The Critical 1%

Closing Systemic Gaps In
Global Identity Verification

Abstract

This white paper sheds light on the small 1% gap in fraud prevention that most companies overlook. Even though it seems very small, this gap can cause serious financial loss and long-term damage to a company's reputation. Most identity verification providers and fraud prevention solutions claim 99% protection against common frauds of phishing, stolen cards and counterfeit invoices. But long-time criminals, such as Jack, continue to exploit the loopholes numerous users still find in old identity-check systems, fragmented regulations, and lax adherence to compliance in rapidly expanding businesses.

The paper demonstrates that fraud has evolved beyond simple forgeries to advanced AI-based schemes, such as deepfakes, biometric spoofing, and synthetic identities, through examples of cryptocurrency, Forex, iGaming and social media marketplace. It also identifies systemic vulnerabilities, such as unregistered populations, biometric blind spots that are exploitable, and fragmented document-authentication systems, which, when combined, enable industrial-scale fraud.

Finally, the story demonstrates how Shufti bridges these gaps with adaptive AI, forensic document inspection, human-in-the-loop intelligence, working closely with stakeholders, and KYC coverage across over 240 countries and regions. Having a false-acceptance rate of only 0.63% and an SDK-based live-capture tool, Shufti turns verification into more of an active defence mechanism, representing that behind every Jack and his network lies a pattern that can be detected, disrupted, and ultimately prevented.

1.0 Meet Jack

Does 99% Accuracy Matter If The 1% Left Unchecked Brings The Biggest Losses? The Story Of Jack Highlights How 99% Accuracy Claims Are Nothing But A Sham.

Meet Jack, at first, he appears as any other human being, quite silent, unobtrusive, and disappears into the background. But Jack sees what other people fail to see. Where most people see routine forms and nonchalant details, Jack sees a hole, an inconsistency, and a slight crack in the system. He is not noisy or careless; he is systematic, observant, and never careless.

99%

of businesses proudly advertise their system's accuracy,but rarely highlight what the number leaves out.

1%

is the small gap that opens the door to risk, where financial and reputational damage begins.

$410M

is lost every year to deepfake-driven fraud, showing how even tiny loopholes have big impact.

$40B

is drained through synthetic identity fraud, one of the fastest-growing threats for businesses.

$4.60

is the hidden cost for every $1 stolen, covering chargebacks, penalties, and recovery.

Scam operations keep ahead of fraud defences, applying deepfakes, synthetic identities, and even faking credentials of children to put organisations at increased risk.

For businesses, the fraud does not merely damage finances; it leads to investigations, penalties, and damage to reputation.

Criminal gangs have transformed into expert international networks, which focus on the 1 percent loophole in fraud detection. Their control over precision and enormous scale is driving losses to new records, and the numbers are growing.

The story of Jack demonstrates that criminals take advantage of identity and KYC gaps that are very critical. There are numerous ways in which fraud may manifest during the customer experience, but onboarding is the most important one.

Think of your business as a house. You do not want to hold Jack up until he gets inside. As soon as he is inside, the damage is increased. Onboarding with strength prevents fraud in its initial stages and increases security in the later stages.

In this whitepaper, we explore how fraud unfolds in the blink of an eye. A single weak defence triggers a chain reaction, where even a 1% lag can set off a domino effect that companies find impossible to escape. And how a recursive approach with Identity Verification tech built from scratch can help prevent fraud.

2.0 Jack Traces The Evolution Of Fraud:

Leaving No Stone Unturned

Modern fraud has evolved from individual opportunistic crimes to coordinated industrial operations. Jack saw this evolution not as history but as opportunity. Analysis of recent fraud patterns reveals three distinct evolutionary phases:

Phase 1: Manual Document Forgery (1990s–2000s)

Jack's earliest lessons came from the old playbooks of fraud. In this era, fraud was largely about manipulating physical documents and leveraging social engineering. He discovered how counterfeit paperwork fueled massive financial scams, like when U.S. mortgage-fraud Suspicious Activity Reports revealed that nearly 3 in 10 cases involved forged documents, while over 1 in 10 hinged on fake IDs. This phase showed him that even simple manual tricks could destabilise institutions.[1]

[1] https://www.fincen.gov/system/files/shared/MortgageLoanFraudSARAssessment.pdf

Phase 2: Digital Exploitation (2000s–2010s)

As Jack studied further, he saw how fraud migrated online. Verification systems began to digitise, but authentication protocols lagged behind. Fraud networks started specialising in specific attack vectors: phishing rings, credential stuffing, and cross-border mule accounts. For Jack, this was proof that fraud was no longer about lone hustlers, it had become a global enterprise where collaboration and specialisation multiplied its impact.

Phase 3: AI-Powered Coordination (2010s–Present)

Now, Jack observes a world where fraud is industrialized and algorithmically supercharged. Criminal networks deploy AI to generate fake documents, spoof biometrics, and create entire synthetic identities. One striking case in 2024 saw a Hong Kong firm lose $25 million after fraudsters used AI-generated executive impersonation. For Jack, this was the culmination of the craft he once studied—fraud had evolved from trickery into technologically orchestrated deception.[2]

[2] https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk

3.0 Jack's Initial Plan:

To Focus On Industries Prioritizing Growth Over Assurance

Years of testing the cracks showed Jack exactly where systems fail. He focused on segments where compliance was loosely followed, authentication controls were weak, and rapid growth allowed companies to overlook risk.

Cryptocurrency

Jack just kept thinking about how these loopholes are inviting criminals into the mix, and the numbers backed up his belief. In the FBI's 2024 Cryptocurrency Fraud Report.

The FBI's Internet Crime Complaint[3] Centre received 149,686 complaints from victims involving cyber-enabled crime and financial fraud involving cryptocurrency, and the reported combined losses in these complaints were a total of $9.3 billion,[4] which is a 66% increase in losses. For Jack, this confirmed that the rapid growth of cryptocurrency adoption, with little to no regulatory frameworks and very limited identity verification, was an invitation for exploitation to exploit the system.

149,686
Complaints with
Cryptocurrency Nexus

Most Reported:
Cryptocurrency Fraud

$9.3
Billion Losses

66%
Increase in Losses
since 2023

[3] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[4] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Forex

The forex market told a similar story. Jack found it incredible that a market this size was still the wild west, and the evidence was there to support him.

The forex market has grown its business to over $7 trillion[5] a day and is expected to reach $10 trillion this decade, attracting a community of good traders as well as many bad traders. Ponzi schemes, fake signal traders, and high-yield investment programmes (HYIPs) now exist freely, often on unwatched online platforms that have low oversight or are completely unregulated.

IGaming

Next, the iGaming industry showed Jack how the fallout can happen when growth-at-all-costs is the strategy. He was left wondering if those businesses even realize that they are turning themselves into playgrounds for criminals.

His excitement increased to learn that online gaming fraud cases rose by 60%[6] in 2024 alone, predominantly due to bonus abuse, affiliate fraud, money laundering, and account takeovers. In their quest to have a big user base, many platforms cut corners on strict verification policies, allowing fraudsters to pounce. Within this, Jack and, ultimately, his future fraud network saw a huge opportunity.

Social Media Platforms

Jack also realised that fraud was expanding beyond financial services into social channels.

FTC[7] data show that scams starting on social media led to about $1.9B in reported U.S. losses in 2024, and most people (70%) who were contacted there reported losing money. In addition, the FTC's Consumer Sentinel Network Data Book 2024 logged 22,258 identity-theft reports tagged "Email or Social Media", up 14% year over year, underscoring the identity-theft dimension of social platforms.
For Jack, this was proof that criminals were exploiting not just weak compliance but also human trust at scale.

[5] https://www.dailyforex.com/forex-articles/forex-scams-15-may-2025/228368
[6] https://northeasttimes.com/igaming-fraud/
[7] https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf

4.0 Jack's Playbook:

Weaknesses In Global Identity Verification Frameworks

Jack is a fraudster but is not content to simply exploit vulnerable industries. He has grown with the technology and learned and adapted to new trends. He discovered that the same fundamental weaknesses that allowed him to cheat smaller target markets had the same opportunities in the larger industries, only veiled beneath more layers.

Birth Registration Gaps

Jack then began mapping systemic weaknesses to real-world opportunities, and birth registration gaps quickly caught his attention. UNICEF estimates that one in every five children under the age of five, or about 150 million, are not officially registered, with half of them in just five countries: Ethiopia, Pakistan, Nigeria, India, and the Democratic Republic of the Congo.[8]

Without reliable governmental registries, forged documents that contain genuine barcodes but altered photos can usually pass through verification checks easily. To Jack, this wasn't just a statistic but a blueprint showing how falsified identities could be created at scale and used to infiltrate even the most secure systems.

unicef

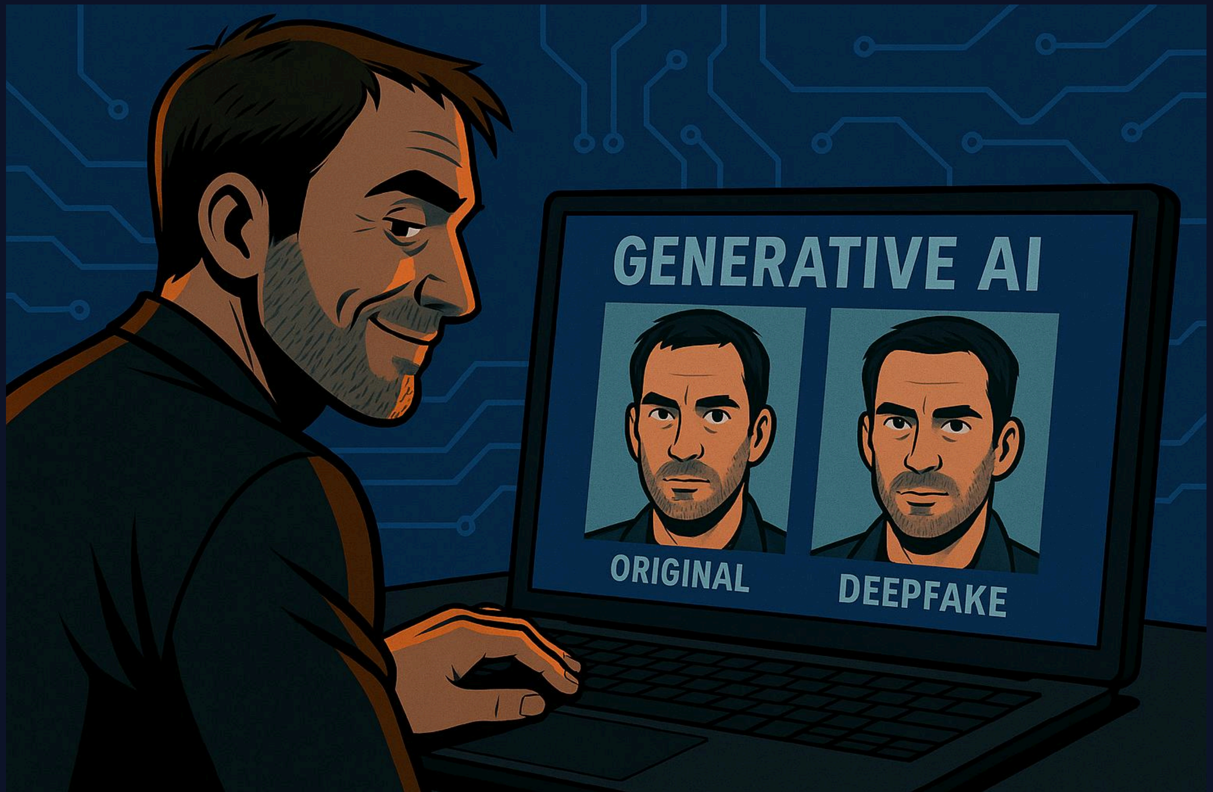
150 MILLION CHILDREN UNDER THE AGE OF 5 REMAIN UNREGISTERED

[8] https://www.unicef.org/protection/birth-registration#:~:text=How%20many%20children%20are%20not,currently%20have%20a%20birth%20certificate.

Biometric Blind Spots

Jack’s next target was biometric blind spots, where technology’s promise of security often outpaced its actual performance. He learned that generative adversarial networks (GANs) could produce faces so statistically “average” that fraud-detection systems often failed to flag them. According to the National Institute of Standards and Technology, the error rates of facial-recognition algorithms may range between 5% and 50"% depending on conditions and datasets.[9]

Now with Generative AI, Jack saw how easy it is to create pixel-perfect deepfakes that look nearly identical to the actual face. The added realism of these deepfakes makes it even less likely that the detection systems will find differences, and it is putting the deepfake detection technology to spot fakes. For him, this wasn't just an innovation but an opening invitation to slip through identity verification undetected.



Synthetic Identity Fraud

Jack eventually turned his attention to synthetic identity fraud, the ultimate ghost in the machine. He discovered that, unlike stolen identities, these weren’t tied to real people at all but built from fragments: a name from one person, a Social Security number from another, and an address plucked from somewhere else entirely. According to the National Credit Union Administration,[10] synthetic identities are one of the fastest-growing forms of identity theft.

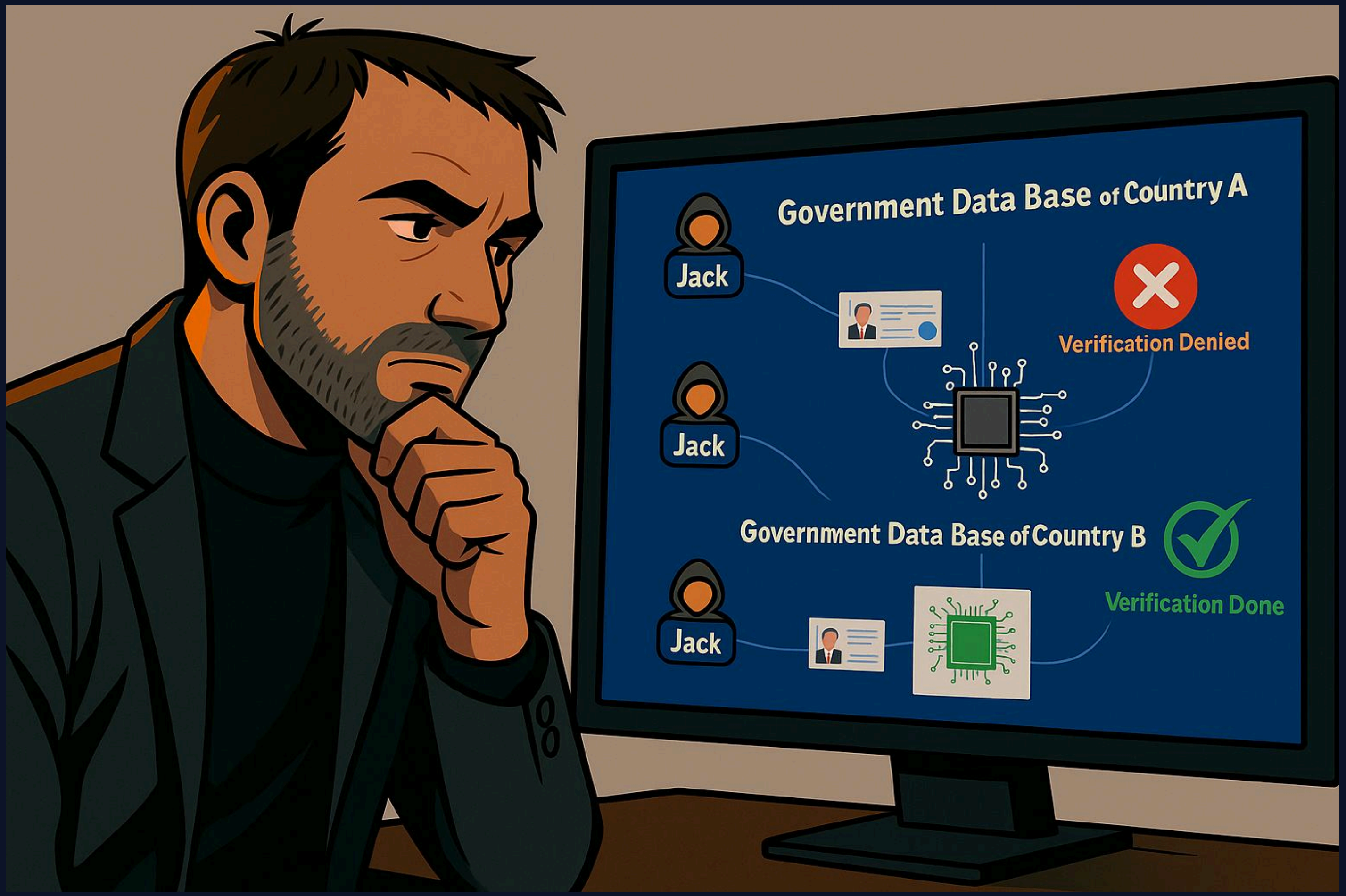
By piecing together fake profiles, fraudsters like Jack could apply for credit, build fake financial histories, make large purchases, and leave banks holding the bill for people who don’t even exist. To Jack, it wasn’t just crime; it was an art form perfected by exploiting systems desperate to approve customers.

[9] https://www.nist.gov/news-events/news/2020/07/nist-launches-studies-masks-effect-face-recognition-software

[10] https://ncua.gov/news

Document Authenticity Gaps

Jack quickly realized that document authenticity gaps offered yet another entry point. While industries touted high-tech verification, he knew there was no single global framework to validate identity documents across borders. Even though the International Civil Aviation Organisation (ICAO) sets standards that still exist, such as Doc 9303[11] for machine-readable travel documents. Many nations still rely on outdated paper-based ID systems or multiple systems that do not link with one another.


Government Data Base of Country A
Jack
Verification Denied
Jack
Government Data Base of Country B
Verification Done
Jack

It meant one thing for Jack that an outdated ID accepted in one country could be completely unverifiable in another. He saw how fraudsters could exploit these mismatches to move easily between jurisdictions and slip past checkpoints designed to stop them but never built to talk to each other.

[11] https://www.icao.int/sites/default/files/publications/DocSeries/9303_p1_cons_en.pdf

5.0 Jack Learns His Tricks Now Threaten Entire Industries

Although Jack had already mapped global weaknesses from his earlier exploits, he now wanted to see how those same vulnerabilities were playing out at the highest level. Curious about their real impact, he began digging through industry reports and breach analyses.

UNITED STATES DEPARTMENT OF THE TREASURY
FinCEN
FINANCIAL CRIMES ENFORCEMENT NETWORK

Federal Bureau of Investigation
Alert FIN-2024-Alert004 on November 13, 2024, focusing on the rising use of deepfake media

Federal Bureau of Investigation
Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence

Financial Crimes Enforcement Network
Fraud Schemes Involving Deepfake Media Targeting Financial Institutions

Deloitte's Center For Financial Services Predicts AI Fraud

Despite years of warnings, Jack realised that large organisations were still hemorrhaging billions while reacting far too slowly. The Deloitte current forecasts stunned him with the loss to AI-related fraud, which will reach $40 billion for U.S. businesses by 2027, from $12.3 billion in 2023, a compound annual growth rate of 32%. The proof was in Jack's eyes that the cracks he'd seen in smaller markets were just as dangerous, only on a much bigger scale.[12]

FBI Warns Of AI-Powered Cybercrime Surge

The FBI's San Francisco division, on May 8, 2024, officially warned of an escalating threat from cybercriminals leveraging artificial intelligence tools, especially in the form of sophisticated phishing and social engineering attacks.[13]

They emphasized that these scams could lead to severe financial loss, damage to reputation, and exposure of sensitive data. The FBI urged businesses and individuals to adopt measures such as staying vigilant and implementing multi-factor authentication to counteract these AI-enhanced fraud attempts

FinCEN Issues Alert On Deepfake Videos And Synthetic IDs

Similarly, FinCEN (Financial Crimes Enforcement Network) issued Alert FIN-2024-Alert004[14] on November 13, 2024, focusing on the rising use of deepfake media, both videos and synthetic identity documents, to bypass identity verification, especially within financial institutions.

Some of the key observations included a notable increase in suspicious activity reports tied to deepfake media over the past two years and the growing ability of fraudsters to create realistic, AI-generated documents, photos, and videos that deceive traditional KYC and due diligence processes.

[12] https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html

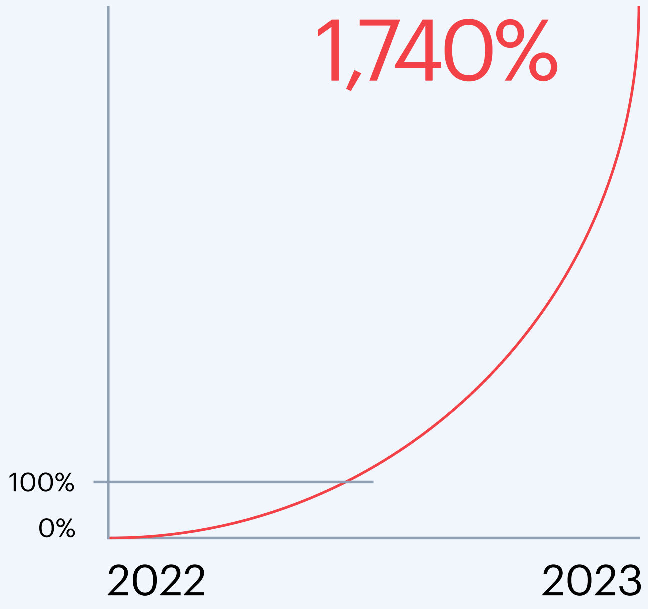
[13] https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence

[14] https://www.fincen.gov/system/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf

Deepfake Attacks Driving Corporate Impersonation Worldwide

Jack also watched as deepfake-enabled scams skyrocketed. In the first quarter of 2025 alone, losses from AI-generated CEO impersonation and other video-based fraud soared beyond $200 million, underscoring how easily advanced AI can fool legacy systems and human trust.[15]

In North America, deepfake-related incidents surged 1,740% between 2022 and 2023,[16] demonstrating how rapidly attackers adapt while defences lag behind.



Synthetic Identity Fraud Growing As The Silent Risk

Jack recognized that behind many loan defaults are identities that don't exist. The synthetic identities accounted for a record $3.2 billion in lender exposure by mid-2024, a 7% increase from the prior year, with such fraud rising 18% year-over-year.

Globally, this type of fraud is surging. Over 80% of all new-account fraud in the U.S. is attributed to synthetic identities, with average losses of about $15,000 per confirmed case.[17]

[15] https://variety.com/2025/digital/news/deepfake-fraud-caused-200-million-losses-1236372068/

[16] https://www.weforum.org/stories/2025/07/why-detecting-dangerous-ai-is-key-to-keeping-trust-alive/

[17] https://www.gci-ccm.org/insight/2024/07/rise-synthetic-identity-growing-threat-digital-age

6.0 How Weak Legacy Systems Gave Jack The Advantage

Jack realised that even high-risk companies were relying on off-the-shelf third-party vendors with stagnant fraud-fighting capabilities and no timely response mechanisms. This dependency limited their ability to adapt to emerging threats or collaborate effectively with stakeholders and detect advanced deepfake threats.

Meanwhile, fraud was evolving at scale, and criminals were innovating rapidly, while the tools designed to stop them remained static. The result was a widening gap where outdated defences left businesses increasingly vulnerable.

Weak Foundations In Identity Verification:

Most solutions lacked accuracy in verifying identities, struggling to detect synthetic IDs, manipulated documents, or sophisticated fraud schemes that bypassed traditional checks.

False Sense Of Security:

Many businesses assumed they were protected, yet evolving fraud tactics went unnoticed, creating hidden risks that exposed them to significant vulnerabilities.

Lack Of Coordination:

Vendors and businesses often failed to align solutions effectively, leading to gaps between product capabilities and actual fraud prevention requirements.

Static Solutions Vs. Evolving Threats:

Compliance-driven, box-ticking tools quickly became outdated, leaving businesses unprepared against rapidly evolving fraud tactics and cybercriminal innovation.

Dangerous Vacuum:

Fraudsters advanced faster than defenders, exploiting innovation gaps and creating a dangerous imbalance that left businesses vulnerable to constant threats.

The Shufti Playbook:

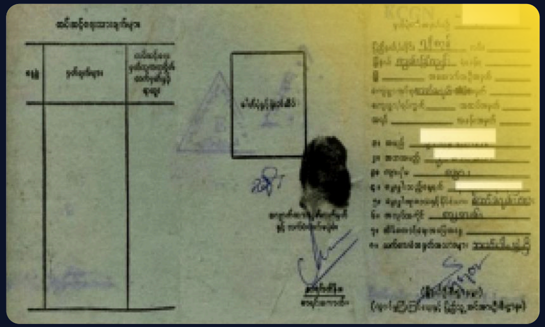
From Detection To Defense

Closing The 1% Gap Begins With Accurate And Customized Identity Verification:

Custom OCR Extraction

Generic OCR engines struggle with non-Latin scripts.

Example: An Arabic national ID is often misread by standard OCR, dropping characters or mistranslating fields. Our custom OCR, trained on complex scripts, extracts data with precision and prevents onboarding errors.



Verifying Complex Non-Latin Identity Documents

Challenge: OCR for Arabic scripts and cross-language names

Results: Reliable ID checks across UAE and MENA

Transliteration & Standardization

Spelling and script variations can bypass checks.

Example: A Japanese resident card showing “タナカ” (Tanaka) may appear as “Tanaka” or “Tannaka” when converted. Our transliteration engine standardizes names, ensuring consistent and accurate AML screening.

Japan's time warp

Challenge: The Reiwa era calendar system can confuse Western-trained AI4

Results: Context-aware processing handles any date format't

Verification Of Diverse IDs

Less-standard documents require specialized handling.

Example: A paper-based Myanmar household registration document could be dismissed by generic systems. Our template recognition validates these IDs, giving equal assurance across digital and paper-based formats.

Myanmar's paper trail

Challenge: 1950s handwritten documents with no digital standards

Results: Shufti's OCR reads what others can't

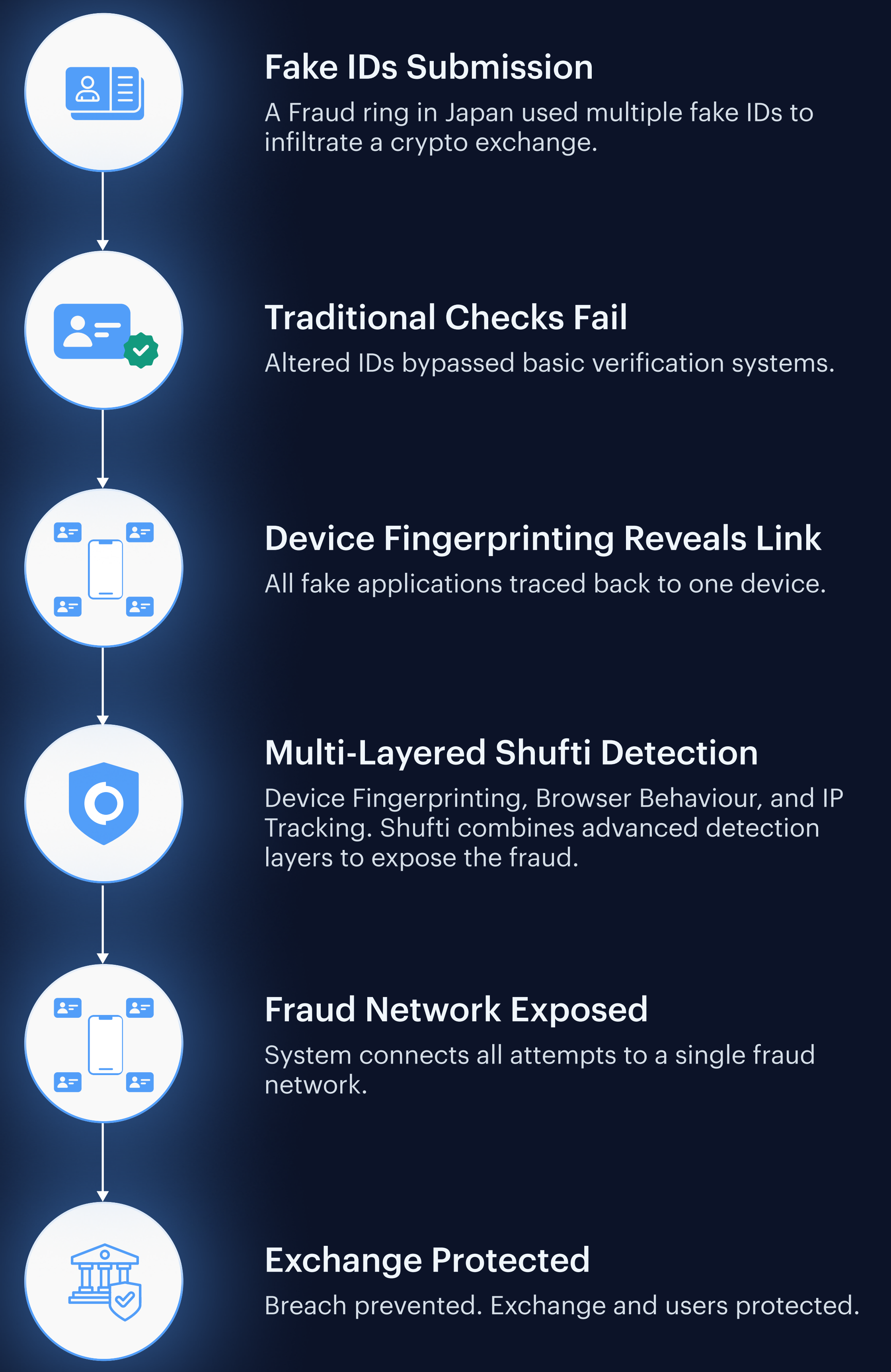
Shufti’s Multi-Layer Fruad Detection Strategy:

Breaking A Coordinated Network In Japan

Fraud today doesn’t happen in isolation but in a coordinated, calculated, and increasingly sophisticated way. A striking example emerged in Japan, where a criminal network attempted to infiltrate a leading crypto exchange using multiple, slightly altered original IDs. Traditional verification systems, built for compliance rather than resilience, failed to spot the deception.

Shufti’s **multi-layered detection strategy,** integrating device fingerprinting, IP intelligence, and browser behaviour analysis, shifted the balance. By connecting disparate attempts back to a single device, Shufti not only exposed the fraud ring but also demonstrated a critical truth:

Effective Fraud Prevention Demands Adaptive, Layered Defences That Evolve As Fast As The Threats Themselves.



Fake IDs Submission

A Fraud ring in Japan used multiple fake IDs to infiltrate a crypto exchange.

Traditional Checks Fail

Altered IDs bypassed basic verification systems.

Device Fingerprinting Reveals Link

All fake applications traced back to one device.

Multi-Layered Shufti Detection

Device Fingerprinting, Browser Behaviour, and IP Tracking. Shufti combines advanced detection layers to expose the fraud.

Fraud Network Exposed

System connects all attempts to a single fraud network.

Exchange Protected

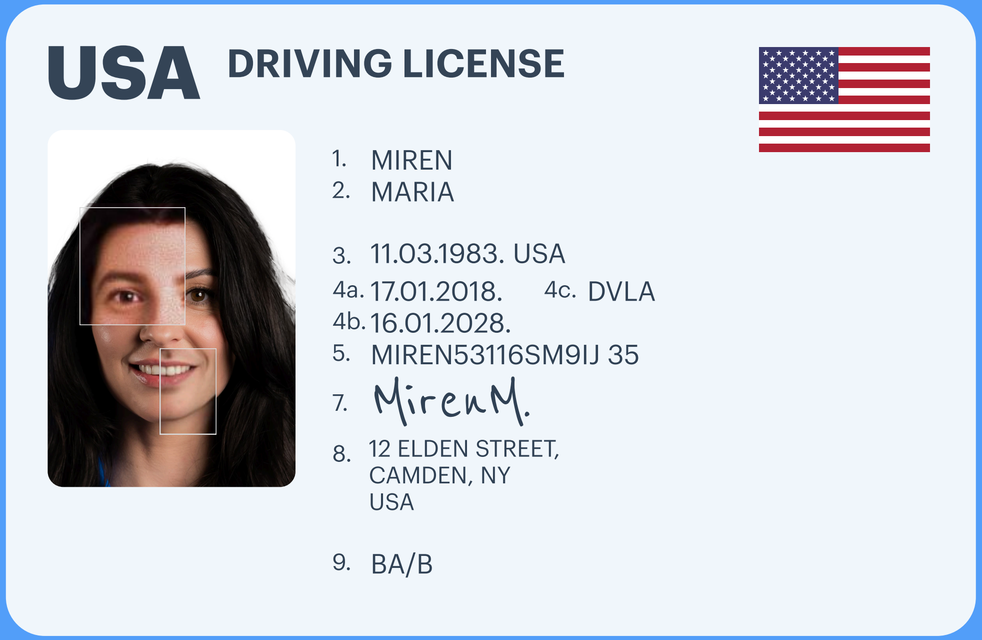
Breach prevented. Exchange and users protected.

Shufti's Recursive Method In Action:

Fighting Fraud In The Forex Sector

A Shufti client on a retail forex platform faced a deepfake attack. The attack pattern included a convincing ID by morphing the portrait through an AI face swap that blended a male face into a female template, so the image looked natural to standard checks. Because the selfie and the doctored portrait showed the same person, similarity scores spiked, increasing the chance of false acceptance. The submission evaded first line KYC and fooled basic face matching, showing how quickly gender swap morphs are advancing.

A recursive defense used layered forensic image analysis, liveness, attribute checks, and retrospective audits to expose the morphing artifacts in near real time and hence detected the attack. Shufti's R&D teams analyze the false declines in close collaboration with stakeholders, and then build template libraries to further train its machine learning models, reducing future fraud.

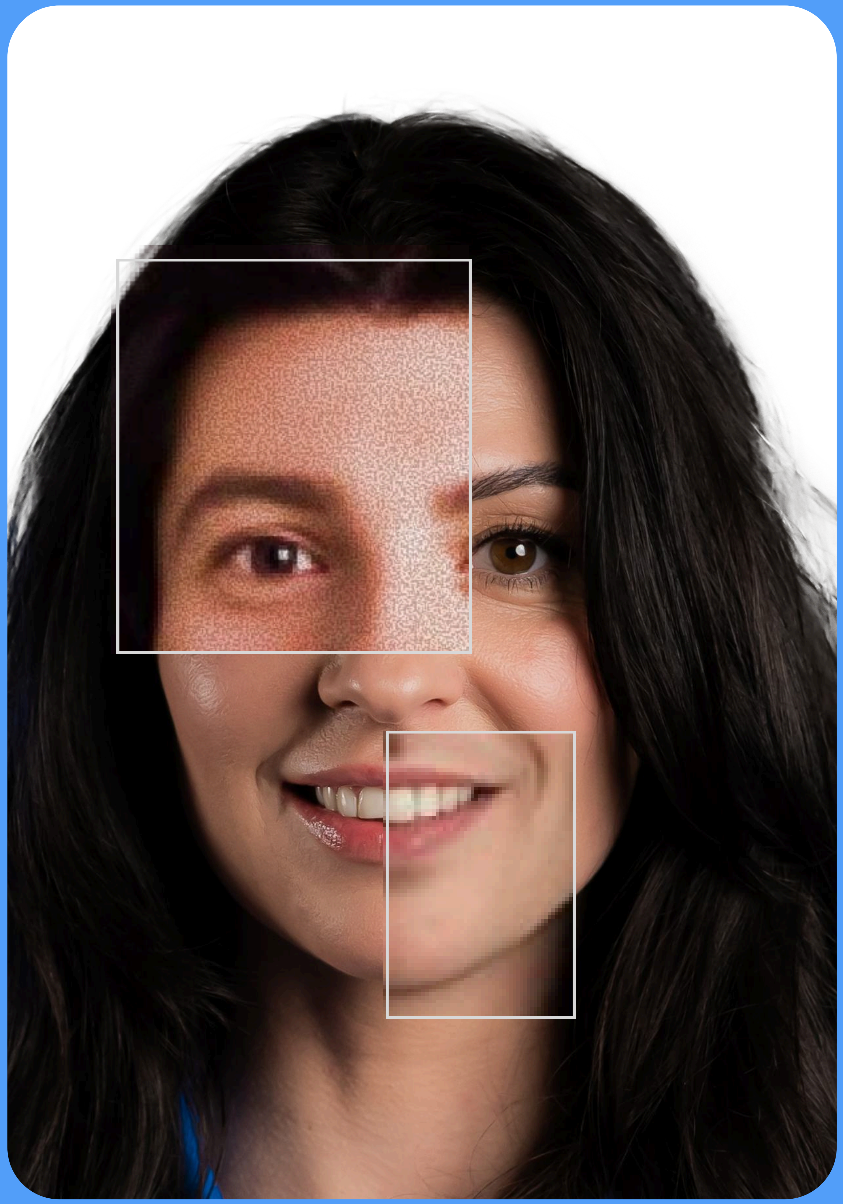


USA DRIVING LICENSE

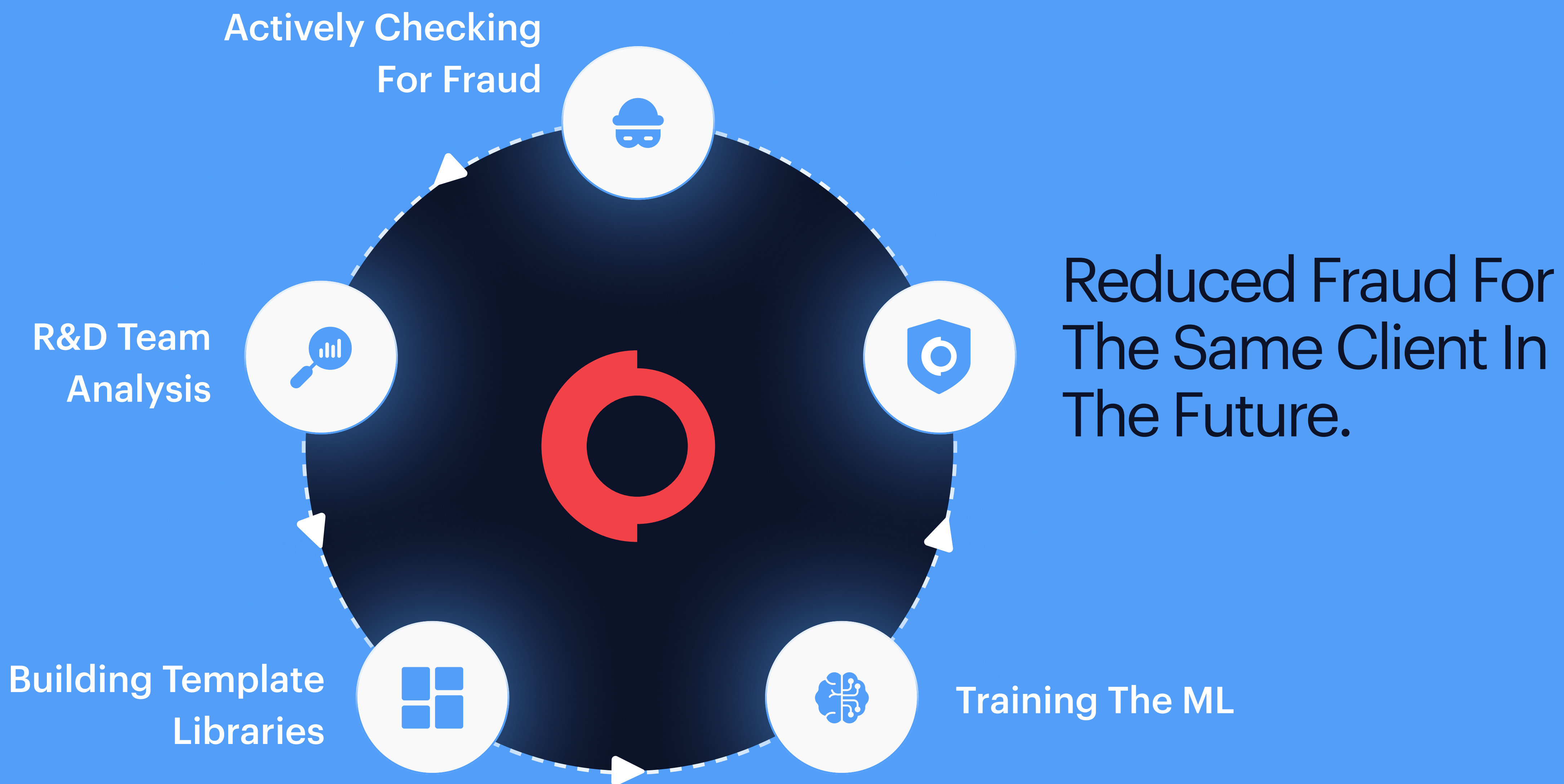
1. MIREN
2. MARIA

3. 11.03.1983. USA
4a. 17.01.2018. 4c. DVLA
4b. 16.01.2028.
5. MIREN53116SM9IJ 35
7. MirenM.
8. 12 ELDEN STREET,
CAMDEN, NY
USA

9. BA/B



Behind The Shield:
R&D Powering Shufti's Fraud Defense



Actively Checking For Fraud

Reduced Fraud For The Same Client In The Future.

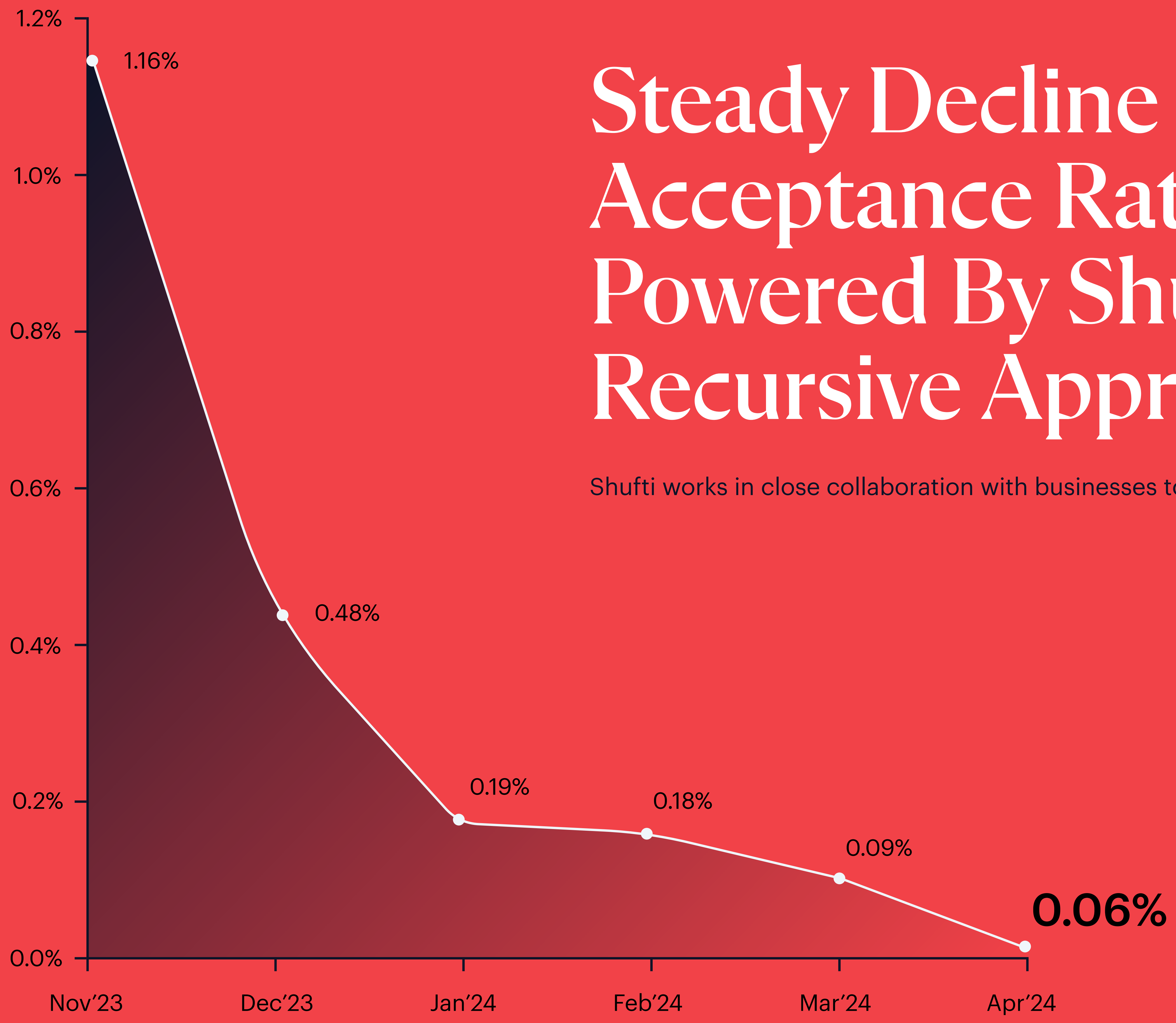
Training The ML

Building Template Libraries

R&D Team Analysis

Steady Decline In False Acceptance Rates Powered By Shufti's Recursive Approach.

Shufti works in close collaboration with businesses to keep fraud below 1%.



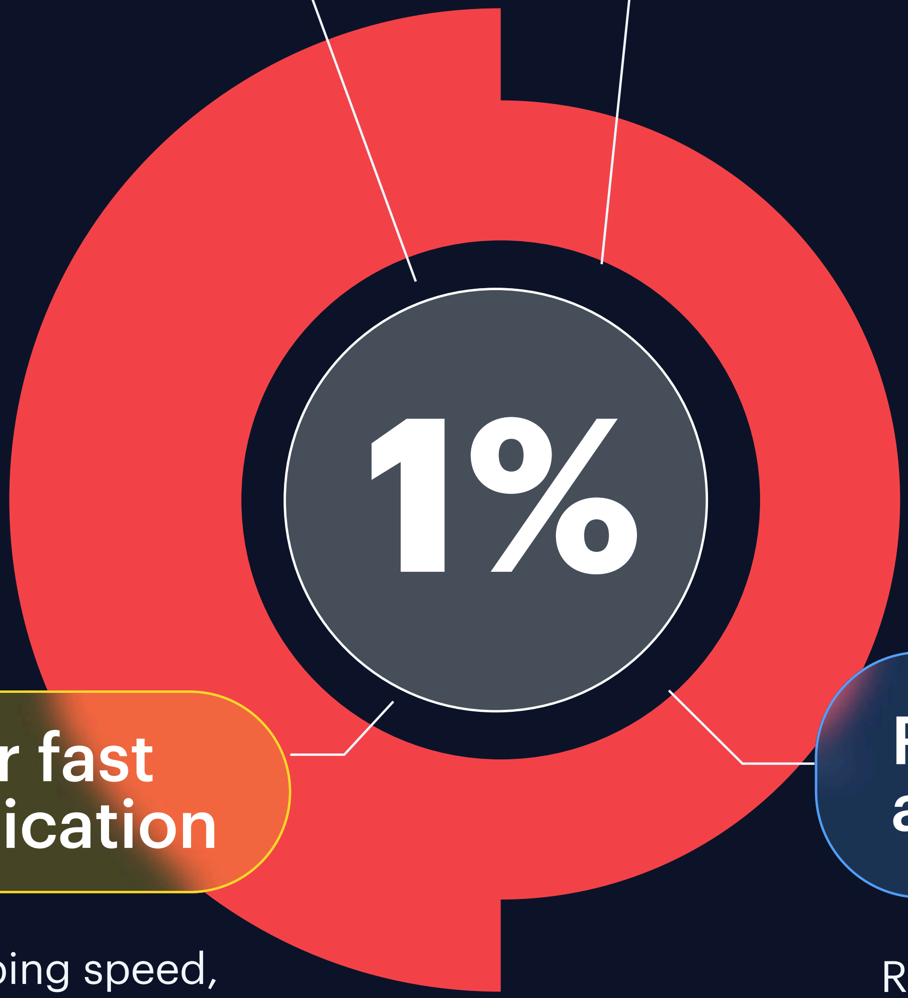
9.0 Shufti's Approach To Keeping Fraud Under 1%

Ensuring The Higher Levels Of Assurance In Authentication And Ensuring Security Throughout Customers' Lifecycle

Identity-related fraud is best prevented at two stages: first at onboarding, when synthetic identities and illegitimate users must be blocked, and then after onboarding, when genuine accounts must be protected from identity theft and takeover. Jack's attempts showed how quickly criminals exploit onboarding cracks, but Shufti ensures those cracks never become entry points.

Shufti delivers stronger assurance from the very beginning with layered document checks, facial biometrics, liveness with injection attacks and deepfake detection, device fingerprinting, and behavioural biometrics. This robust authentication framework at onboarding then underpins security across the entire customer lifecycle.

Fraud Prevention Across The Customer Lifecycle



Device fingerprinting to spot anomalous devices

Device signals (type, OS, browser, screen, locale, timezone), network intelligence (IP, ASN, region, proxy/Tor/VPN), and security posture (emulator, root/jailbreak) are compared against prior sessions, with suspicious patterns like a new device plus a new IP or impossible travel triggering step-up verification or blocks.

MFA and risk-based step-up when behavior or context changes:

Contextual signals such as new devices, unusual velocity, high-value actions, or atypical locations are continuously assessed. Low-risk sessions remain simple, while higher-risk sessions prompt stronger factors such as biometric approval, app-based confirmation, or OTP, depending on client policy.

Behavioral biometrics for fast and seamless re-authentication

Shufti analyzes keystroke rhythm, typing speed, swipe gestures, and device interaction patterns to detect anomalies.

Resilient account recovery anchored to onboarding signals

Recovery is tied back to the strong signals established at onboarding (live face re-verification, document checks) and compared against known device and network patterns.

About Shufti

Shufti keeps fraud under one percent by starting where it matters most, which is ensuring accuracy in legal identity document verification. Our **in-house tech** reads and validates more than 10,000 government issued document types across 240+ countries and territories, including nonstandard formats and complex scripts. Because the core stack is **built in house,** it is highly customizable to each client's flows and jurisdictions. Custom OCR, layout intelligence, and forensic checks catch what generic engines miss.

From there, we layer signals. Liveness and face matching work alongside device, behavioral, and contextual risk. When something looks off, we escalate to expert reviewers. That same customizability lets us quickly analyze similar attack patterns, build template libraries, and retrain our models. Prevention gets better with every iteration and fraud is stopped earlier.

This end to end loop keeps the false acceptance rate below 1% across deployments, and in some sectors as low as **0.06%,** while preserving conversion and the auditability regulators expect.

The Critical 1% That Matters