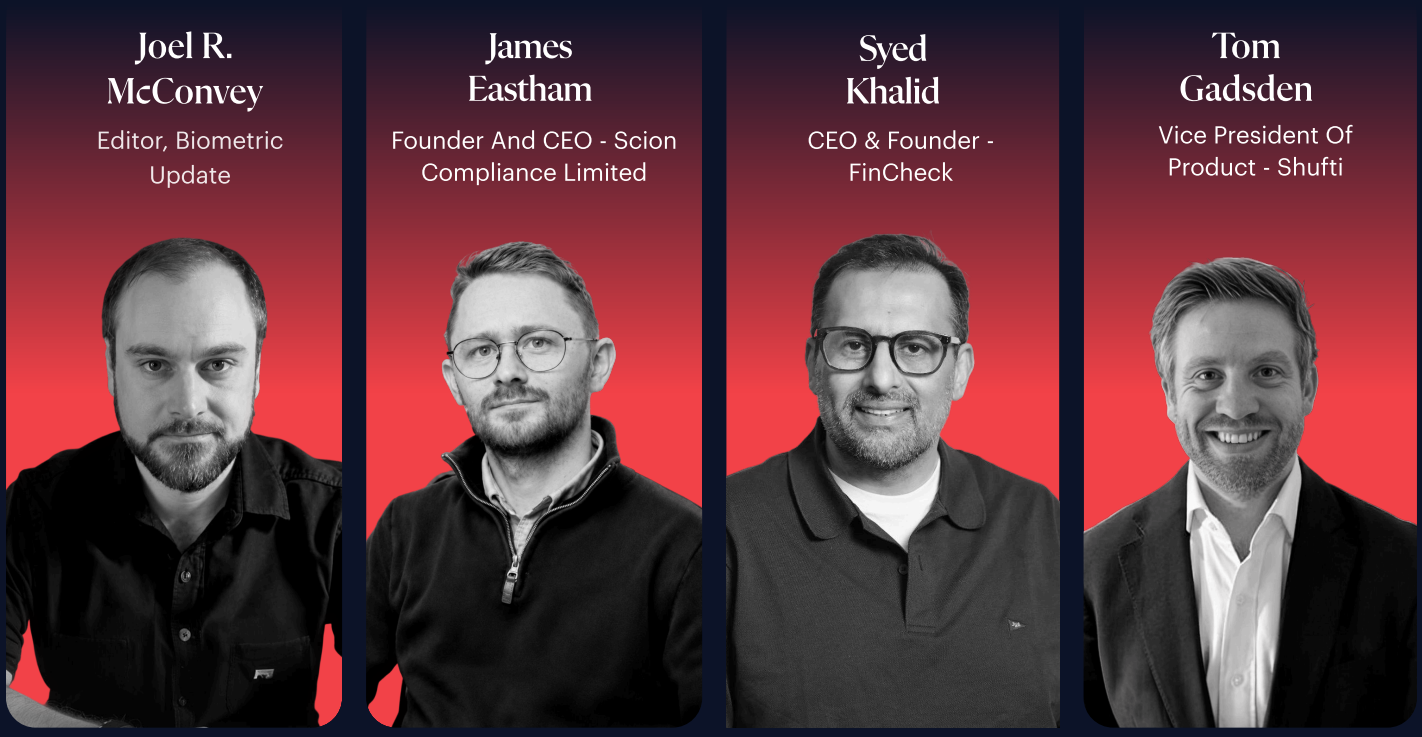
Shufti | BIOMETRIC UPDATE.COM

FRICTION VS FRAUD

How Much Security Is Too Much?

WATCH WEBINAR HERE

www.shuftipro.com



OVERVIEW

Fraud prevention and customer experience have long been treated as opposing forces. Tighten controls, and you lose customers to drop-off, loosen them, and you expose the business to account takeover, synthetic identity fraud, and AML penalties. For most digital businesses, that tension has become one of the defining product challenges of onboarding and growth.

In this webinar, hosted by Shufti and **Biometric Update,** our experts set out to challenge that dichotomy. The discussion reframed friction-versus-fraud not as a risk problem but as a product problem, where the KPI that matters is the joint outcome of approval rate and loss rate, not either one in isolation.

The conversation explored the real business cost of friction, the cost of having too little of it in an era of industrialized AI-driven fraud, where biometrics and digital identity move the curve, and how a risk-based, calibrated approach lets businesses protect themselves without turning good customers away.

DISCUSSION POINTS

Fraud and friction are not a binary choice.

Tom Gadsden set the context for the discussion, arguing that recent advances let businesses address both pressures at once rather than trading one for the other:

"Fraud and friction are both important, but we can break through both with recent breakthroughs and what's coming around digital identities, ongoing monitoring, and considering the subject holistically."

Friction is about timing, not volume.

The panel agreed that high-value and institutional customers expect to be asked questions, but not to be stopped mid-transaction. Where checks sit in the journey, matters more than how many you run.

James Eastham explained why friction belongs at the start:

"Businesses want that friction at the start, front-load that friction, because when I start moving money, I want to be able to do it in a really streamlined fashion."

What looks like friction is often a safety net.

From a compliance officer's seat, the cost of getting it wrong runs in both directions, and onboarding controls protect against a far larger bill of fines, remediation, and reputational damage.

Syed Khalid reframed how the business should view those steps:

"From a business perspective these look like friction, but to be honest, these are safety nets that protect you from bigger issues."

Fraud has industrialized.

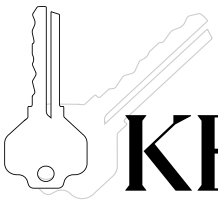
Sophisticated attack tooling, which was once the domain of specialists, is now widely accessible, pushing fraudulent attempts from a manageable fringe to a structural threat across customer bases.

Tom Gadsden described the shift:

"The percentage of fraudulent attacks we see is around 20% plus. This is really industrialized, and the relative sophistication has really risen."

Challenges Discussed

- Onboarding drop-off carries a direct competitive cost, and even a small abandonment gap can separate a hyperscaling business from one falling behind.
- AI-driven, industrialized fraud, including deepfakes, injection and presentation attacks, and synthetic identities, now targets even low-value accounts to stand up mules and drop accounts.
- Friction applied in the wrong place punishes genuine customers, with high-value and institutional users facing declines and delays when checks come too late.
- Rules-based monitoring and disconnected lines of defense generate false positives and create gaps behind many of the largest fines.



KEY TAKEAWAYS

- Optimize the joint outcome: measure approval rate and loss rate together, not either one alone.
- Make friction risk-based and dynamic, and front-load it at onboarding so genuine customers move freely afterward.
- Too little friction has its own risk. A frictionless journey can cause drop-off and erode trust, because customers, especially high-value ones, expect to feel secure and want to be asked the questions.
- Treat friction as protection, because direct fraud loss is only a fraction of the true cost once fines, remediation, and reputation are included.

ABOUT US

Shufti is a global identity verification platform built on fully owned technology, helping businesses strengthen onboarding, fraud prevention, and compliance at scale, without forcing a trade-off between security and growth. Backed by iBeta Level 3 conformance under ISO/IEC 30107-3, Shufti delivers independently validated liveness detection for advanced spoofing and AI deepfake threats.

- One platform, fully owned technology for greater control, flexibility, and consistency across the verification journey.
- Global coverage with real local depth, supporting 10,000+ document types across 220+ countries and in-house OCR across 150+ languages.
- Flexible deployment options, including local cloud and on-premises deployment, to support data residency, security, and enterprise compliance needs.

What We Deliver

- End-to-end identity verification with passive liveness and deepfake detection to counter industrialized, AI-generated fraud.
- Risk-based, dynamic friction that applies the right level of checking to the right customer at onboarding and across the lifecycle.
- In-life biometric re-identification and step-up authentication to detect mule and drop accounts and prevent account takeover.
- Hybrid KYC and AML orchestration that combines identity, transaction monitoring, fraud signals, and audit-ready controls for stronger compliance and smoother conversion.

JOIN THE SHUFTI COMMUNITY

Stay connected for expert insights, regulatory analysis, and practical guidance on compliance, AML, and digital identity.

Follow us. Learn with us. Grow with us.

Shufti on Website | Shufti on LinkedIn | Shufti on Twitter/X | Shufti on Facebook | Shufti on YouTube