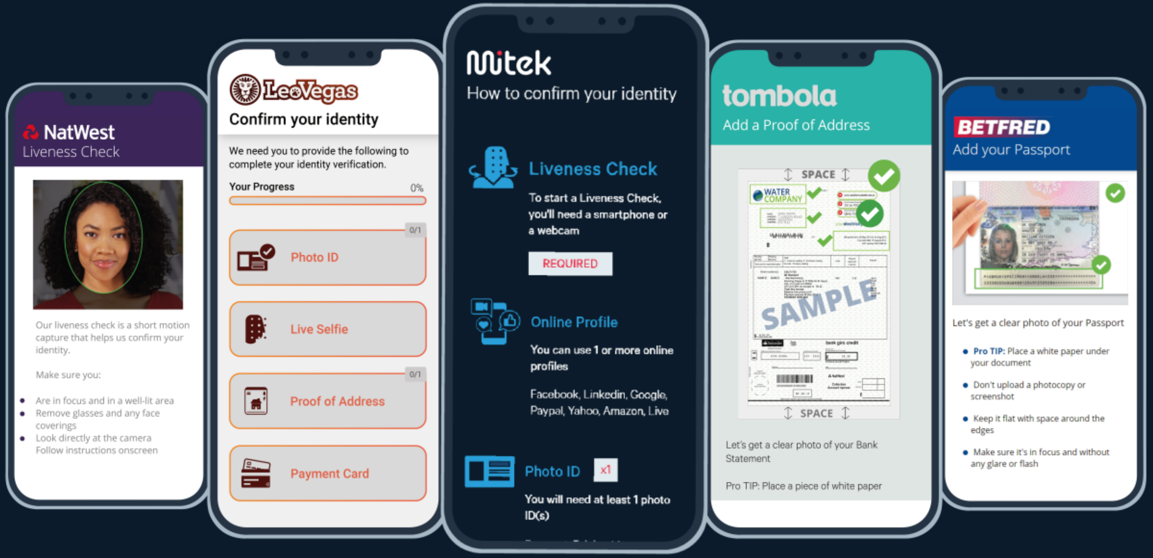
Combatting Identity fraud & crime rings ´The threat is real, helplessness is not´

PETER MURRAY: DIRECTOR OF STRATEGY BETTING AND GAMING

MITEK

Mitek

1986	Founded
2007	Mobile Check Deposit – start of Mitek's SDKs
2013	IPO
2015	ID Checker Acquisition
2017	Mobile Verify
2021	ID R&D Acquisition
2022	HooYu Acquisition



NatWest
Liveness Check

Our liveness check is a short motion capture that helps us confirm your identity.

Make sure you:

- Are in focus and in a well-lit area
- Remove glasses and any face coverings
- Look directly at the camera
Follow instructions onscreen

LeoVegas
Confirm your identity

We need you to provide the following to complete your identity verification.

Your Progress 0%

0/1 Photo ID

Live Selfie

0/1 Proof of Address

Payment Card

Mitek
How to confirm your identity

Liveness Check
To start a Liveness Check, you'll need a smartphone or a webcam
REQUIRED

Online Profile
You can use 1 or more online profiles
Facebook, Linkedin, Google, Paypal, Yahoo, Amazon, Live

Photo ID x1
You will need at least 1 photo ID(s)

tombola
Add a Proof of Address

Let's get a clear photo of your Bank Statement

Pro TIP: Place a piece of white paper

BETFRED
Add your Passport

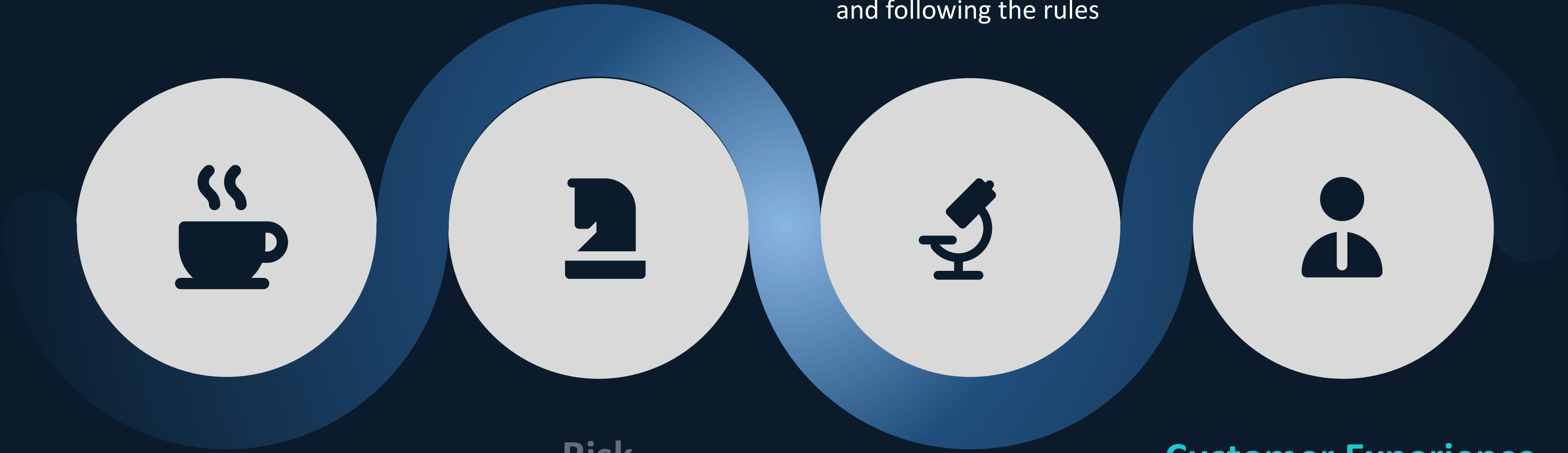
Let's get a clear photo of your Passport

- **Pro TIP:** Place a white paper under your document
- Don't upload a photocopy or screenshot
- Keep it flat with space around the edges
- Make sure it's in focus and without any glare or flash

Trusted by

BETFRED LeoVegas SUPRNATION tombola BoyleSports

What's on your mind right now?



Revenue

Customer acquisition

Risk

Letting the good people in and keeping the bad ones out

Compliance

Ensuring you're doing the right thing and following the rules

Customer Experience

Making it easy to work with you

What's on our mind right now?

Tech development for AI, Liveness and voice verification
https://www.idrnd.ai/

The changing face of fraud

Generative AI

It's easier than ever to generate deepfakes, impersonations, synthetic identities

Crime rings

Organized fraud rings use mules, template attacks, and bot-driven attacks

Injection attacks

Fraudsters are circumventing biometric and liveness checks with injection attacks

What is the threat?

- Synthetic identity created using a combination of real and fabricated PII, forgeries
- Real people are used to pass liveness checks
- Repetitive attack cycle creates an opportunity for us to identify the actions as fraudulent behavior

The

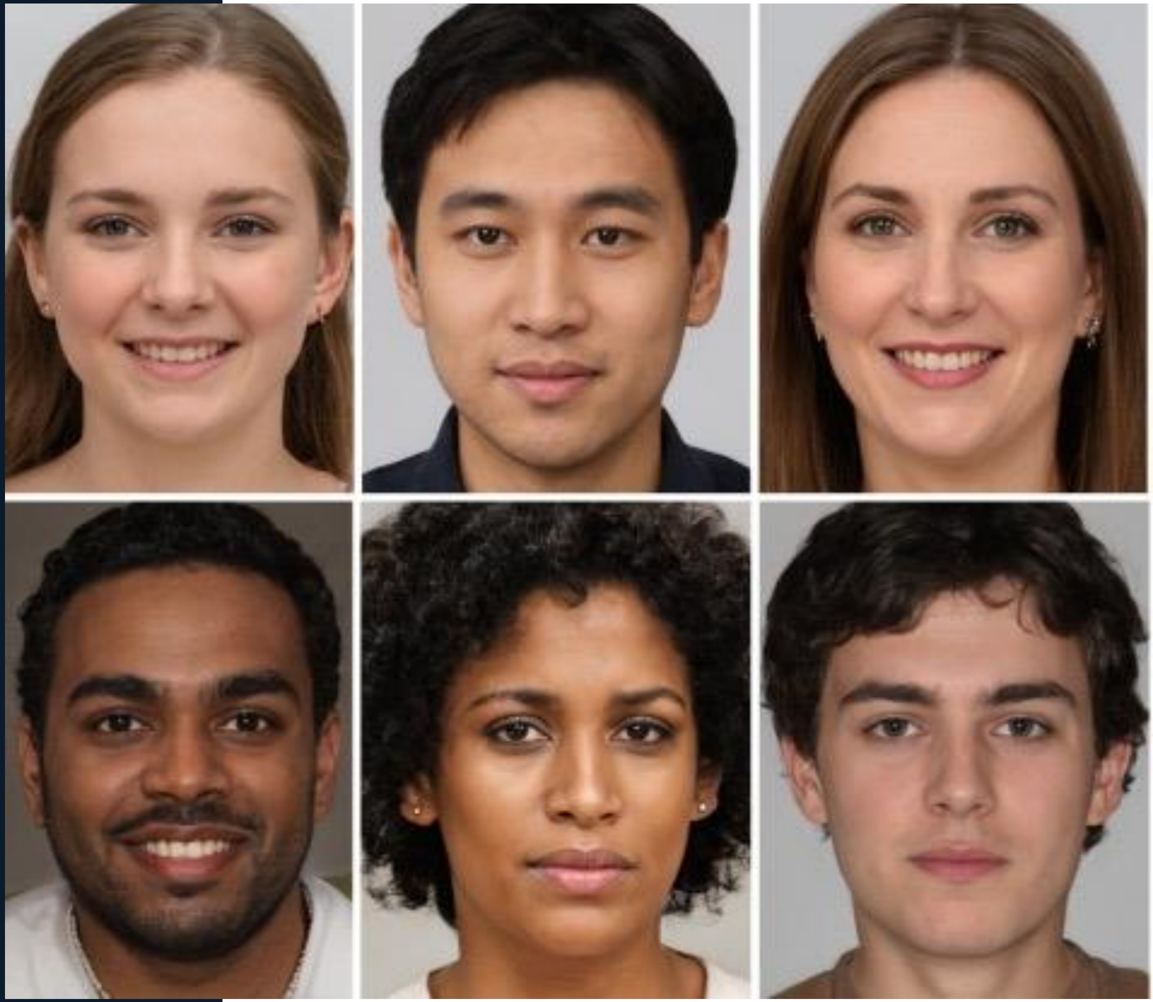
The volume of human-initiated attacks grew

88% YOY

Source: LexisNexis 2022 Global State of Fraud and Identity Report

The threat of deepfakes is substantial. In 2024, 20% of successful account takeover attacks will leverage deepfakes.

SOURCE: GARTNER



Account takeover attacks

84% of financial institutions experienced ATO fraud in 2022 - costing up to 8% of revenue.

Driven by online banking, bot-driven attacks, ease of creating "Fullz" profiles.

SOURCE: RETAILBANKER.COM

Where do we start?

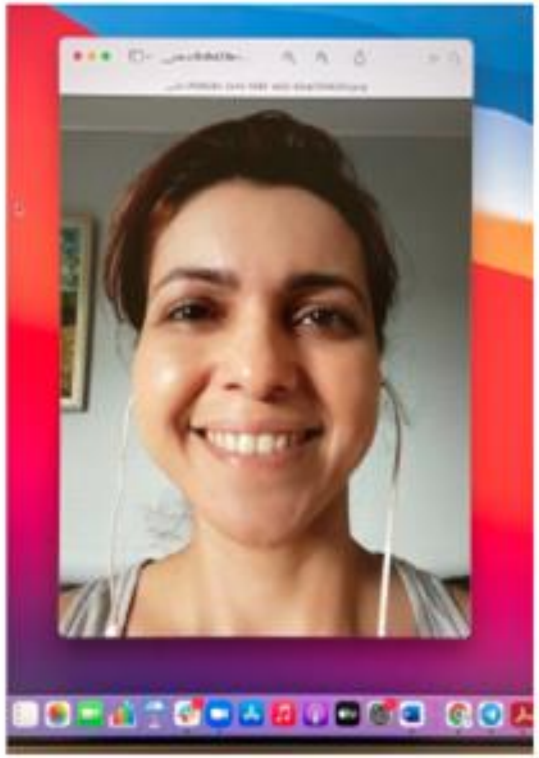
Detecting screen replays?

Detecting printed copies?

Biometric attacks – presentation and injection?

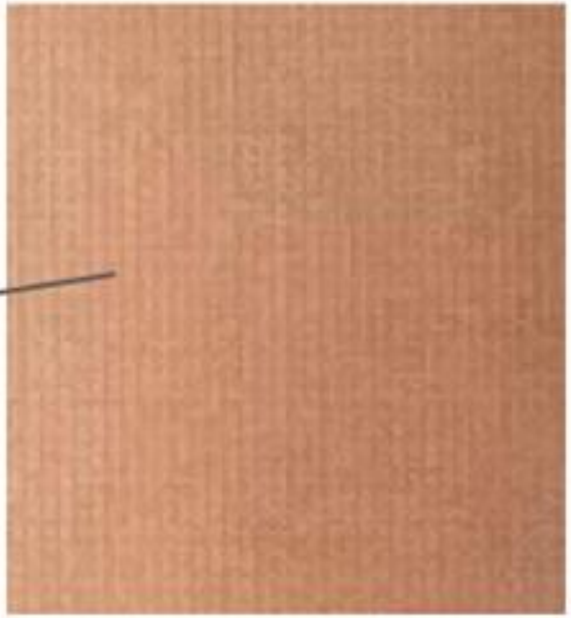
Detecting screen replays

What fraudsters do



What the camera sees

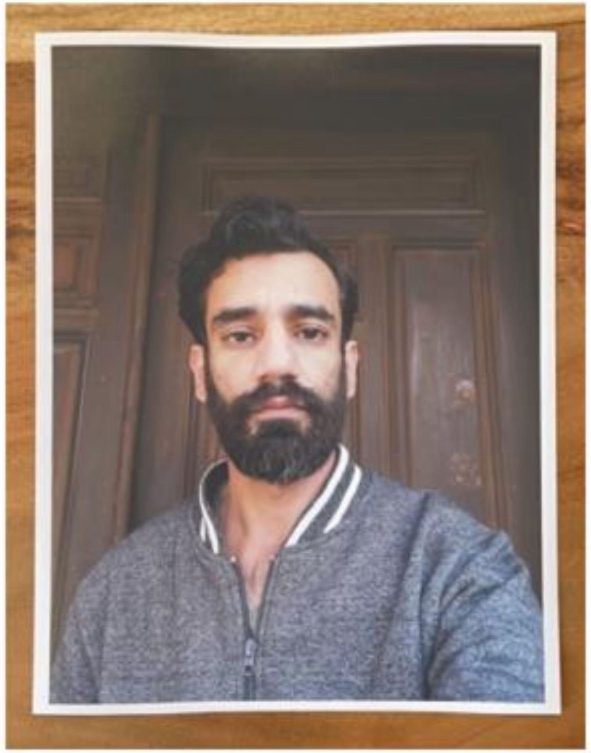
What the neural network sees



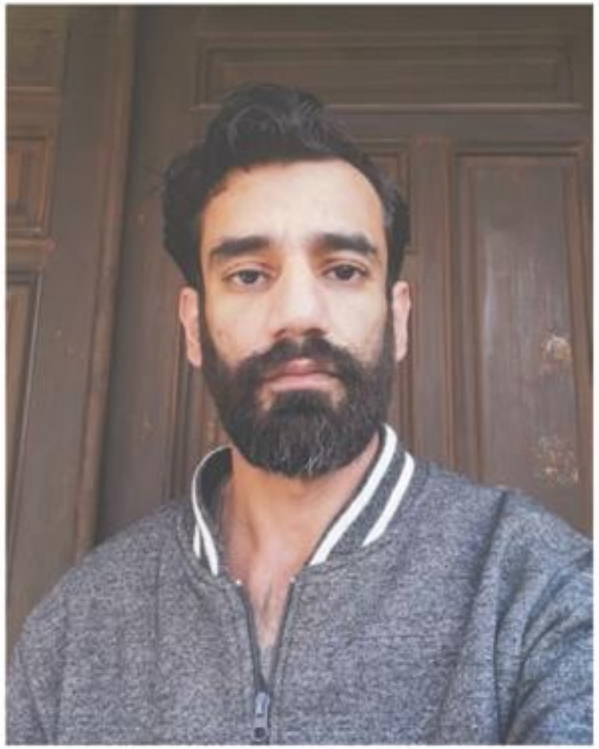
"SCREEN DOOR EFFECT"

Detecting printed copies

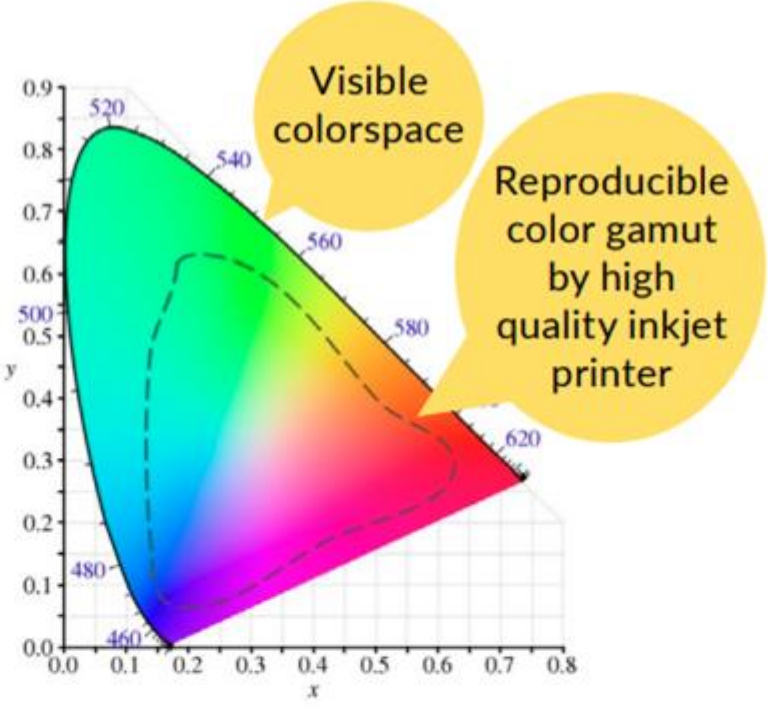
What fraudsters do



What the camera sees



What the neural network sees



CIE xy chromaticity diagram

Algorithms evolution

Wax mannequins

Virtual backgrounds

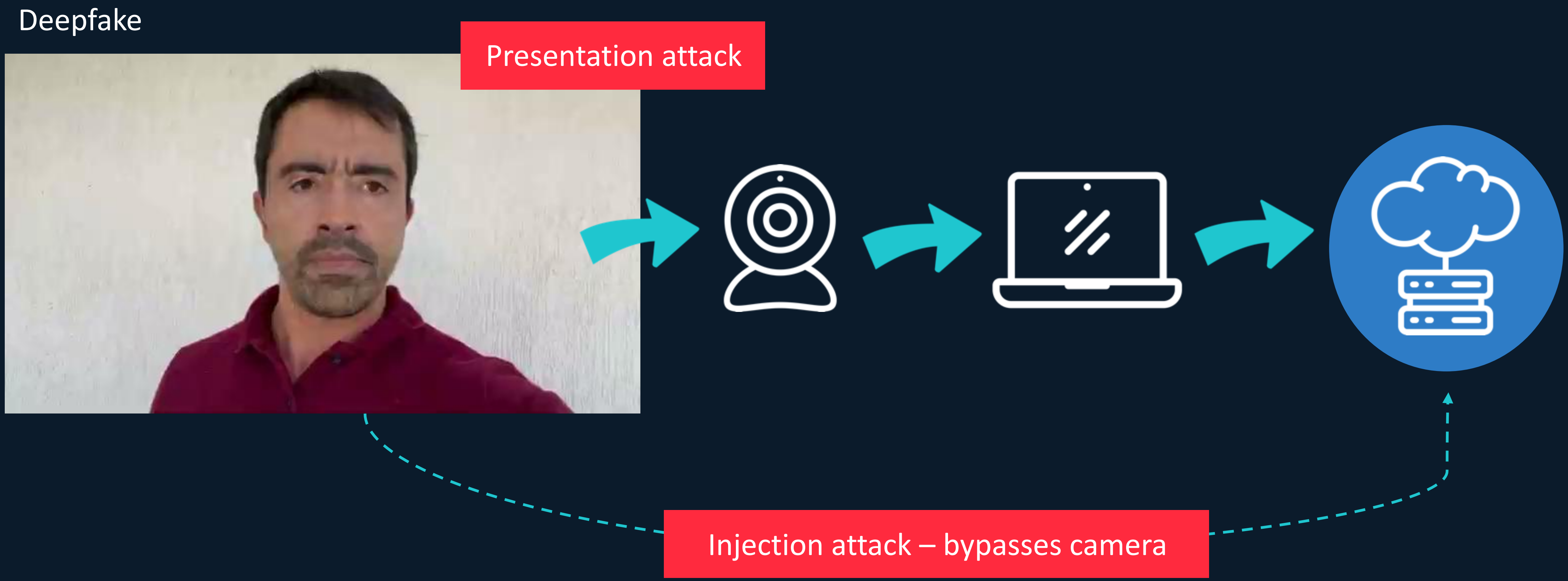
3D Faces

4k monitor replays

4k mobile replays

Deepfakes

Biometric attacks – presentation and injection



Deepfake

Presentation attack

Injection attack – bypasses camera

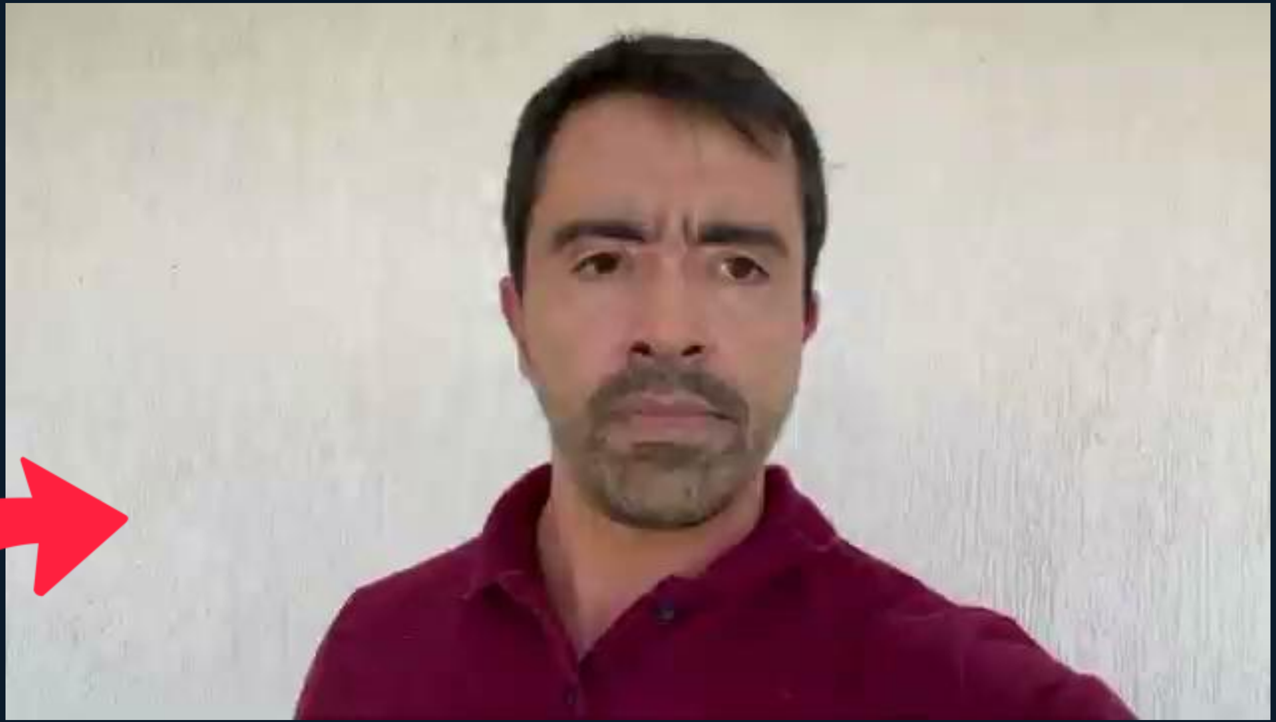
The threat of deepfakes

- Deepfake video + face morph
- Biometrically matches to victim on 96% of attempts

Selfie video of attacker

+

Photo of victim from the internet



Deepfake face morph

Fraud mitigation strategies

Adopt modern AI identity verification solutions

- Fight AI fraud with AI-fueled IDV, biometrics, liveness detection
- Implement injection attack detection
- Catch more fraud while keeping friction low

Stop fraud rings and bot attacks with velocity checks

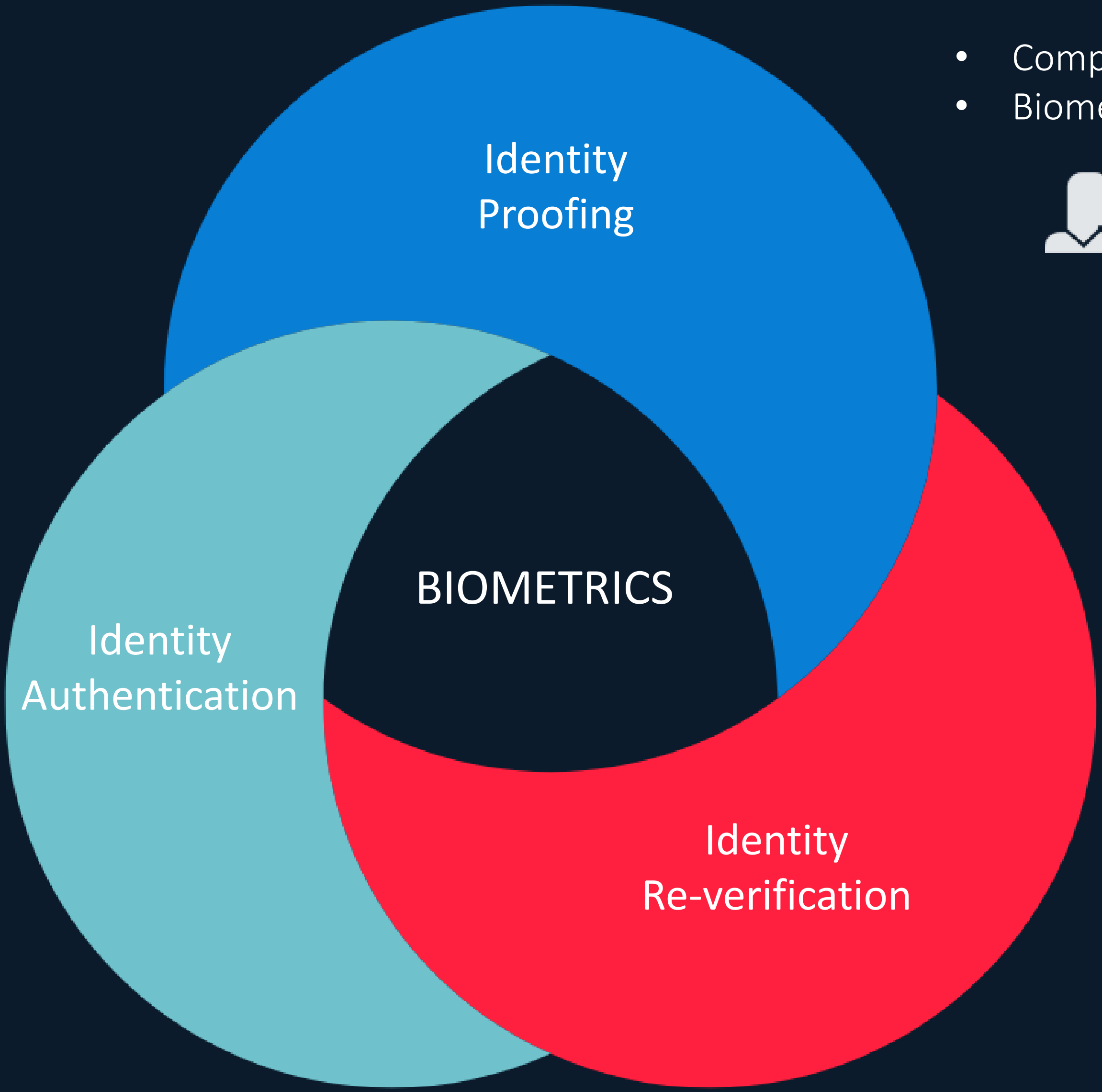
- Identify fraud patterns in real time
- In the past [X] days, we’ve seen this face [Y] times
- We’ve seen this face before, and last time the PII was different

Block bad actors when you learn of them

- Check new user faces against list of known fraudsters

THE FUTURE OF IDENTITY VERIFICATION

Application of Biometrics



- Compare new selfie against new document
- Biometric-account binding

Compare new selfie/voice against original (enrolled) selfie/ voice

Compare new selfie against original document

Biometric authentication benefits

Imagine replacing passwords

Eliminate password frustrations with a simpler and more secure way to access digital accounts.

Reduce account takeover risks

Use face/voice matching with liveness checks, to reduce fraud/abuse losses associated with bots and bad actors

Enable secure device rebinding

Leverage cloud based biometrics, that are captured at account opening for re authenticating, re issuing, etc.

Enrich KYC practices with New Digital Signals

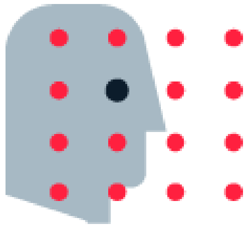
Unique new signals through our partnership with telecom industry

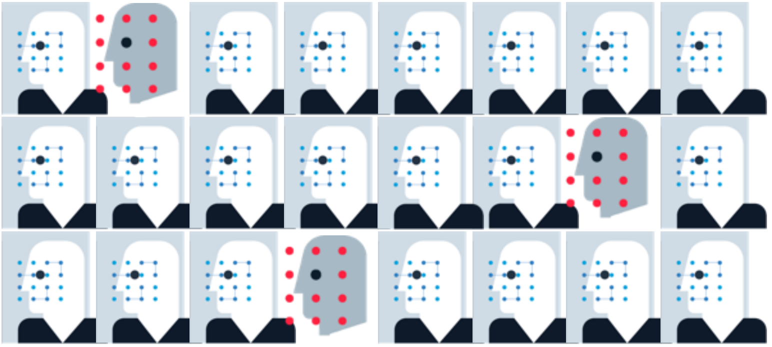
Streamline in-store/call center experience

Empower trusted customers with secure self service access
Leverage signals to defend against fraud/policy abuse

Duplicate Identity Scan

- **Customer-controlled blocklists**
  - You tell us who the bad guys are (by giving us a face or a prior transaction ID), and we'll stop them automatically.
- **Selfie velocity**
  - In the past [X] days, we've seen this face [Y] times. Here are the associated transaction IDs.
- **PII to Selfie Disconnect**
  - We've seen this face before, and last time the PII was different. Here's the previous associated transaction ID, and we've blocked the transaction.

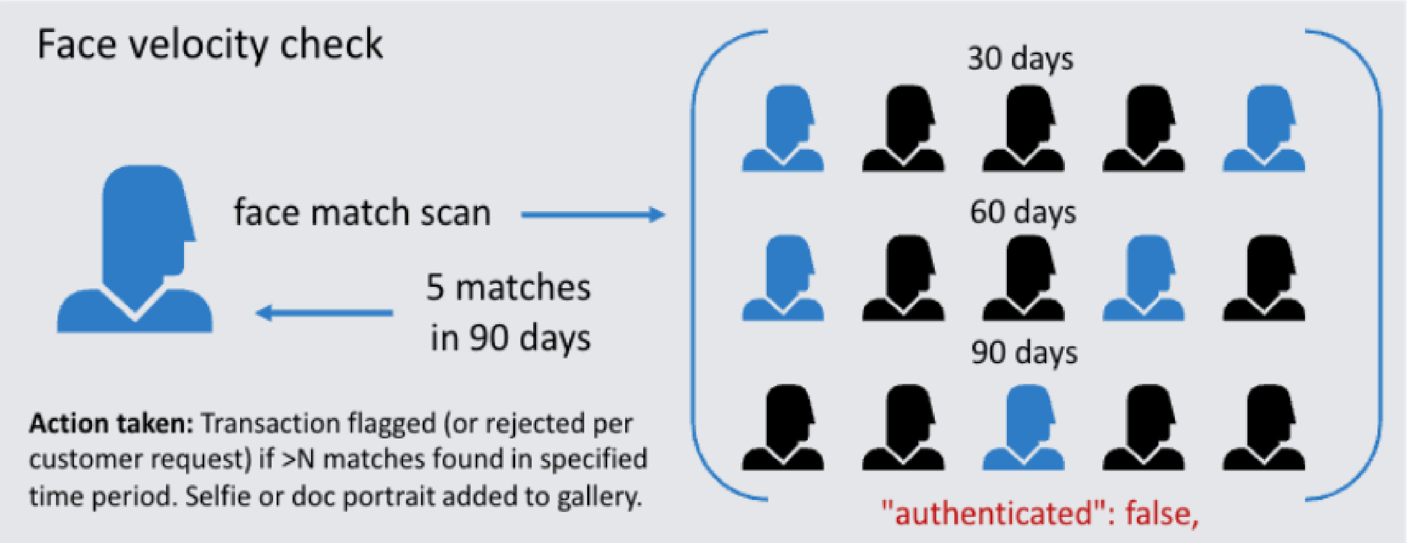




Duplicate Identity Scan – How it works

Velocity scan

- Activated as an onboarding verification signal
- Performs a 1:N face comparison check to identify duplicate selfie photos that have been submitted more than once over a specified period



Face velocity check

face match scan

5 matches in 90 days

30 days

60 days

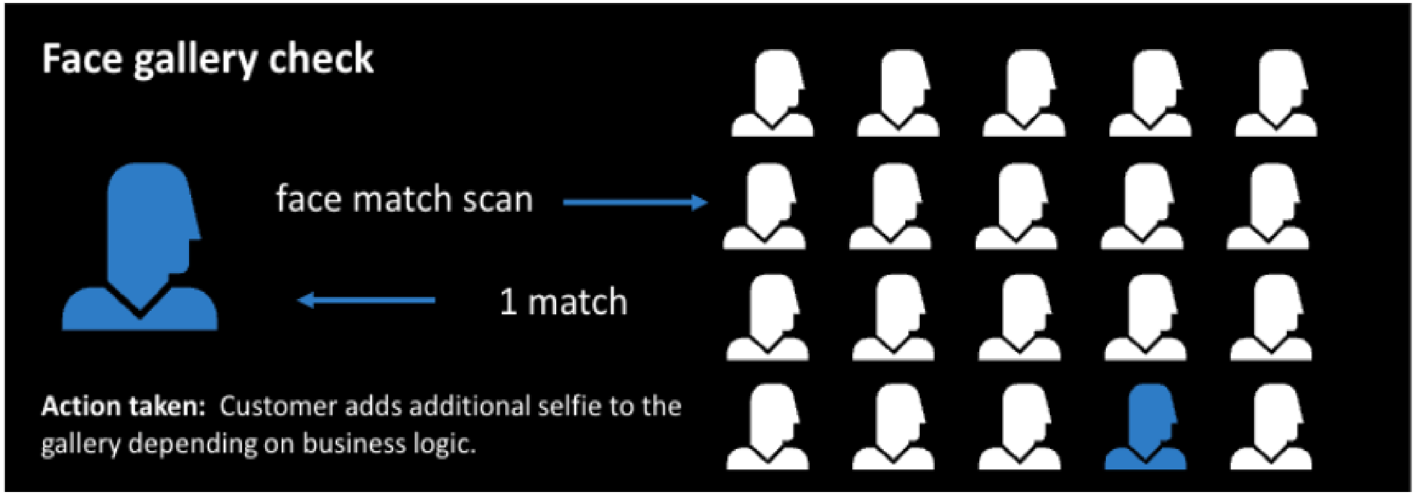
90 days

Action taken: Transaction flagged (or rejected per customer request) if >N matches found in specified time period. Selfie or doc portrait added to gallery.

"authenticated": false,

Gallery scan

- Stores selfies that have already been submitted to the gallery based on business logic
- Gallery is scanned to determine if a newly submitted selfie is in the gallery



Face gallery check

face match scan

1 match

Action taken: Customer adds additional selfie to the gallery depending on business logic.

Thank you!
pmurray@miteksystems.com

Identity is evolving. **Stay in control.**

Mitek