Welcome!

The webinar will begin shortly

Regula

Webinar

Biometrics Under Attack:

Lessons from Building Stable Identity Verification

Name/Surname

Henry Patishman

Business role

Executive VP, Identity Verification Solutions at Regula

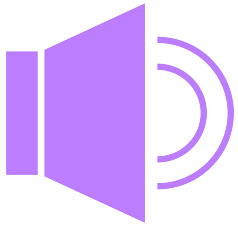
Name/Surname

Andrey Terekhin

Business role

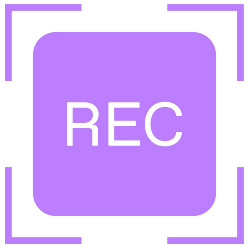
Head of Product at Regula

Housekeeping



Trouble with audio?
Try dialing in!

Submit your questions
in the Q&A section



We’re recording!
We’ll email you the link

Why Is This Topic So Urgent?

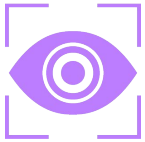
244% rise in amateur fraudsters in 2024
Digital identity fraud is shifting from pros to amateurs

21% adoption growth YoY.
Biometrics moved from ‘nice-to-have’ to critical infrastructure

40.8% of all attacks globally are now **AI-assisted**

Fines of up to millions for inadequate age verification—e.g., Ofcom’s **£1.05M fine** against OnlyFans

Types of Biometrics: Not All Are Equal



Eye/Retina

Voice

Fingerprint

Palm

Behavioral

Face

Face Biometrics Take the Front Seat

- **#1 tool used to counter fraud across sectors**
- Quickly growing in banking, fintech, telecom, travel, healthcare, and more
- Critical for remote onboarding, transaction confirmation, and access control
- Passive liveness and face matching now default in top-tier verification flows

Core Questions of the Webinar

1

Who is attacking and how?

2

Which technologies actually help?

3

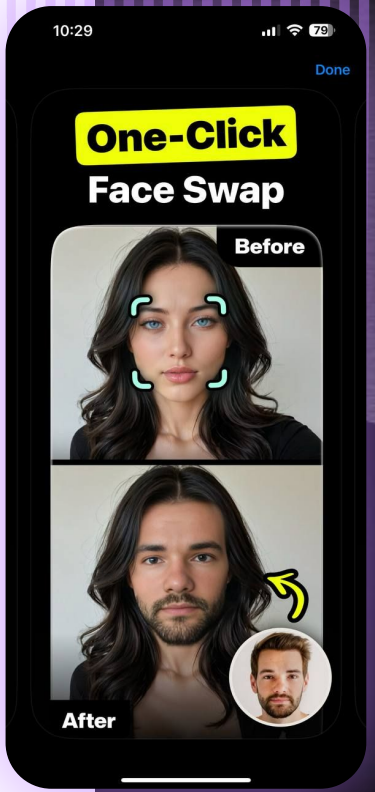
How do we verify real robustness?

Fraud Today:
Easy to Make, Hard to Catch

Why breaking biometrics has become easier than ever

- AI tools now generate spoof videos in seconds
- $2 stocking mask outperforms $200 silicone mask
- Attacks don’t need hackers—just Tik Tok tips

Simple presentation attacks like photos, tablets, and basic masks can bypass less secure systems



Spoofs So Simple — Yet They Still Work

Basic printed photo

Cut-out photo mask

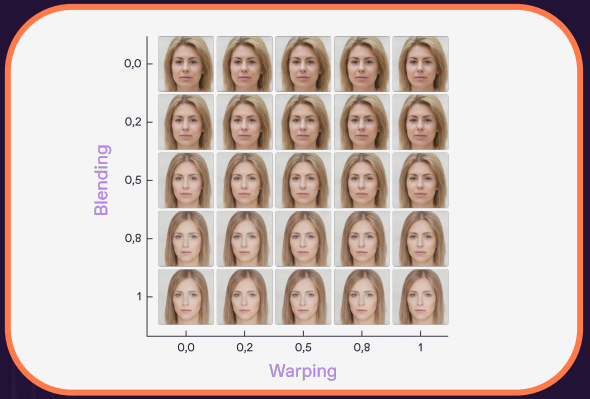
Layered print

**Examples of presentation attacks tested in Regula lab*

Advanced Attacks: AI in Action

Deepfake

Morphing



Animated face avatars

AI — Confidence Boost or Illusion?

AI in Biometric Systems

Key areas of value:

- ➔ Feature extraction (embeddings)
- ➔ Presentation attack detection (anti-spoofing)
- ➔ Multimodal analysis (face + doc + context)

Strengths of AI:

- ➔ Scalable across millions of sessions
- ➔ Fast real-time processing
- ➔ Handles massive volumes of user data

Where AI Can Fail

Overfitting
Trained too tightly on limited datasets—fails in the wild.

Wrong signals
Models latch onto irrelevant patterns (e.g., background noise, lighting artifacts).

Blind spots
Misses real attacks due to lack of data (e.g., rare spoof types, skin tones, lighting setups).

Overconfidence
High confidence scores even on spoofed or borderline samples.

The Problem Is the Illusion of Certainty

98.5% match

System Output

Reality

Different person

When the System Is Wrong — But Looks Right

South Wales Police (UK), 2017

A facial recognition system used during a major public event misidentified 2,297 out of 2,470 people. That's a 92% false positive rate—yet the system continued to be used for months.

Maryland (USA), 2022

A man was arrested and jailed for 10 days due to a false facial recognition match. Despite physical differences and an alibi, the system's result was trusted more than the evidence.

Detroit (USA), 2020

A facial recognition system misidentified Robert Williams, a Black man, as a robbery suspect. He was wrongfully arrested and held in jail, based solely on the AI match—despite no physical resemblance in surveillance footage.

Online Safety Act (UK), 2025

Failure to meet age gate obligation can lead to severe penalties, including fines of up to 10% of global revenue or £18 million, whichever is greater.

Why Mistakes in ID Verification Cost More

AI decision:
match / no match

Identity check

Access **granted**

Services, rights

Access **denied**

Delay, exclusion, error

Real Consequences

For individuals

- ➔ Denied access to services
- ➔ Wrongful arrest or exclusion

“Detroit police wrongfully arrested a pregnant woman because of facial recognition technology”

For the system overall

- ➔ No clear appeal path
- ➔ Error becomes “truth” in the record

“BBC reporter and his twin bypassed HSBC’s voice ID system”

For institutions

- ➔ Onboarding fraud
- ➔ Regulatory and legal risk

“Australia’s Social Media Minimum Age Act requires to implement age assurance, with fines of up to A$49.5M”

Time for a Poll

Why We Built a Lab

1

Testing as the foundation of real trust

2

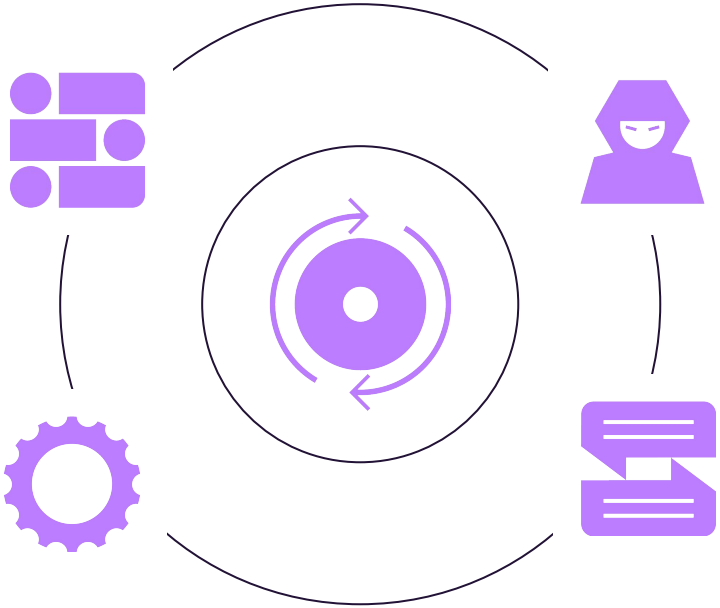
It’s not a final step— it’s a continuous process

Deep Dive #1

The Loop We Rely On

White-Box Testing

Real-World Attacks



External Validation

Customer Feedback Loop

Deep Dive #2

Why Liveness Is Hard to Get Right

Large data needs: hundreds of thousands of samples

Enough fraudulent samples to simulate real fraud

Diversity matters—ethnicity, age, gender, backgrounds

Risk of mislearning—any imbalance or bias

Human in the loop—expert oversight is key

How We Train AI to Recognize “Live” and Why It’s Not Magic

Define the goal

1

- ➔ What “liveness” really means (not just “is it moving?” but “is it real?”)
- ➔ Choose the right detection signals: texture, light, motion artifacts

How We Train AI to Recognize “Live” and Why It’s Not Magic

Build the dataset

2

- ➔ 500K+ samples: real + spoof
- ➔ Real-world variety (devices, lighting, angles)
- ➔ Skin tone & age diversity to avoid bias

How We Train AI to Recognize “Live” and Why It’s Not Magic

Annotate and validate

3

- ➔ Expert manual labeling
- ➔ White-box understanding of true/false samples
- ➔ Review cycles to catch edge cases and noise

How We Train AI to Recognize “Live” and Why It’s Not Magic

Train, test, iterate

4

- ➔ Model training on anti-spoof signals
- ➔ Validate against known attacks (e.g., deepfakes, silicone masks, screen replays)
- ➔ Use feedback loop to detect weak points

How We Train AI to Recognize “Live” and Why It’s Not Magic

Deploy and monitor

5

- ➔ Embedded into SDK
- ➔ Real-time analysis of false accepts / rejects
- ➔ Used in Regula Lab feedback loop

Deep Dive #3

Spoofing Materials We Test Against

Deep Dive #4

Benchmarked Against the Highest Industry Standards

- ISO/IEC 30107-3 compliance (anti-spoofing standard)
- iBeta PAD Level 1 & 2 certification
- Resistance to real-world attacks (prints, videos, deepfakes, masks)
- Process & resilience validation (failure handling included)
- NIST FATE participation (Face Analysis Technology Evaluation - FATE)

Takeaways for Vendors and Buyers

- ➔ Fraud got cheaper → Defenses must be faster and adaptive
- ➔ AI ≠ guarantee → Requires testing, oversight, and control
- ➔ Don’t trust feature lists → Look for resilience, response, and transparency

- ➔ Ask vendors how often they test against new spoof types
- ➔ Check whether liveness has been certified externally—not just claimed
- ➔ Look for feedback loops, not static models.

Why

Across the globe, regulators are introducing heavy fines for non-compliance in age and identity verification

Up to £18M or 10% of global turnover

Up to 6% of global turnover

Up to €20M or 10% of turnover

Up to AU$49.5 million

Regula Track Record

- **34+ years in identity verification**
  Standing at the origins of ID tech—long before AI went mainstream.
- **We build all our tech in-house**
  Full control = better quality and fair pricing.
- **5 of 9 Gartner MQ IDV vendors are our clients**
  We enable the leaders of the industry.
- **iBeta Level 1 & 2 passed**
  Independent validation of biometric resilience.
- **#1 in NIST Age Estimation benchmark**
  The only vendor recognized among top performers in all critical age estimation scenarios.
- **Used at 80+ borders worldwide and the world's major banks**
  Trusted by the most security-critical institutions.

Questions?

Thank you!

kate.johnson@regulaforensics.com

Regula

Decades of Forensics for Seamless Identity Verification.
Bringing together 33 years of experience in forensics, border control and business, to create industry standards to trust and follow.