

CAMERA HARDWARE-ANCHORED IDENTITY VERIFICATION IN THE AI ERA

AI fakes the customer. Only the camera sensor proves them.

Financial institutions face a surge in AI-driven attacks — identity theft, phishing, synthetic accounts. ToothPic binds every transaction to a **specific physical device** using the microscopic optical noise of its camera sensor (PRNU): multi-account enrolment and money-mule operations on the same hardware are flagged instantly, while legitimate users are approved at a higher rate.

3–5%

of total IT budget already spent on fraud prevention

49%

of transaction-monitoring alerts are false positives

54%

of good customers rejected by overly strict rules

95%

of institutions still rely on MFA as the main defence

Threat alignment & market realities

Fraud & risk officers · AI escalation & mule networks

Phishing and social engineering have spiked sharply, while synthetic accounts created during KYC slip past standard verification.

ToothPic: fingerprints the physical camera. One phone enrolling or managing multiple fake accounts is detected and alerted automatically.

IT & CISO · AI cyber investment & system integration

GenAI and security analytics are the #1 priority in bank cybersecurity budgets, yet integration remains the top transaction-monitoring hurdle (71%).

ToothPic: runs alongside existing risk engines without altering system architecture — predictable scaling, no per-transaction fee.

Securing banking identity at the hardware sensor level

The failure of standard MFA in the AI era. 95% of institutions rely on MFA as their main pre-emptive defence, yet generative AI bypasses software OTPs, synthetic documents and behavioural biometrics.

The unclonable hardware anchor. ToothPic operates at Layer 1 — the hardware sensor. Capturing photon interactions on the physical camera chip, it reconstructs credentials in memory, validating real device origin and stopping injection and emulator attacks cold.

7 · AI / GenAI fraud layer

Vulnerable: synthetic IDs, deepfakes, OTPs

6 · Banking mobile app

5 · Anti-fraud risk engine

4 · Mobile OS

3 · Camera driver

2 · Firmware

1 · Physical camera sensor (PRNU)

ToothPic trust: unclonable optical fingerprint

Strategic business value & key anti-fraud metrics

01**Maximise approval rates & revenue**

Approval rate is a primary success metric (**69%**). A definitive hardware trust score helps approve good transactions that would otherwise be blocked.

02**Prevent legitimate customer rejection**

Incomplete information (**61%**) and strict rules (**54%**) turn away good users. Implicit hardware verification adds no disruptive friction.

03**Money mule & multi-enrolment detection**

Identifies when a single physical smartphone is used across multiple user enrolments or accounts, stopping organised money-mule rings immediately.

04**Reduced false positives & analysis costs**

Cuts monitoring false positives (**49%**) and lowers per-analysis investigation costs for understaffed fraud teams.

Step-by-step device identity & fraud prevention flow

00**KYC enrolment**

During onboarding the app extracts the camera's unique PRNU hardware fingerprint.

01**High-risk trigger**

User initiates a sensitive transaction, wire transfer or account change.

02**Photon validation**

The app takes a seamless background photon capture to verify physical sensor presence.

03**Cross-device check**

The anti-fraud engine checks the fingerprint against the multi-account registry.

04**Risk decision**

Approve a single legitimate device, or alert when one device spans many accounts.

ADDRESSING ANTI-FRAUD MARKET CHALLENGES WITH TOOTHPIC TECHNOLOGY

Four market realities. One hardware answer.

MARKET CHALLENGE & DATA REALITY	TOOTHPIC ANTI-FRAUD IMPACT
Legacy MFA vulnerability 95% of enterprises use MFA as their primary pre-emptive defence. But GenAI voice cloning, presentation and injection attacks make standard MFA insufficient to guarantee legitimacy.	Unclonable MFA enhancement ToothPic anchors MFA directly to the smartphone's physical optics (PRNU). AI software bots and deepfakes cannot replicate physical silicon sensor flaws, reinforcing standard MFA to absolute hardware integrity.
Good customer rejection in KYC Overly stringent verification criteria (54%) and incomplete customer data (61%) cause institutions to reject legitimate accounts during KYC/KYB.	Zero-friction contextual signal ToothPic adds a deterministic device identity signal in the background. Anti-fraud engines can confidently approve legitimate applicants without subjecting them to complex manual checks.
Transaction monitoring friction Top monitoring challenges include system integration complexity (71%), high transaction volumes (65%) and excessive false positives (49%).	Seamless integration & noise reduction Requires no changes to core architecture. ToothPic dramatically reduces false-positive noise, letting understaffed fraud teams focus purely on high-probability fraudulent attempts.
Money mules & synthetic IDs Fraudsters create synthetic identities during KYC (56%) and operate money-mule networks using single devices to control dozens of accounts.	Hardware multi-account alerting Because ToothPic identifies the exact physical phone camera, any attempt to register or operate multiple profiles from one single device is instantly flagged as a syndicate / mule risk.

Global scale & ongoing enterprise deployments

India · 400M+ user base Major Indian fintech infrastructure integration Currently integrating ToothPic directly inside the core mobile payment stack. The implementation radically elevates device-binding capability, preventing unauthorised multi-account operations across high-throughput payment networks.	Indonesia · 200M user base Indonesian fintech anti-fraud optimisation Partnered to optimise transaction analysis by eliminating false-positive triggers and cutting unnecessary manual verification steps. Automated hardware validation substantially lowers operational case-management and anti-fraud costs.
--	---

Validated. Certified. In production.

Gartner Sample Vendor, Emerging Tech Impact Radar: Disinformation Security, 2026	4 patent families US · EU · IT · CN · JP · IL · KR — 20-year terms	FIDO2 + U2F Certified. Politecnico di Torino spin-off, 2 EIC Seals of Excellence	4 paid EU deployments Insurance, payments and academia — live in production
--	--	--	---

90 days to proof. One flow. Your own data.

Listening mode: the signal runs beside your current controls and writes to a log, not to a decision. Nothing is decided, so nothing can go wrong for a customer. Existing controls stay live and reversing costs one sprint.

EMAIL

info@toothpic.eu

WEB

www.toothpic.eu