Shufti | BIOMETRIC UPDATE.COM

You Think You Know Your Customers Till You Don't

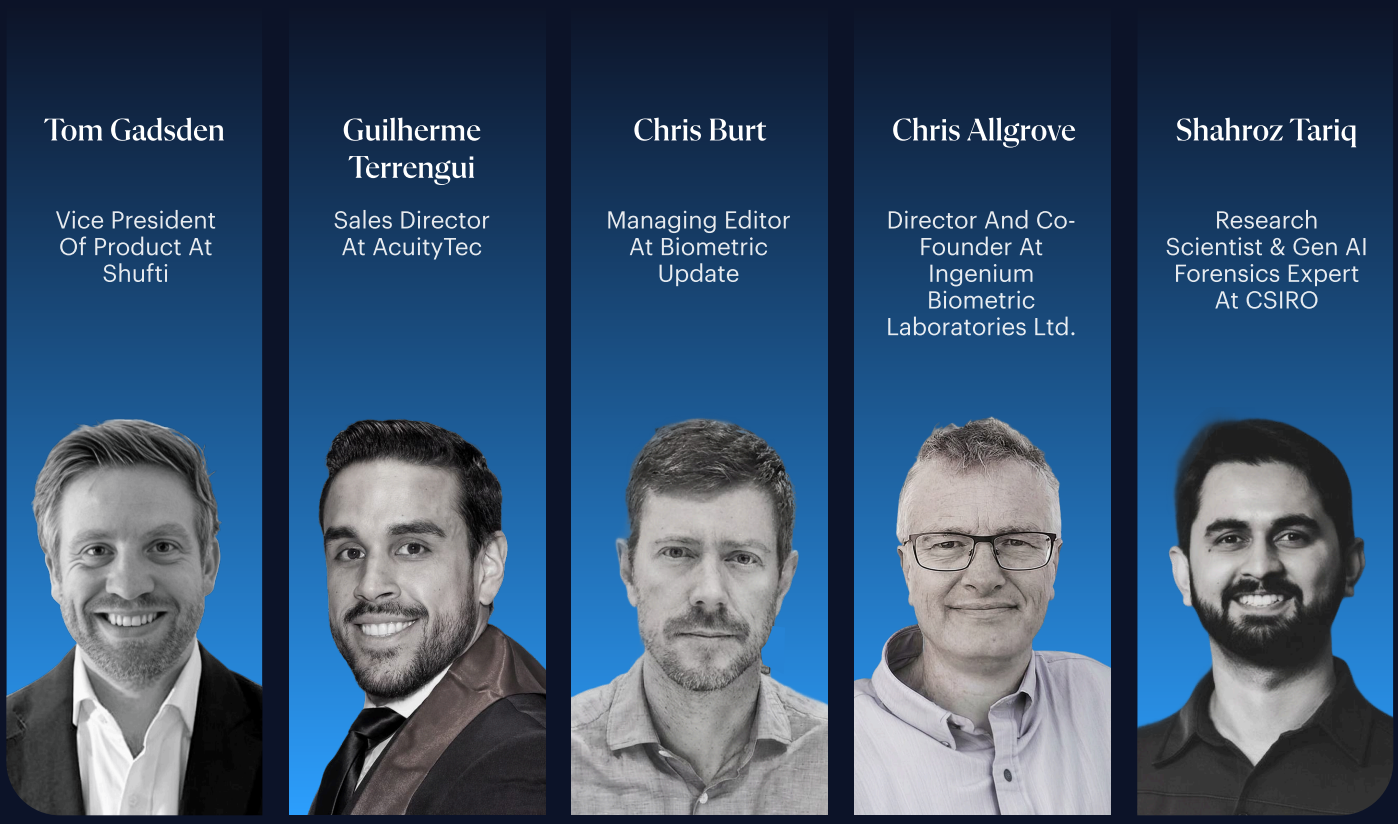
- Deepfakes Edition

Watch Webinar Here

Chris Burt
Managing Editor At Biometric Update

Moderator

www.shuftipro.com



Overview

The deepfake threat landscape has undergone three generational leaps in under a decade. For regulated firms, the challenge is whether those controls are still defensible against a threat that has evolved faster than most organizations have responded.

The discussion, hosted by Biometric Update in partnership with Shufti, focused on an uncomfortable reality: synthetic identities and injection attacks that were approved before today's detection capabilities existed, and what organizations must do now to understand and manage that legacy exposure.

The panel examined the shift from presentation attacks to injection attacks, the scalability of modern fraud, the role of behavioral intelligence in post-onboarding risk management, and Shufti's Blind Spot Audit, which is a capability built specifically to surface historical deepfake exposure within an organization's own infrastructure.

Discussion Points

The KYC you did yesterday may be the fraud risk of today.

Tom Gadsden set the context for the entire discussion:

> *"We've moved from a world where a great happy-path onboarding journey was enough, to a much more complex world with deepfakes, sophisticated fraud, and sophisticated fraud tools now in the hands of amateurs."*

Deepfakes have evolved past most defenses.

Shahroz Tariq mapped three generational leaps, from basic image manipulation, to real-time face reenactment, to today's diffusion model era, where synthetic identities arrive with fabricated documents, backdated photos, and fully constructed digital footprints.

> *"It's not just face and audio anymore. Completely fake documents, totally fabricated identities — everything needed to make a synthetic person look plausible and real."*

Injection attacks have replaced presentation attacks as the primary threat.

Deepfakes are no longer shown to a camera. They are injected as the camera, bypassing liveness detection entirely. Chris Allgrove explained the scale consequence:

> *"I make one deepfake. I send a million emails. A hundred people click. I've just executed a hundred attacks for relatively little time, effort, or expense."*

Onboarding is the starting line, not the finish line.

Guillherme Terrengui made the case for behavioral intelligence post-onboarding — combining transaction monitoring, device fingerprinting, and geolocation consistency into a dynamic risk score that makes the customer relationship an ongoing conversation, not a closed file.

> *"Once someone has technological access to a stolen phone, the question becomes: what other parameters are you combining with that initial verification?"*

The Blind Spot Audit: replacing assumption with evidence.

Regulated institutions already retain biometric and customer data for AML purposes. The question is whether that data has ever been evaluated against today's detection standards — not the standards in place when those customers were originally onboarded.

Shufti's Blind Spot Audit enables robust batch auditing of historical records, deployable within an organization's own AWS infrastructure, ensuring data never leaves their control.

Challenges Discussed

- **Injection Attack Scalability:**
  Unlike presentation attacks, injection attacks require no bespoke effort per target. One deepfake payload delivered at scale can produce hundreds of fraudulent approvals at minimal cost, fundamentally changing the risk calculation.
- **The Legacy Record Problem:**
  Controls built for earlier deepfake generations may have approved synthetic identities still active in databases today. The window between system deployment and remediation is where historical exposure lives.
- **Generalization Gaps in Detection Tools:**
  Detection systems do not automatically generalize across deepfake generations. Even frontier vision-language models can be bypassed with trivial triggers — timestamps, vintage filters, VHS aesthetics, causing synthetic images to be classified as authentic.
- **Siloed Post-Onboarding Controls:**
  The gap between what a customer declares at onboarding and how their account behaves afterward remains one of the most underutilized risk signals in the industry.

Key Takeaways

- **Audit Your Historical Records:**
  Legacy KYC data carries exposure from weaker, outdated controls. Retrospective auditing against modern detection capability is a risk management imperative, not an option.
- **Move Beyond the Onboarding Gate:**
  Behavioral intelligence, transaction monitoring, and device consistency checks throughout the customer lifecycle transform a point-in-time check into a defensible, ongoing control.
- **Multi-Stage Defense Is Non-Negotiable:**
  No single detection layer is sufficient. Multiple detectors at each stage, combined with regular updates and retrospective scanning, are the only architecture that keeps pace with an evolving threat.
- **Test Your Systems Proactively:**
  Conformance certificates from 2020 or 2021 are timestamps, not assurances. Ongoing adversarial testing is the only way to close the gap between your risk model and real-world vulnerabilities.

About US

At Shufti, we empower regulated firms to move beyond legacy KYC toward high-assurance, risk-orchestrated identity verification. Our approach directly addresses the friction points surfaced in this webinar:

- **Industrialized Deepfake Threats** require injection attack defense, not controls designed for a previous generation of fraud.
- **The Legacy Exposure Gap,** where historical records approved under weaker controls represent an unquantified and unaudited risk sitting inside live databases.

What We Deliver

- **Blind Spot Audit:**

  Enhanced batch auditing of historical biometric and identity records, deployable within your own AWS infrastructure. Understand your legacy deepfake exposure before regulators or fraud events force the issue.

- **Risk-Orchestrated Identity Verification:**

  Intelligently combine device intelligence, automated biometrics, and behavioral signals to pass legitimate customers confidently while tightening controls where risk is genuinely elevated.

- **Injection Attack Defense:**

  Advanced multi-layer detection architecture built to defend against the full spectrum of modern deepfake attack vectors — not just the ones from three years ago.

Join the Shufti Community

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

SHUFTI ON WEBSITE | SHUFTI ON LINKEDIN | SHUFTI ON TWITTER/X | SHUFTI ON FACEBOOK | SHUFTI ON YOUTUBE