Shufti

A SHUFTI FRAUD INTELLIGENCE REPORT

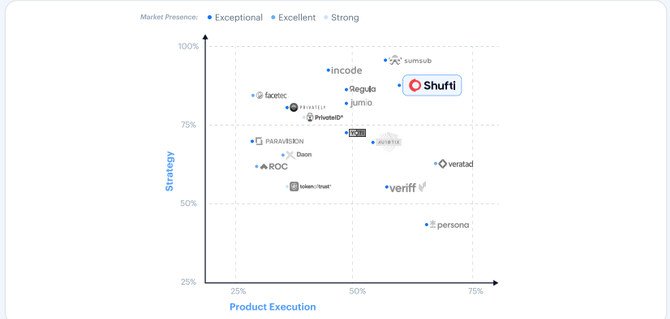
Forex Fraud Intelligence Report

Detecting multi account and fraud ring activity in Forex.

Industry Recognition 2025–2026

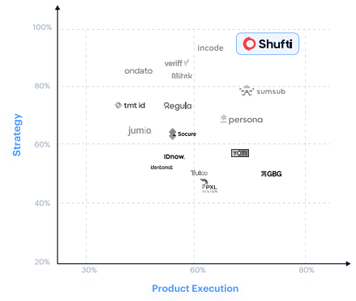
Recognised by leading analyst firms, government bodies and independent research organisations

Ranked Exceptional in Liminal's 2026 Age Estimation Index

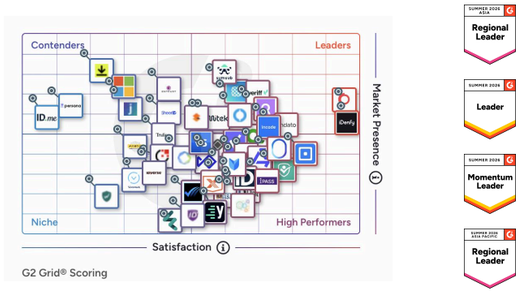


Ranked Exceptional in Liminal's 2026 Age Verification Index

Broadest global reach in the 2025 KuppingerCole Extended IDV report



Recognised as a Leader across four G2 Summer 2026 reports



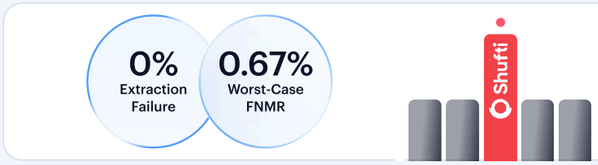
Differentiated by Gartner on document diversity and country coverage

First EU company to achieve iBeta Level 3 Conformance to ISO/IEC 30107-3, with 0% APCER

iBeta Level 3 Conformance

0% APCER

Ranked Top 5 in the DHS RIVR 2025 for identity validation



Contents

Six sections covering the fraud signals observed in Forex account creation during H1 2026, and how those signals can be assessed together.

The hidden patterns behind Forex account fraud

According to Shufti's Identity Verification Network data, fraud in the Forex sector during the first half of 2026 stood at 19.07%, highlighting the scale of fraudulent activity at the account creation stage.

The data indicates that fraudulent activity extends across several connected patterns, including duplicate identities, multiple account creation, coordinated fraud rings and geographic evasion. These patterns can create financial exposure for Forex firms when apparently separate accounts are connected through common identities, devices, registration behaviour or locations.

Historical fraud intelligence provides an additional indicator of repeat activity. 37.55% of Forex fraud was associated with identities with a previous history of fraud, demonstrating the importance of connecting new registrations with established fraud intelligence.

The analysis therefore focuses on how identity, device, velocity, IP and historical fraud signals can be assessed together to identify connected fraudulent activity while reducing the risk of legitimate customers being incorrectly rejected.

Three areas stand out in particular

Multi trader accounts

One individual can establish multiple accounts using the same identity. This creates opportunities for bonus abuse and for circumvention of the restrictions placed on a single account.

Fraud rings

Multiple traders can operate through shared infrastructure and closely timed registrations. Coordinated activity of this kind is difficult to identify when each account is assessed individually.

Geographic evasion

Location masking can obscure the origin of account activity. 3.68% of Forex fraud was associated with VPNs, proxies or anonymized networks, which makes connections between fraudulent registrations harder to establish.

Key Findings

19.07%
Fraud rate in the Forex sector

37.55%
Fraud associated with previous fraud history

4.49%
Fraud involving duplicate identity documents

3.68%
Fraud associated with anonymized networks

Methodology: Counting Fraud Through Corroborated Evidence

Scope of the Analysis

The analysis examines Forex onboarding activity during H1 2026 across 30 countries, focusing on the signals that can reveal duplicate account creation, connected fraud activity and geographic evasion.

Distinguishing Fraudsters from Legitimate Users: The Challenge

Several of these signals also appear in entirely legitimate use, which is what makes the assessment difficult. Customers may maintain multiple trading accounts in order to separate strategies, manage different portfolios or operate under different account structures, and a single device or network can be shared by household members, by colleagues, or by customers who were verified in the same location or through the same assisted onboarding process. A shared device count on its own therefore says nothing about whether the accounts behind it are fraudulent.

The Six Signals Assessed

Six signals are assessed together rather than in isolation: reuse of the same identity document across registrations, correlation between device fingerprints, the timing between connected registrations, IP intelligence covering VPN, proxy and anonymized network use, historical fraud associated with the identity, and resemblance to identity verification patterns already associated with fraud.

Why No Single Signal Is Conclusive

A connection is only treated as evidence of fraud once two or more of these signals corroborate one another, or where the identity carries an established history of fraudulent activity, and it is this requirement for corroboration that allows a fraud decision to be strengthened without rejecting legitimate customers whose activity produces one signal and nothing further.

Historical Fraud as an Additional Indicator

Historical fraud sits alongside the other signals rather than above them, and where an identity has been associated with fraud before, that record gives the assessment a reference point which a new registration on its own cannot provide.

37.55% of Forex fraud was associated with identities that had a previous history of fraud

Shufti

Three Prominent Patterns in Forex Fraud

Multi trader accounts through duplicate identities

Multi trader account activity creates exposure when the same underlying individual establishes multiple trading accounts while appearing to the Forex firm as separate customers.

Duplicate identities can be used to circumvent account restrictions, repeatedly access promotional incentives and fragment an individual's activity across multiple customer records. This makes it difficult to establish whether a new registration represents a genuinely new customer or an existing trader returning through another account.

4.49%

of Forex fraud involved duplicate identity documents

Loss to Forex Exchanges through Multi Trader Accounts

Where several accounts trace back to one trader, the firm applies limits, prices risk and pays acquisition costs against records that do not describe separate people. Promotional value is claimed repeatedly, and restrictions placed on one account are circumvented through another.

Customer histories fragment across those records, which weakens the view a firm holds of any individual trader. Previously fraudulent traders can also return through new registrations without that history following them.

Where the exposure shows up

Coordinated hedging across multiple accounts

Multiple accounts can take opposing or coordinated positions to reduce trading risk while exploiting bonuses or account structures. Detecting this requires connecting trading patterns, account relationships and promotional activity across accounts rather than assessing each one independently.

Hidden connections between apparently separate accounts

Two accounts may appear legitimate in isolation while sharing devices, IP addresses, identity details, payment information or trading patterns. Establishing whether those similarities reflect legitimate shared access or coordinated activity requires corroborating signals across the wider customer network.

Bonus abuse across connected accounts

Promotional incentives can be accessed repeatedly through several accounts used together. Identifying this requires connecting account, identity, device and trading relationships before promotional value is released, rather than investigating each account after the event.

Ring fraud

Fraudulent activity in the Forex sector is not limited to one individual opening several accounts. Groups of traders can register through common infrastructure and within narrow time windows, producing a set of accounts that appears independent when each registration is reviewed on its own.

The registrations described here were not classified as fraudulent because they shared a device. A shared device is treated as a starting point and nothing more. Every registration in this set was confirmed through corroboration, where the device link was accompanied by further evidence such as reuse of the same identity document, resemblance to identity verification patterns already associated with fraud, or an identity carrying an established history of fraudulent activity.

Within that confirmed set, registration velocity is tightly compressed. Accounts sharing a device were typically opened inside a 13 hour period, and a quarter of them inside a single 1.2 hour window. Additional signals were applied so that clusters arising from a shared corporate setting, where several employees are verified from the same office network and the same equipment, were not quantified as ring fraud.

Registration velocity within confirmed fraud

13 hours typical window across confirmed fraudulent registrations sharing one device

1.2 hours window containing a quarter of those same registrations

Loss to Forex Exchanges through Ring Fraud

Coordinated account creation scales fraudulent activity across multiple identities, and promotional or bonus value can be distributed across several accounts rather than concentrated in one. The exposure therefore grows with the size of the network rather than with the individual account.

Where each account is assessed independently, the relationships between traders remain concealed. Action taken against a single registration can leave the connected accounts active and trading, so the loss continues after the case appears closed.

Geographic evasion

3.68%

of Forex fraud identified during the first half of 2026 was associated with geographic evasion. These cases were detected through IP intelligence, which identifies registrations arriving through VPNs, proxy servers and other anonymized networks that conceal the address an account is operating from.

Location masking places distance between an account and its actual operating environment. Where the origin of a registration cannot be established, the firm loses a signal it relies on both for applying market access rules and for connecting one fraudulent registration to another.

Loss to Forex Exchanges through Geographic Evasion

Geographic restrictions can be circumvented where the true origin of an account is concealed. This exposes a firm to customers in markets it does not serve, and to the regulatory consequences that follow from onboarding them.

Location signals that conflict with identity and account information also reduce the value of the wider case file. Fraud investigations lose contextual information, and geographically distributed networks become considerably harder to connect.

Registration
Account created

›

VPN or proxy
Origin masked

›

Apparent IP
Seen by the firm

The address the firm observes belongs to the anonymizing service, not to the customer behind the registration.

Actual location, not observed

Connecting the signals behind Forex fraud

The findings show that fraudulent activity can manifest through multiple connected account behaviours. Duplicate identities can reveal repeat account creation, shared devices and registration velocity can expose relationships between traders, while anonymized networks can obscure the geographic origin of account activity.

Historical intelligence adds another layer of context, with 37.55% of Forex fraud associated with identities that had a previous history of fraud.

For Forex firms, combining these signals provides a broader view of the relationships behind account creation. Identity, device, IP and behavioural signals can be assessed together to establish stronger evidence of fraudulent activity while allowing legitimate customers to proceed when individual signals do not provide sufficient grounds for rejection.

37.55%

of Forex fraud was associated with identities that had a previous history of fraud

19.07%

fraud rate observed across Forex account creation in H1 2026

How to Assess an Identity Verification and Fraud Intelligence Solution

Solution assessment guide

In the Forex sector, identity verification is not simply a part of customer due diligence carried out to satisfy KYC and AML obligations. It is a safeguard against the financial loss caused by identity fraud, whether that fraud is committed by one individual operating several accounts or by a network operating together. It has to perform that role without penalising legitimate customers whose activity happens to resemble a fraud signal.

The right solution must therefore hold the following attributes.

Identity document coverage

Passports, national identity cards and residence permits verified across every market you onboard from.

eIDV and digital wallets

Identities confirmed against authoritative electronic data sources, with digital identity wallet credentials accepted.

Liveness and anti-spoofing

Presentation attack detection independently tested to iBeta Level 3 conformance rather than assessed in house.

Deepfake detection

Synthetic video, face swaps and camera injection attacks detected, not only printed photographs and screen replays.

Synthetic identity detection

Identities assembled from a mix of real and fabricated attributes identified before an account is opened.

Behavioural biometrics

Typing, navigation and interaction patterns assessed during onboarding alongside the document check.

Device fingerprinting

Devices fingerprinted so that separate registrations sharing the same hardware can be connected.

IP intelligence and spoofing checks

VPN, proxy and anonymized network use identified, along with attempts to spoof the address the firm observes.

1:N verification for deduplication

Each new face checked against every previously enrolled identity, not only the document presented with it.

Next steps

Speak to Shufti

Shufti is the trust infrastructure of the digital world. Its global platform was built from scratch and runs on technology developed in house, with no aggregators and no third party dependencies behind the verification stack.

The mission is to help digital first businesses meet compliance with convenience, so that regulatory obligations are satisfied without slowing down the customers a business is trying to onboard.

Fraud protection that evolves

Deepfakes, synthetic identities and account takeover attempts change faster than any fixed rule set can follow. Adaptive models are retrained as those patterns move, and independent testing at iBeta Level 3 conformance for presentation attack detection returned a 0% attack presentation classification error rate.

The platform in numbers

240+

countries and territories covered for document verification

10,000+

global documents used to train Shufti AI, which learns new formats through zero shot learning

150+

languages supported across verification flows

2,000+

businesses verifying their customers through the platform

Who Shufti already serves

2 of the top 3 global crypto exchanges
60% of Europe's leading Forex exchanges
The number one social platform by daily active users
The number one payment infrastructure platform

Alongside iGaming operators, marketplaces, banks and fintechs across regulated markets.

shuftipro.com

This report examines Forex onboarding activity during H1 2026 across 30 countries.