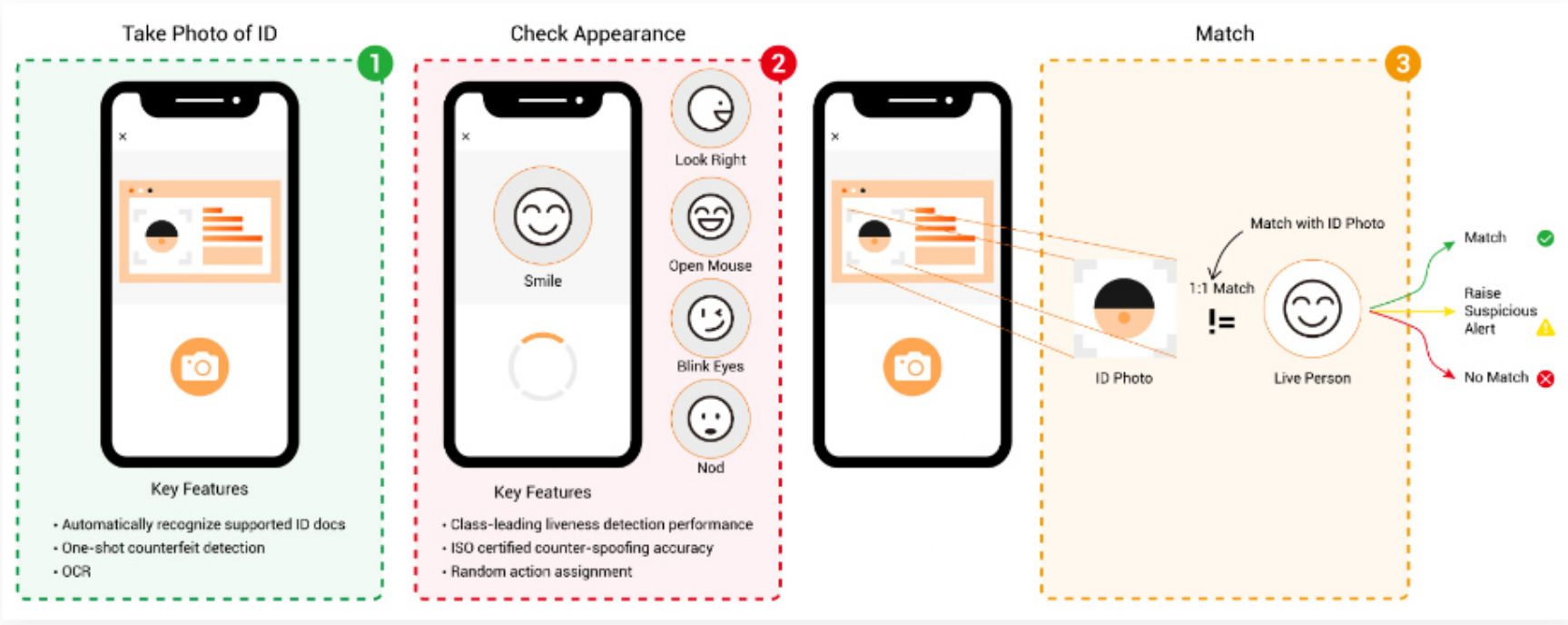
Dominance of Screen-Captured IDs and Photos

The most prevalent fraud attempt in 2024 involved **ID documents captured from screens,** often in the form of high-resolution screenshots or full-colour photocopies designed to bypass document authenticity checks. These made up the largest share of suspicious activity in our systems. However, due to enhanced detection capabilities, their occurrence dropped by **over 35% year-on-year.**

Following closely were attempts where **faces were captured from static images or screens** to spoof liveness detection and facial verification. These patterns indicate that fraudsters are increasingly targeting the biometric layers of eKYC systems, attempting to outsmart motion-based or live interaction checks.

The diagram below illustrates **how eKYC systems are designed to verify** that:

1. The ID document is valid and untampered.
2. The user is physically present and not using spoofing tools such as photo or video.
3. The individual submitting the ID is indeed the rightful owner, confirmed via facial matching and liveness detection actions such as blinking, smiling and etc.



Rise in Photocopied and Full-Colour Forged IDs

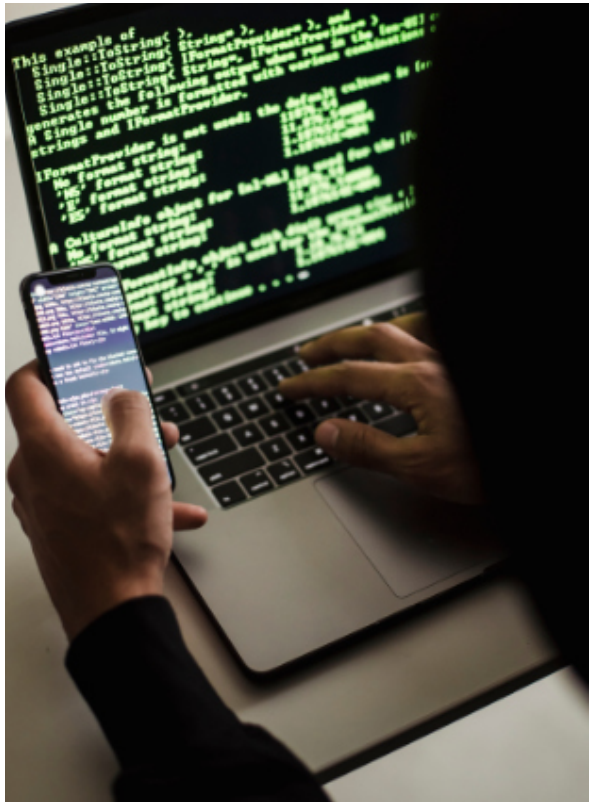
2024 saw a notable increase in the use of **full-colour photocopied IDs** — a subtle yet dangerous form of identity spoofing. These forgeries are designed to resemble legitimate documents but often fail automated checks due to tell-tale inconsistencies in lighting, glare, or printing artifacts.

Suspicious Behavior Detection through Scorecards

While deepfakes and synthetic identities were not directly confirmed in flagged cases, Innov8tif's fraud scorecard system detected **numerous suspicious identity submissions.** Many of these failed onboarding attempts were traced back to **screen-captured IDs** or invalid document sources — prompting further internal review and investigation by fraud analysts.

Growing Demand for Real-Time Fraud Intelligence

With fraud tactics becoming more unpredictable and layered, there has been a **noticeable increase in client demand for real-time fraud flagging and instant decision APIs.** Businesses are increasingly embedding eKYC into their onboarding flows to prevent fraud at the earliest possible stage — especially in high-risk sectors like fintech and e-wallets.



Trends Snapshot

Biggest Growing Threats in 2024
1. ID Captured from Screen
2. Photocopy ID (Full Color)
3. Face Captured from Photo/Screen

Top 3 Most Targeted Industries
1. Fintech and e-Wallets
2. BNPL and Digital Lending
3. Government Digital Services

Most Vulnerable Document Type
1. National ID Card
2. Passport

Region With The Highest Fraud Rate
1. Asia

DATA STORIES

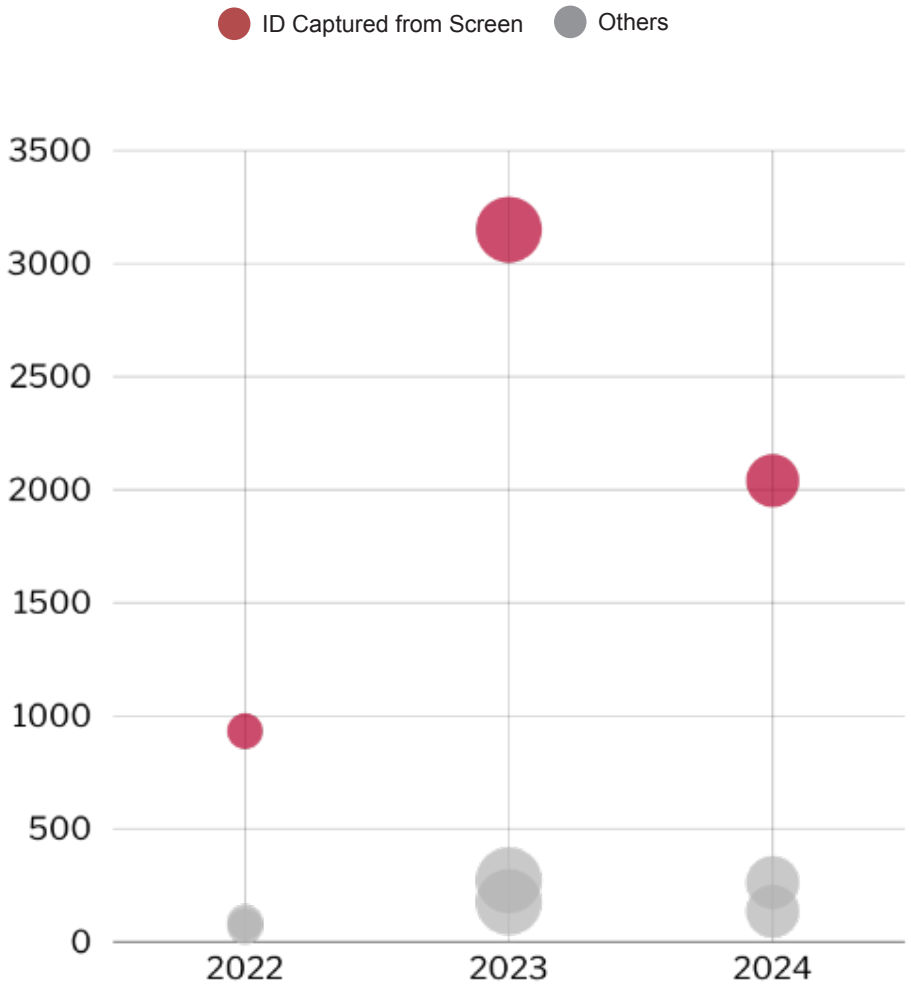
TOP 3 OF FRAUD CASES

ID Captured from Screen

Still the most frequent fraud tactic, but reduced by 35% YoY. Attackers use screen grabs to simulate ID document uploads. Continuous fraud scoring and image artifact detection helped drive down attempts.

Since 2022, **ID captured from screen** has emerged as one of the most common fraud tactics observed in our systems. That year, a total of **932 cases** were recorded. In 2023, this number **surged by 238%, reaching 3,150 cases,** marking a significant spike in fraudster activity exploiting static or non-genuine ID presentations.

By 2024, enhanced detection mechanisms helped reduce the number of such attempts to **2,040 cases**, **a 35.2% decrease** compared to the previous year. Despite the drop, screen-captured IDs **remained the most dominant tactic** among all fraud attempt types, demonstrating that fraudsters continue to exploit vulnerabilities in the ID image submission step of the eKYC process.

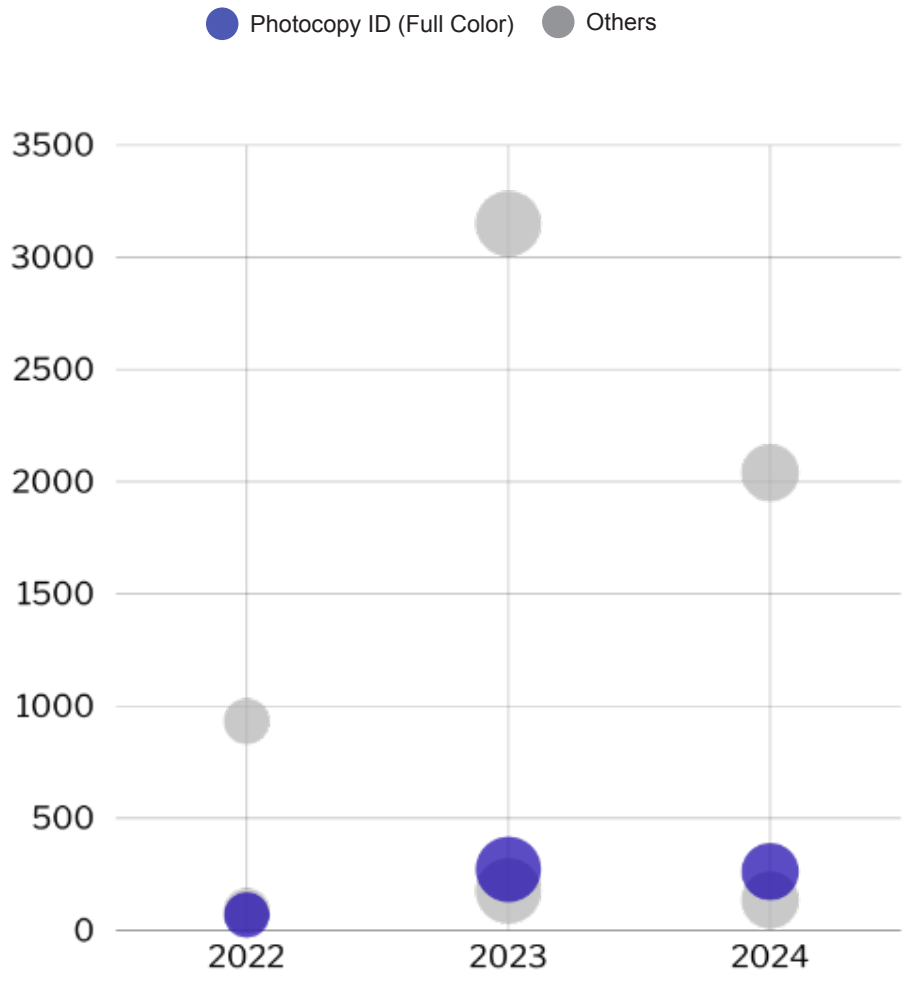


Photocopy ID (Full Color)

Another rising tactic involved the use of **full-color photocopies of ID documents** — often scanned or printed at high resolution to closely mimic the original. These attempts are difficult to detect with the naked eye but typically fail under closer **image integrity analysis**. Fraudsters use this method to simulate a “live” document upload or bypass camera-based verification when original IDs are unavailable.

While not as frequent as screen-captured documents, this technique has seen **consistent growth since 2022**, when **69 cases** were recorded. In **2023, the number surged by 294% to 272 cases,** signaling a sharp rise in the use of static or recycled ID images to exploit verification loopholes.

Although **2024 saw a slight dip of 3.7% to 262 cases,** photocopy ID fraud **remained among the top three tactics** detected by Innov8tif’s systems. This sustained presence highlights the need for verification technologies that analyze document texture, security features, and image source reliability to effectively counter such attacks.

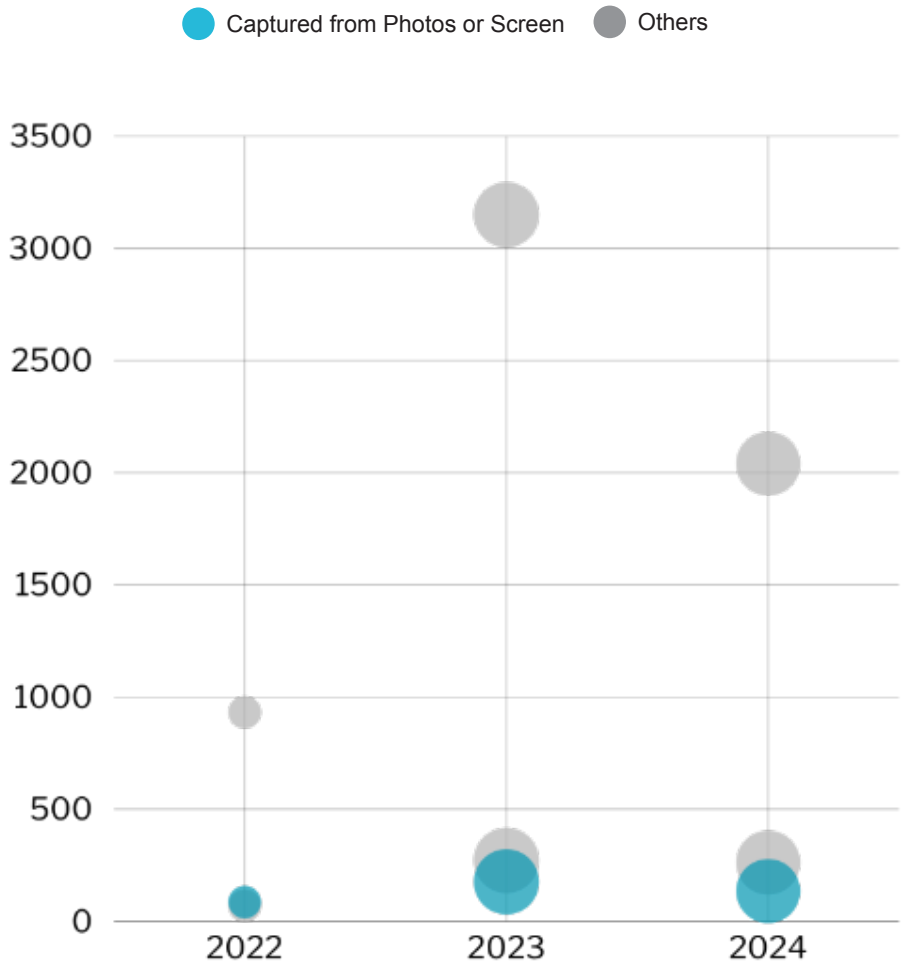


Targeting the Liveness Layer

Biometric spoofing remained a core strategy for fraudsters in 2024, especially those attempting to defeat liveness detection systems. Common tactics included submitting **faces captured from static images or displayed on screens** such as printed photos, screenshots, or even digital avatars — to trick facial recognition into treating non-live inputs as real subjects. These methods were often used to impersonate genuine users or gain unauthorized access to accounts, posing a serious risk to biometric security layers.

While lower in volume compared to document-based fraud, this technique has steadily gained traction. **In 2022**, Innov8tif **detected 86 such cases, which then more than doubled in 2023 to 176 cases** — 104.7% increase.

By 2024, enhanced liveness detection measures **helped reduce incidents to 135 cases, a 23.3% drop from the previous year.** Still, *face-from-photo or screen attacks remained one of the top three most prevalent fraud types,* reinforcing the need for strong anti-spoofing defenses such as motion-based prompts, challenge-response liveness, and image source validation.



DEEP DIVE

FRAUDSTER TECHNIQUES

Spoofing and Presentation Attacks

- **Screen-captured ID — Reused images taken from chat apps, email, or stored on phones**
- **Photocopy or printed ID — High-resolution printouts to mimic real documents**
- **Face spoofing using photos or screens — Static images shown to the camera to defeat liveness checks**

The most prevalent approach remained spoofing and presentation attacks — where fraudsters use pre-existing media to impersonate legitimate users during the eKYC process. This includes ID cards captured from screens, photocopies in full color, and faces displayed via photos or screens to trick liveness detection systems.

These methods are typically carried out using screenshots, downloaded files, or printed images, and can bypass weak capture controls if image source integrity is not enforced. Many attackers recycle the same images multiple times or submit slight variations across attempts to test system thresholds.

Artificial Intelligence and Image Manipulation

- **Deepfake facial animations**
- **Face swaps or AI-retouched images to simulate legitimate selfies**
- **Blurring or editing of MRZ or text fields to bypass OCR systems**

In parallel, the landscape is witnessing the early influence of AI and image manipulation technologies in fraud execution. Although full-scale deepfake attacks were not widely observed in Innov8tif's 2024 dataset, subtler forms of manipulation became more frequent.

Fraudsters have begun leveraging AI tools to enhance, retouch, or edit ID photos, including blurring specific ID fields, swapping faces, or altering text regions to evade OCR systems. These edited assets are designed to appear authentic to both human reviewers and automated engines, demanding more advanced detection capabilities.

FRAUD PREVENTION

BEST PRACTICES

How to Fight Fraud at Onboarding and Beyond

As fraud tactics grow in both scale and sophistication, safeguarding digital onboarding requires more than just reactive measures, but, it demands a layered, proactive defense strategy. Innov8tif's analysis of 2024 fraud patterns highlights two critical areas where organizations can strengthen resilience and reduce exposure to high-risk threats:

1. **Guarding against deepfakes and synthetic media** to prevent AI-generated or altered biometric data from bypassing verification.
2. **Detecting and blocking recycled ID documents** to stop the reuse of captured, scanned, or printed IDs in fraudulent applications.

By prioritizing these practices, businesses can not only address the most prevalent fraud tactics of today but also prepare for the next generation of attacks.

1. Guard Against Deepfake and Synthetic Media

Advancements in AI have made it increasingly easy for fraudsters to generate highly convincing fake faces, manipulate genuine facial images, or create entirely fabricated biometric data. These deepfakes and synthetic identities can bypass basic liveness detection if systems rely solely on static image matching.

- **Deploy active and passive liveness detection** techniques that challenge the user to perform unpredictable actions (e.g., turning the head, blinking, speaking a phrase).
- Use **image artifact analysis** to detect signs of AI rendering, pixel inconsistencies, or unnatural facial movements.
- Continuously update detection algorithms with the latest deepfake samples to stay ahead of emerging manipulation methods.

2. Detect and Block Recycled ID Documents

Recycled ID fraud involves the repeated use of a previously captured, scanned, or printed identity document to impersonate legitimate individuals. Fraudsters may present these in high resolution to simulate a live capture, bypassing verification checks that do not analyze image origin or texture.

- Implement **image fingerprinting and hashing** to identify duplicate or previously submitted IDs across onboarding attempts.
- Enforce **texture and hologram checks** to confirm that the ID is physically present during capture.
- Cross-reference with internal and industry-wide watchlists to flag known compromised documents before they can be reused.

WHO WE ARE, OUR CLIENT & SOLUTIONS

ABOUT INNOV8TIF

“At Innov8tif, we believe that digital transformation must go hand-in-hand with trust. By building secure, inclusive, and scalable digital identity solutions, we’re helping organisations create safer online spaces, while supporting broader ESG goals centered around transparency and digital inclusion. Technology should empower people and protect systems, and that’s the balance we strive for every day.”

George Lee
Chief Executive Officer,
Innov8tif Solutions

About Innov8tif

Innov8tif is an ISO 27001:2022 certified AI identity fraud prevention company specialising in digital identity verification, compliance automation, and fraud prevention solutions. We are also a subsidiary of NexG Berhad, a technology investment holding company listed on Bursa Malaysia.

Innov8tif’s approach towards fraud prevention has always emphasised on regional relevance, compliance readiness, and enterprise-grade integration. Our solutions are designed to operate in complex ecosystems, integrating with national ID systems, AML databases, and internal risk engines to support end-to-end digital trust infrastructure.

With a strong foundation in AI-driven identity verification, workflow automation, and digital onboarding, Innov8tif delivers practical solutions that bridge the gap between user convenience and institutional trust. Our flagship offering, EMAS eKYC, powers secure onboarding for a wide range of sectors including financial services, telecommunications, and government services.

Driven by a mission to simplify and secure the way people connect, transact, and engage online, Innov8tif continues to innovate at the intersection of technology, and transformation.

Contact Us

Malaysia
Innov8tif Solutions Sdn Bhd
sales-my@inov8tif.com

Cambodia
Innov8tif Solutions Co., Ltd.
sales-kh@innov8tif.com

Singapore
Innov8tif Solutions Pte Ltd
sales-sg@innov8tif.com

Philippines

sales-ph@innov8tif.com

Indonesia
PT Innov8tif Karta Solusi
sales-id@innov8tif.com

International

sales@innov8tif.com

innov8tif
FAST LOCAL ID ASSURANCE