

TRUST GRID

Securing Digital Onboarding in the Age of Deepfakes

Why BFSI Needs More Than Video KYC

India's digital financial ecosystem has transformed customer onboarding. Every day, millions of Indians open bank accounts, apply for loans, purchase insurance products, and invest through entirely digital journeys.

That trust has traditionally been built on one assumption: the person appearing during identity verification is genuine.

Today, that assumption is being challenged.

Following recent regulatory amendments by India's Ministry of Electronics and Information Technology (MeitY) on synthetic media, deepfake-enabled identity fraud has evolved from a theoretical concern into an operational risk for India's BFSI ecosystem.

Every day, millions of Indians open bank accounts, apply for loans, purchase insurance products, and complete digital identity verification directly from their smartphones. The trust that powers this digital economy relies heavily on one assumption: that what appears on screen is genuine.

That assumption no longer holds true.

Deepfake technology has made it possible to fabricate highly convincing videos, voices, and facial movements that are difficult to distinguish from genuine interactions. For banks, NBFCs, insurers, fintechs, and investment platforms, the challenge is no longer simply verifying who a customer claims to be. It is proving that the identity evidence itself is authentic.

The conversation around digital trust has moved beyond identity verification and into identity provenance.



How Deepfake Fraud Works

To defend against synthetic identity attacks, enterprises must first understand how they operate.

A deepfake is not a manipulated image or a simple video filter. It is synthetic media generated using advanced AI models capable of recreating human appearance, expressions, and voice characteristics with remarkable accuracy.

Fraudsters typically execute attacks in four stages:



Data Collection

Images, videos, and voice samples are collected from social media profiles and publicly available sources.



Synthetic Generation

AI models are trained to replicate facial structures, expressions, and voice patterns.



Real-Time Impersonation

During a Video KYC session, fraudsters deploy face-swap technology or synthetic avatars capable of responding in real time.



Identity Abuse

The fabricated identity is then used to obtain loans, open mule accounts, or bypass onboarding controls.

The result is a successful verification performed on an identity interaction that was never real in the first place.



Why Traditional Video KYC Is No Longer Enough



When RBI formalized the Video-Based Customer Identification Process (V-CIP), the fraud landscape looked very different.

Most verification systems relied on basic liveness detection techniques such as blinking, smiling, or head movement challenges to distinguish real customers from static images.

Modern deepfake attacks are designed specifically to bypass these controls.

Rather than presenting manipulated videos through a physical camera, sophisticated fraud networks inject synthetic video streams directly into the verification workflow, allowing fabricated identities to appear legitimate to both human agents and legacy systems.

In this environment, proving that a verification occurred is no longer sufficient.

Enterprises must now prove that the verification itself was authentic.

The Cost of Synthetic Identity Fraud

As the RBI has repeatedly emphasized in the context of digital transactions and identity risk, institutions must remain vigilant against misuse of financial systems. Failure to detect synthetic identities during onboarding creates significant business and regulatory consequences.



Loan Defaults

Fraudsters obtain unsecured loans using fabricated identities, leaving institutions with unrecoverable losses.



Money Laundering Risks

Synthetic identities enable the creation of mule accounts used for illicit financial activity.



Regulatory Exposure

Financial institutions are expected to continuously strengthen KYC controls to address emerging fraud vectors.



Reputational Damage

A single high-profile onboarding fraud incident can erode customer trust and attract regulatory scrutiny.

For compliance and risk leaders, synthetic identity fraud is no longer an emerging threat category. It is an active operational challenge.

Why Enterprises Need Identity Orchestration

- Many institutions respond to emerging fraud by adding individual point solutions whenever a new threat appears.
- The problem is not the absence of security tools.
- The problem is fragmentation.
- Deepfake attacks exploit the gaps between disconnected systems, where device intelligence, identity verification, fraud detection, and compliance workflows operate independently of one another.
- This is where identity orchestration becomes critical.
- An orchestrated identity framework coordinates every trust signal into a unified verification journey, ensuring that fraud controls operate together rather than in isolation.

The Future of Identity Verification

Synthetic media has fundamentally changed the economics of digital trust.

For BFSI institutions, manual review and traditional verification controls are no longer sufficient to defend against increasingly sophisticated identity fraud.

The organisations that lead in digital trust over the coming decade will not simply verify who someone is.

They will verify that what they are looking at is real and that every identity claim can be independently proven.

By combining orchestration through Protean RISE with emerging trust frameworks such as Verifiable Credentials, enterprises can build onboarding journeys that are resilient against synthetic fraud, aligned with regulatory expectations, and designed for the next generation of digital identity.

Because in the age of deepfakes, trust cannot rely on what we see.

Trust must rely on what we can prove.



Moving Beyond Detection to Trust by Design

While anti-spoofing technologies and fraud analytics remain essential, the long-term future of digital trust lies in reducing dependence on visual verification altogether.

Emerging identity ecosystems are increasingly adopting cryptographically verifiable identity credentials issued by trusted authorities and validated in real time.

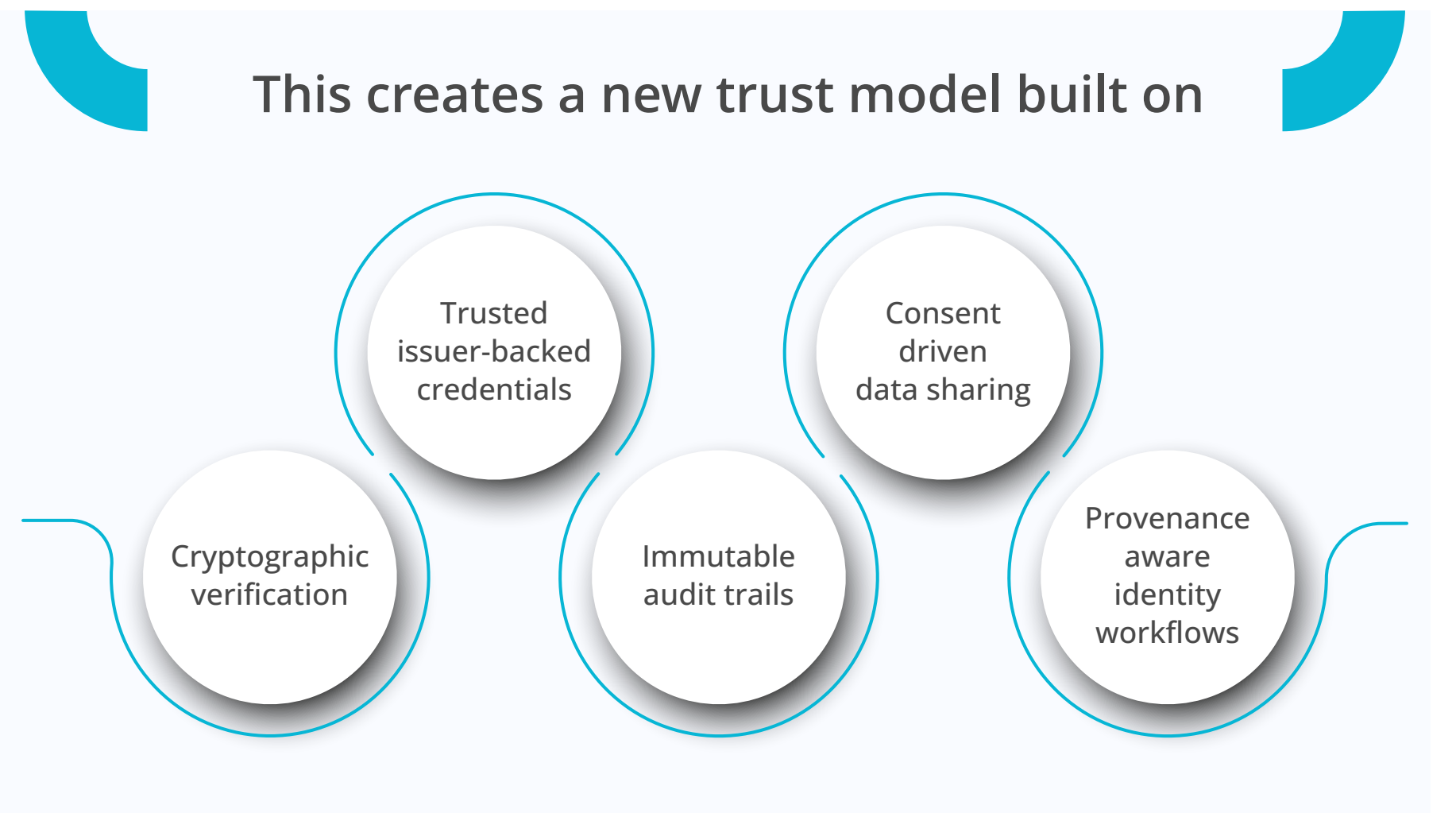
“

Instead of asking:
"Does this face look real?"

The question becomes:
"Can this identity attribute be cryptographically proven?"

”

Verifiable Credentials enable organisations to validate trusted customer attributes directly from credential issuers while maintaining integrity, provenance, and tamper resistance.



The shift is fundamental.
Digital identity is moving from trust based on appearance to trust based on proof.

- Building Multi-Layered Trust with Protean RISE**

Protean RISE enables enterprises to build layered trust across digital onboarding journeys through a unified API orchestration framework.

The platform combines multiple verification and fraud intelligence capabilities into a single workflow designed for modern identity threats.
- Deep Device Integrity Checks**

Before a verification session begins, the platform analyses devices for virtual camera drivers, emulators, screen injection tools, and other indicators of manipulation.
- AI-Powered Anti-Spoofing Intelligence**

Advanced algorithms analyse video streams at a pixel level to identify visual inconsistencies, facial blending artefacts, unnatural lighting patterns, and audio synchronisation anomalies commonly associated with deepfakes.
- Intelligent Network Analysis**

IP intelligence and geolocation checks help identify suspicious access patterns, foreign VPN usage, and potential violations of V-CIP requirements.
- Adaptive Risk-Based Verification**

Where risk indicators exist but fraud cannot be conclusively established, additional verification layers such as DigiLocker integration, Aadhaar Offline Verification, or document validation can be dynamically triggered. This helps organisations strengthen trust without adding unnecessary friction for genuine customers.