Shufti

IF YOUR VERIFICATION SYSTEM IS 99% ACCURATE, ARE YOU REALLY SAFE?

WEBINAR LINK

Roger-Redfearn-Tyrzyk

CCO At Shufti

Moderator

www.shuftipro.com

Ray Blake

FinCrime Expert At RiskAlert247

Roger-Redfearn-Tyrzyk

CCO At Shufti

Andrei Sribny

CEO At AML Certification Centre

OVERVIEW

Shufti brought together frontline practitioners to unpack what really sits behind the last, most dangerous area of fraud and financial crime risk.

Instead of debating headline accuracy numbers, the panel looked at how governance failures, jurisdiction-specific weak spots, and human factors quietly create the small openings criminals exploit.

Moderated by Roger Redfearn-Tyrzyk, the session brought together:
Ray Blake, who works at the intersection of financial crime intelligence, regtech, and corporate risk through The Dark Money Files and Risk Alert 247.
Andrei Sribny, whose AML Certification Centre trains thousands of professionals across the first, second, and third lines of defense worldwide.

Together they examined:

- Why does the 1% gap created by governance and people, not just tech?
- How do criminals exploit weak jurisdictions instead of strong tools?
- What do regulators now expect for speed, accountability, and human judgment?
- How can firms balance conversion, customer experience, and regulatory risk?

DISCUSSION POINTS

The 99% myth and the global nature of fraud

- Identity fraud evolves faster every year than the systems meant to stop it, from deepfake-driven impersonations to AI-built synthetic identities.
- Fraud is a cross-border enterprise. Criminals do not respect geographic boundaries; they exploit jurisdictional gaps and target the weakest point in any chain of controls.

Governance, not technology, creates the 1% gap

Andrei Sribny stressed that the AML/KYC gaps are rarely a pure technical limitation:

- Many firms buy advanced tools, yet their policies, ownership, and review cycles are years out of date.
- Control ownership is vague, escalation paths are unclear, and review cycles lag behind evolving typologies.
- The result is predictable exposure: the system has capacity, but the organization does not use it properly.

Keeping up with fraud typologies and risk intelligence

- Internal historical cases are not enough. New fraud types may simply not have reached your organization yet.
- Emerging realities are reshaping the threat landscape: synthetic identities, money mule networks 2.0, and deepfake-assisted onboarding.
- The hardest layer to manage is real-time global intelligence on typologies and methods. Few organizations have a clear view of what is happening outside their own four walls.

Regulation alone is not a silver bullet

Ray highlighted that more regulation by itself has never solved financial crime:

- The last 30 years have proved that increasing the volume and detail of compliance regulations does not automatically lower crime.
- Regulatory regimes expect a risk-based approach and clear ownership of risks and controls.
- Regulators do not hold systems accountable. They hold people and firms accountable for how they use those systems.

Legacy stacks and the reality of transformation

- Newer firms can adopt integrated systems from the start, while large incumbents must modernize without slowing down operations.
- Adding new technology to old infrastructure is complex, which makes ongoing calibration and strong human oversight essential.

Challenges Discussed

Jurisdiction-Specific Weak Points:

- Fraudsters rarely attack the strongest part of a system; they exploit the weakest.
- They establish identities in countries with weaker document or registry standards, then use them in stricter markets.
- A verification flow is only as strong as the weakest jurisdiction feeding into it.

Fragmented Internal Controls:

- Onboarding, AML screening, KYB, and fraud detection often operate in silos, limiting visibility across the customer lifecycle.
- The 1% gap frequently emerges in the blind spots between these disconnected controls.

Rising Regulatory Expectations:

- Recent enforcement actions show a clear shift: having the right IDV tools is no longer enough.
- Regulators now expect consistent, timely action, and delays alone can lead to significant penalties.

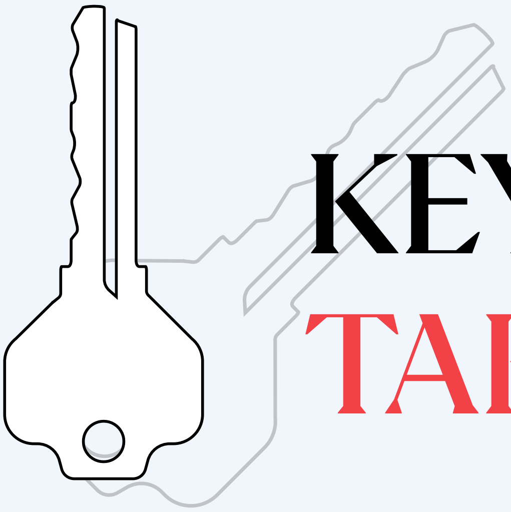
Insights From the Discussion

Digital Identity and Registry Reform

- The UK’s new corporate transparency requirements—mandating identity verification for directors and PSCs—are reshaping KYB.
- A surge in early filings before the rule change highlights attempts to avoid scrutiny, while countries like Estonia and the Nordics already demonstrate the benefits of transparent, digital-first registries.

Global Harmonization and Emerging Markets

- The new EU AML Authority (AMLA) aims to unify expectations across member states, reducing friction for cross-border compliance.
- Emerging markets, especially in Africa and Southeast Asia, have an opportunity to leapfrog by adopting modern digital ID and registry frameworks—unlocking trust, investment, and scalable growth.



KEY TAKEAWAYS

- **Technology is necessary but not sufficient**
  - IDV tools are powerful, but they sit inside governance, people, and culture.
  - You cannot buy a system, switch it on, and walk away. Systems are more like houseplants; they need constant care, calibration, and the right environment to work.
  - Scenario-based, typology-driven training builds the instinct analysts need to spot anomalies before systems label them as such.
- **Conversion vs risk is a risk-based debate, not a binary choice**
  - Conversion is a business metric, but risk-weighted conversion is a safety metric.
  - Fraudsters will look for unverified registries, weak jurisdictions, outdated policy sets, and speed gaps in internal processes.
- **Digital identity and registries will close some windows, not every door**
  - Digital ID verification, stronger registries, and corporate transparency will not eliminate fraud. They will remove some of the most obvious loopholes.
  - Once those "open windows" are shut, firms and regulators can more clearly see where remaining vulnerabilities lie and focus on remediation.

ABOUT US

At Shufti, our mission is to help organizations eliminate the final 1% gap, the space where governance weaknesses, human oversight lapses, and jurisdiction-specific inconsistencies allow fraud to slip through.

We combine intelligent verification technology with the human, procedural, and regulatory layers that modern compliance teams rely on to operate safely and confidently.

Our network-layered verification approach goes beyond accuracy metrics. We focus on the realities highlighted in this webinar: evolving criminal methods, fragmented controls, and regulatory expectations that increasingly demand speed, consistency, and accountability.

What We Deliver

Human-Aligned Technology:

- Explainable, risk-aware verification that strengthens human judgment rather than replacing it.

Integrated Risk Visibility:

- One platform connecting onboarding, KYB, AML, and behavior insights to close internal blind spots.

Global Assurance:

- Verification built to handle cross-jurisdiction inconsistencies, emerging fraud typologies, and evolving regulatory pressures.

In a world where 99% falls short, our aim is to help you shrink that last 1% from a blind spot into a managed, measurable risk.

JOIN THE SHUFTI COMMUNITY

Stay connected for expert insights, updates, and resources that help you stay ahead in compliance and digital identity verification.

Follow us. Learn with us. Grow with us.

Shufti on Website

Shufti on LinkedIn

Shufti on Twitter/X

Shufti on Facebook

Shufti on YouTube