# Emerging Threats In The Remote ID Environment

Andrew Bud
CEO, iProov

28th October 2022

# Company Overview

## Andrew Bud CBE FREng FIET

- Founder and CEO of iProov
- Professional Engineer
- Former chair of ETSI committees
- Former head of mobile comms for Olivetti (IT)
- Serial entrepreneur

## About iProov

- Founded in 2011
- 170 staff in UK, Netherlands, US, Singapore
- eIDAS Modular Certified (by TÜV) for biometric verification and authentication services
  - Qualified Trust Services Provision
  - eID LoA High

# Our Success: Proven Market Leadership

## Government Services

Government Digital Service

ID.me

Home Office

GOVTECH SINGAPORE

## Digital Identity

itsme

SK ID SOLUTIONS

## Banks and Financial Services

knab

Rabobank

## Digital ID for citizens

NHS

## Borders & Travel

EUROSTAR

ING BANK

With approx. **20m verifications** per month

# EU Digital Wallet Must Be Built Around The User

- To enable citizens to prove their identity electronically in a **convenient and trusted way**
- Security **and** ease of enrolment & use are critical for the adoption and use of eID wallet services

## Financial Services


**Reduce onboarding costs** by up to 90%.

**Reduce payroll fraud**, saving up to $1.6 trillion globally.

**Help provide access to financial services** for 1.7 bn currently excluded.

## Economy

Potential to unlock economic **value equivalent to 3% – 13%** of GDP in 2030 with full digital ID coverage.

## Organizations

**Improve customer experience** with swifter access.

**Reduce operational costs** associated with manual identity verification.

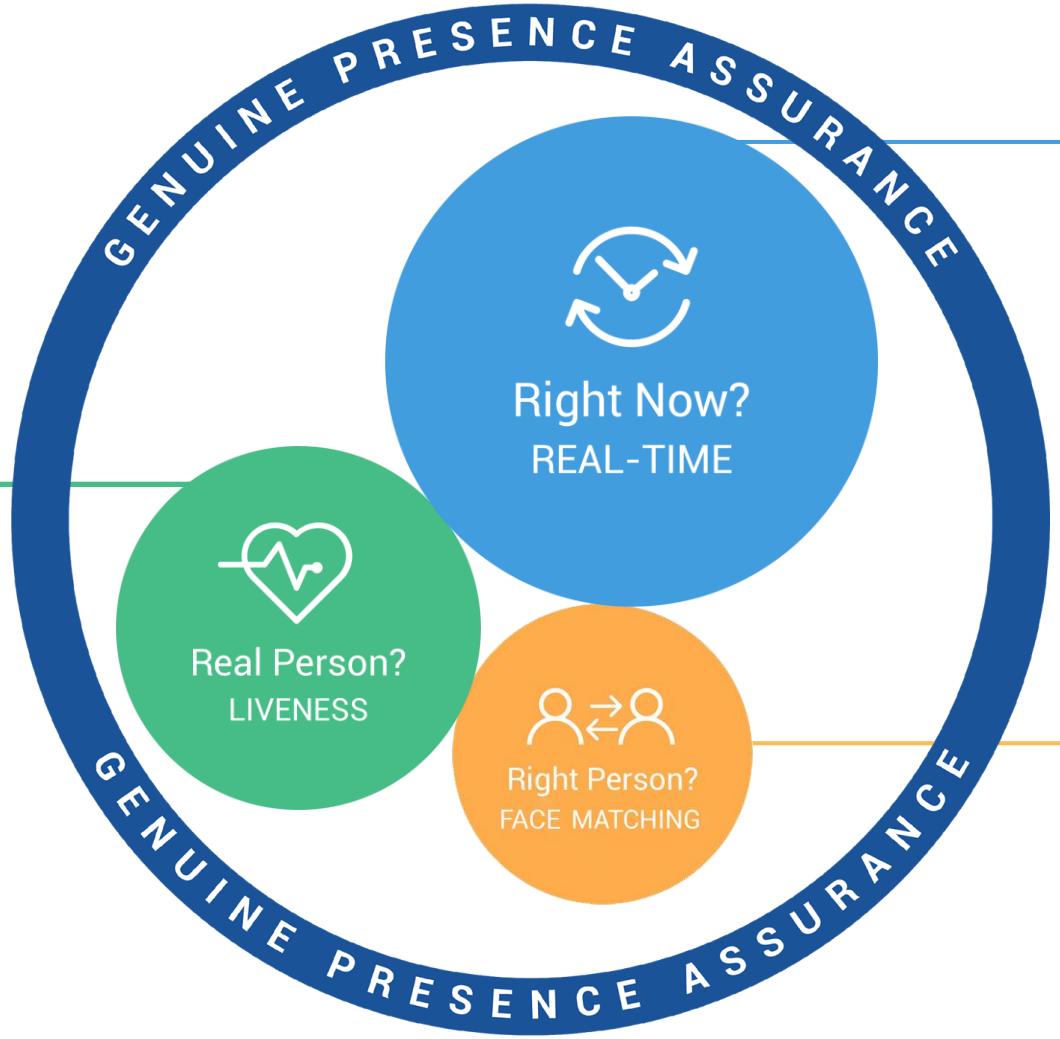
Increase security and trust.

## Governments

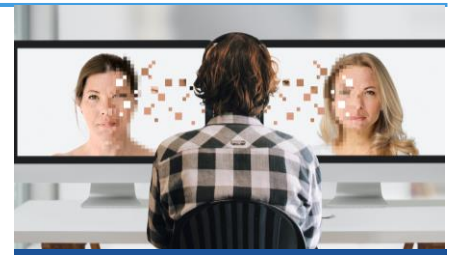
**Save 110 bn hours** through streamlined e-government services, including social protection and direct benefit transfers.

Reference: McKinsey: Digital-identification a key to inclusive growth

# Threats to Remote Biometric Verification




## Digital Injection Attacks



Datastreams containing Deepfakes and replays

## Presentation Attacks

Artefacts presented to the camera

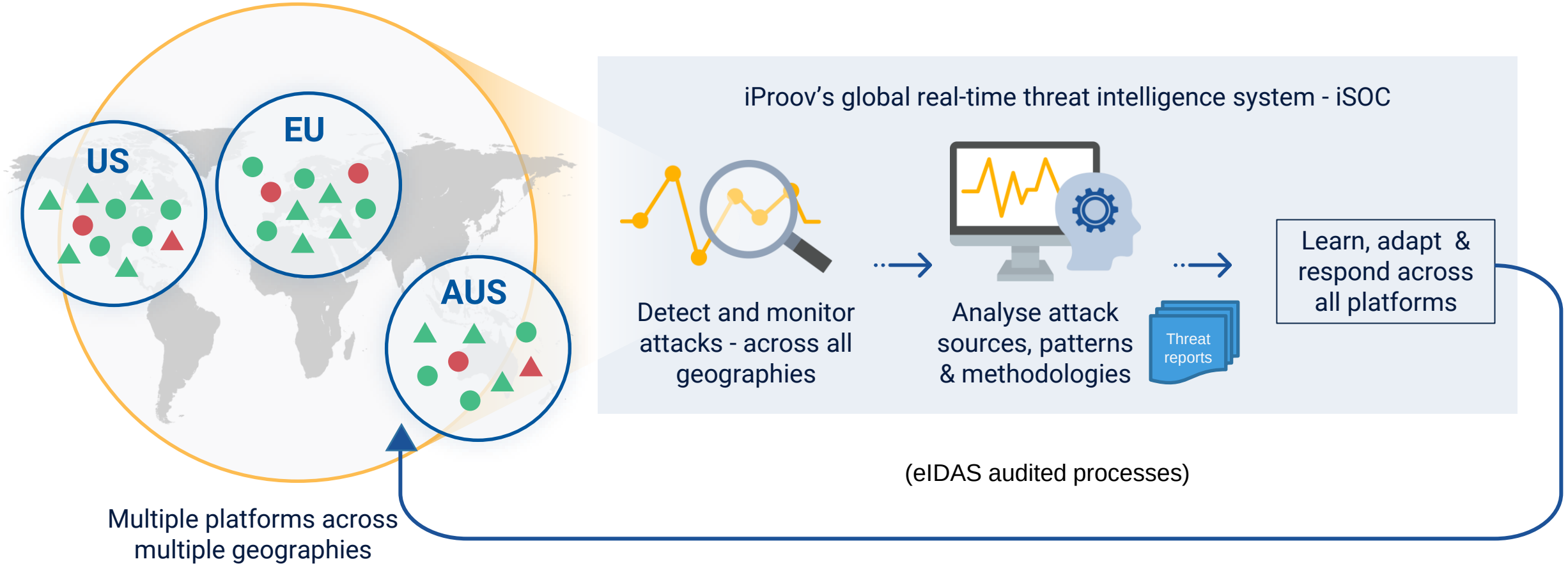
## Impersonation Attacks

Wrong person

# Evolving Threat Landscape

- Threat landscape is becoming dominated by **synthetic imagery attacks**
- **Rapid development and diffusion** of machine-learning computer imagery methods
- Processing on devices allows attackers to **conceal their identity and method of attack**
- Successful exploits can be propagated rapidly as **Crime-As-A-Service**
- **Many established online ID verification methods are now a hazard**

# Sourcing Biometric Threat Intelligence



# Observed Threat Patterns

**6X More**

**Digital Injection Attacks vs. Presented Attacks**


Presentation attacks (ex. masks)

Presented mask attacks only

Digital injection attacks

# Organised, Sophisticated and Persistent Attacks

**Phase 1**

Digital Injection Attack targeting US

**Phase 2**

Attack methodology migrated to Europe and APAC regions

**Phase 3**

Failure to succeed, attack evolved into a form of deepfake

# No Compromises In User-Centric Security Policy

### Inclusion through user choice:

- No imposition or requirement for special device hardware or sensors
- Ability to securely authenticate on any device with a user-facing camera

### Device risk mitigation:

- No reliance on users' device for security
- Mitigate risk from synthetic or compromised devices

### Verification integrity:

- Use inaccessible processing to prevent reverse engineering by attackers
- Mitigate threat of adversarial attack

### Agile response:

- Ongoing threat intelligence to evolve defences

### Inclusion through accessibility:

- Device & platform agnostic to include all users
- Robust performance and bias monitoring
- Cloud-based delivery

### Robust choice pathways:

- Non-biometric enrolment option must be equally secure…
- …even if convenience is sacrificed

### Identity recovery:

- Users should not be required to re-enrol when devices are changed or replaced

### Relieve users of burden of responsibility:

- Implementation of new detection algorithms must not rely on or compel the user to update their personal device

# Thank you

**Genuine Presence Assurance**

**Right person, Real person, Right now**

contact@iproov.com