Shufti

Fortifying Telecom Infrastructure Against Identity Fraud

This document outlines a comprehensive framework for digital identity verification (IDV) tailored for government regulators and telecommunications operators. The proposed solution is designed to create a secure, centralized, and efficient ecosystem for SIM registration and management, effectively combating the rising threats of SIM-based fraud while promoting financial inclusion and digital transformation.

Trustpilot
4.8 ★★★★★ 3K+ reviews

Leading the Industry in Customer Satisfaction

PCI DSS · SOC2 · GDPR · QG GDPR · ISO 27001: 2013 · CE+ · iBeta Level 1 · iBeta Level 2 · KJM Verification age · CCPA

The global shift towards digitalization has positioned the telecommunications sector as the bedrock of a nation's digital economy. However, this critical infrastructure is increasingly targeted by sophisticated fraud. The current reliance on physical, in-person verification for SIM registration is not only inefficient but also vulnerable to identity fraud, including the use of forged, stolen, or synthetic identity documents. This vulnerability directly enables financial crimes, undermines national security, and erodes public trust.

Shufti proposes a strategic partnership to implement a multi-layered, AI-powered identity verification platform. This framework is engineered to solve the core challenges of remote identity proofing by establishing a robust, centralized system for all telecom operators.

Our Solution Will Empower You To

Mitigate SIM Registration Fraud

Implement a fully remote and automated onboarding process that verifies the authenticity of identity documents and the liveness of the user in seconds, effectively blocking fraudulent attempts at the source.

Build a Centralized Identity Database

Create a single source of truth for verified identities, preventing duplicate registrations across all network operators and enabling a robust, national fraud prevention mechanism.

Enhance National Security & Compliance

Screen all new subscribers against global Anti-Money Laundering (AML) watchlists, sanctions, and law enforcement databases in real-time.

Drive Digital & Financial Inclusion

Provide a seamless and accessible digital onboarding experience that works on any standard smartphone, removing the barrier of physical registration for citizens hampered by digital divides or biometric system failures.

Scale with Confidence

Leverage an infrastructure built to handle national-level demand, capable of processing over one million verifications per day without compromising speed or accuracy.

Understanding the Modern Threat Landscape

A successful national strategy must be built on a clear understanding of the evolving methods used by fraudsters to exploit telecom services.

SIM Registration Fraud:

Criminals use high-quality counterfeit, stolen, or synthetic identity documents to register new SIM cards. These cards are then used for a range of illicit activities, including financial scams, terrorism financing, and anonymous communication, making them untraceable to a real individual.

SIM Swap (Port-Out) Fraud:

A fraudster illegally convinces a mobile operator to transfer a legitimate user's phone number to a SIM card in the fraudster's possession. Once they control the phone number, they can intercept critical communications, including one-time passwords (OTPs) and two-factor authentication (2FA) codes, to gain unauthorized access to bank accounts, email, and social media.

Identity Theft & Duplication:

A single individual's identity is used to register dozens or even hundreds of SIM cards across various networks. This allows fraudulent enterprises to operate at scale while pinning the activity on an unsuspecting victim.

Shufti's Solution: A Multi-Layered Defense Framework

To combat these multi-faceted threats, a single layer of security is insufficient. Shufti provides a comprehensive suite of proprietary, in-house technologies that work in concert to establish identity with the highest degree of assurance.

Layer 1
Foundational Identity Verification

This initial layer ensures that every new subscriber is who they claim to be, stopping fraud before it enters the ecosystem.

ID Document Verification

Verifies the authenticity of government-issued identity documents (e.g., National ID cards, passports, driver's licenses) from over **245+ regions**. Our AI-powered forensic analysis performs over 100 validation checks, including forgery detection, layout analysis, and metadata inspection to identify even the most sophisticated fakes with **99.85% accuracy**.

Application to SIM Fraud

Rejects counterfeit and tampered documents instantly, preventing the registration of SIMs with fraudulent credentials. Our engine accurately extracts all data via Optical Character Recognition (OCR), supporting over **100 languages**, including non-Latin and handwritten scripts.

Facial Biometrics & 3D Liveness Detection

Irrefutably links the identity document to a live, physically present human being.
The system matches a live selfie against the photo on the ID document and performs a 3D liveness check to prevent spoofing attempts using photos, videos, masks, or AI-generated deepfakes. Our technology is iBeta Level 1 & 2 certified, achieving a total accuracy of 98.72% with a 0% False Acceptance Rate in testing.

Application to SIM Fraud

Prevents impersonation using stolen IDs and ensures the person registering the SIM is the legitimate owner of the identity. Our 1:N facial matching technology can also scan a central database to instantly detect and block an individual attempting to create duplicate accounts with different ID documents.

Layer 2

Enhancing Assurance & Authentication

These layers provide additional security during onboarding and for ongoing account management.

Two-Factor Authentication (2FA) Via OTP

Confirms ownership of a user's registered email address or phone number by delivering a time-sensitive one-time password (OTP) for verification.

Application to SIM Fraud

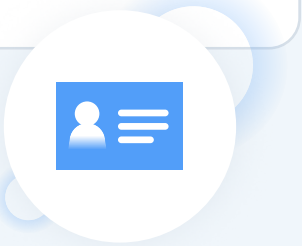
During onboarding, it confirms the user has access to the provided contact details. For ongoing security, it can be used to authorize high-risk transactions or SIM management requests, adding a critical layer of defense against account takeover after a SIM swap.

Electronic Identity Verification (eIDV)

Passively verifies user information extracted from their ID document against trusted independent data sources, such as government, credit, commercial, and utility databases. This is done in the background without requiring any extra steps from the user.

Application to SIM Fraud

Provides a powerful secondary check to confirm that the presented identity exists and is consistent across official records, flagging synthetic identities that may use a valid-looking but entirely fabricated document.



Layer 3

Proactive And Continuous Risk Monitoring

Security does not end at onboarding. This layer provides tools to detect suspicious behavior in real-time.

Behavioral Biometrics & Device Intelligence

Analyzes non-biometric data points to identify high-risk patterns. This includes device fingerprinting (to see if one device is registering many identities), IP address analysis (to detect the use of TOR, proxies, or data centers, or uncover inconsistent IP locations), and geolocation checks (to verify consistency with user profiles).

Application to SIM Fraud

Identifies and flags organized fraud rings that use a limited set of devices to register thousands of fraudulent SIMs. Mismatches between IP location and document origin can serve as an immediate red flag for review.

Anti-Money Laundering (AML) Screening

Screens individuals in real-time against over 1,500 global sanctions lists and law enforcement watchlists, with data updated within 24 hours.

Application to SIM Fraud

Prevents individuals linked to financial crime, terrorism, or other illicit activities from accessing the telecom network, directly addressing national security concerns and strengthening regulatory compliance.

Layer 4

Secure Digital Agreements

Electronic Signatures (E-Signatures)

Allows users to digitally and securely sign terms of service, contracts, or other agreements during the remote onboarding process.

Application to SIM Fraud

Creates a legally binding record of the user's agreement to the terms of SIM ownership, strengthening the operator's position in disputes and ensuring a fully digitized, auditable trail for every new subscriber.

Implementation Approach via Seamless API Integration

Shufti's solution is designed for rapid and secure integration into a national-level framework. The process is straightforward:

Step 1

Initiation

A user begins the SIM registration process through a telecom operator's web portal or mobile application.

Step 2

API Call

The application makes a secure API call to Shufti, initiating the verification journey.

Step 3

Identity Verification

The user is guided through the required steps (document capture, facial scan, etc.) within a secure environment powered by Shufti. All the multi-layered checks are performed automatically in an average of under 30 seconds.

Step 4

Secure Response

Shufti sends a final verification decision (accept/decline) along with detailed data and reasons back to your central identity database via API.

Step 5

Centralized Record

Your central system stores the verified identity data, creating a unique, fraud-proof record for that citizen.

Step 6

Duplicate Prevention

When that same citizen attempts to purchase another SIM from any operator, their facial biometrics can be checked against the central database to instantly flag and prevent a duplicate registration.

Orchestrating the Customer Journey with Shufti's Journey Builder

Shufti's Journey Builder empowers telecom operators to design, deploy, and manage fully customized identity verification workflows with minimal effort. Using Journey Builder offers a strategic advantage by enabling faster, more secure onboarding while enhancing customer satisfaction and regulatory compliance.

Key Benefits

Enhanced Customer Experience

Streamlined, intuitive onboarding reduces friction, helping operators improve conversion rates and retain subscribers.

Tailored Verification Paths

Configure workflows for document capture, facial biometrics, liveness detection, e-IDV, and AML checks to meet specific regulatory and operational requirements

Real-Time Previews

Test and refine workflows before deployment to ensure maximum efficiency and usability.

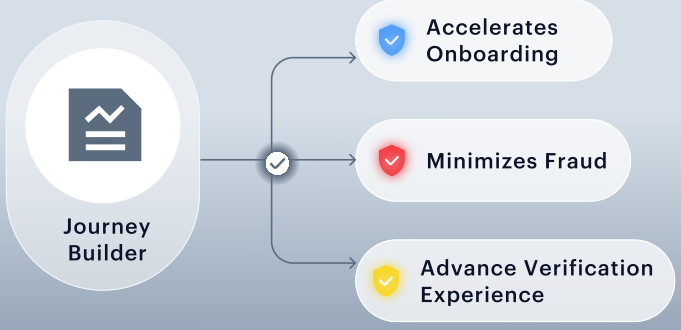
Flexible Integration Options

Launch verification journeys via secure API calls or direct links, supporting rapid rollout across multiple platforms and devices.

Scalable & Updatable

Easily adapt workflows as new use cases or regulations emerge, ensuring long-term operational efficiency and compliance.

By leveraging Journey Builder, telecom operators gain a centralized, flexible, and auditable solution.



Use Cases Beyond SIM Registration

Once a national digital identity framework is established, its applications extend far beyond telecommunications, becoming a catalyst for broad digital transformation:

Financial Services

Secure and remote onboarding for digital bank accounts, loan applications, and payment services.

E-Government Services

Digital access to government portals, tax filing, and social welfare programs.

Healthcare

Secure patient portals and remote access to medical records.

Education

Remote student verification and proctoring for online examinations.

Voter Registration

Creating a secure and verifiable digital voter roll.

The Shufti Strategic Advantage

Proprietary End-to-End Technology

We own our entire technology stack, giving us full control over security, performance, and the ability to rapidly adapt to new fraud threats without reliance on third-party vendors.

Unmatched Speed And Accuracy

Our fully automated system delivers verification results in an average of 28.2 seconds.

Our solution features iBeta Level 2 certified facial biometrics

And AI-powered forgery detection that catches 60% more fraud than human reviewers, on average.

Global Scale And Compliance

Trusted by over 1,200 global businesses, our solutions are built on a foundation of global compliance, including GDPR, ISO 27001, and PCI DSS. Our rating reflects our commitment to a superior user experience.

Proven Scalability

Our infrastructure is engineered to handle national-level transaction volumes, with the capacity to process over one million verifications per day.