Remote identity attacks and fraud prevention

ENISA video identity proofing workshop

May 10, 2023
Amsterdam

Sebastian Elfors, senior architect, IDnow

IDnow.

Agenda.

1 • IDnow products for remote identity proofing

2 • Remote identity attacks and fraud prevention

3 • IDnow product certifications

IDnow products for remote identity proofing.

IDnow offer identity verification products tailored to regulated use cases.

Offline
Shop, Point of Sale, Courier

VideoIdent
Video-chat-based ID verification

AutoIdent IDcheck.io
AI-powered ID verification

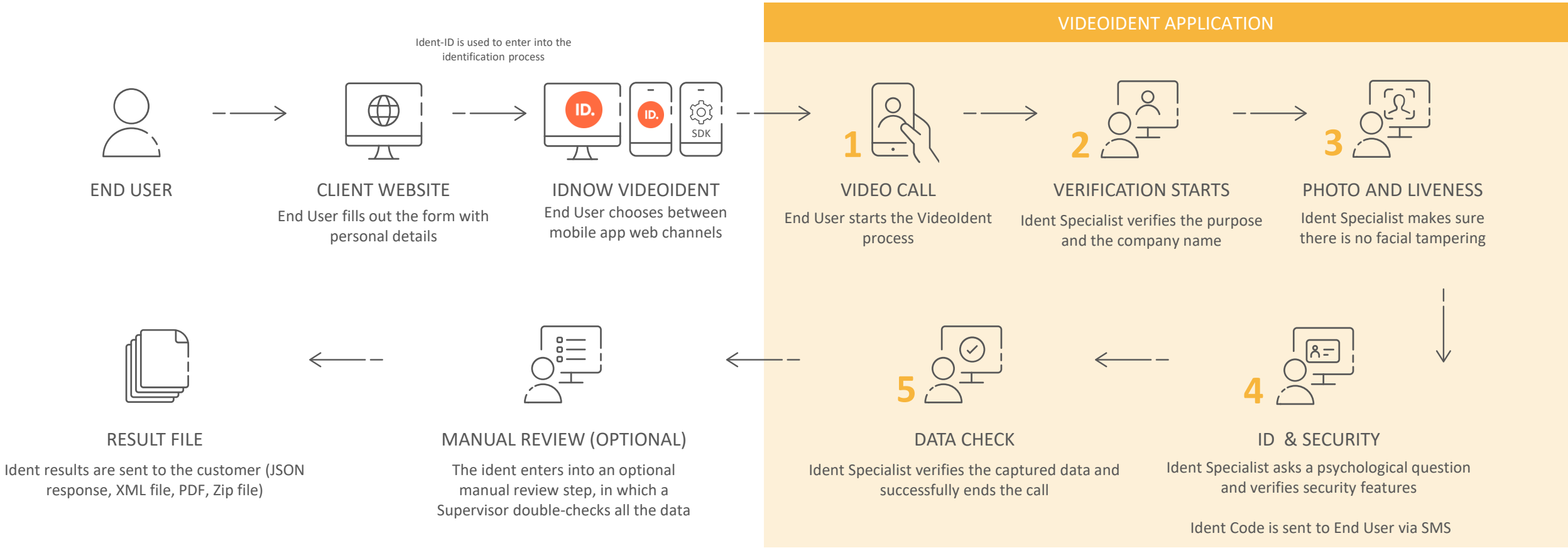
eID / NFC
NFC-based ID verification

NEW
Wallet
Identities stored on the smartphone

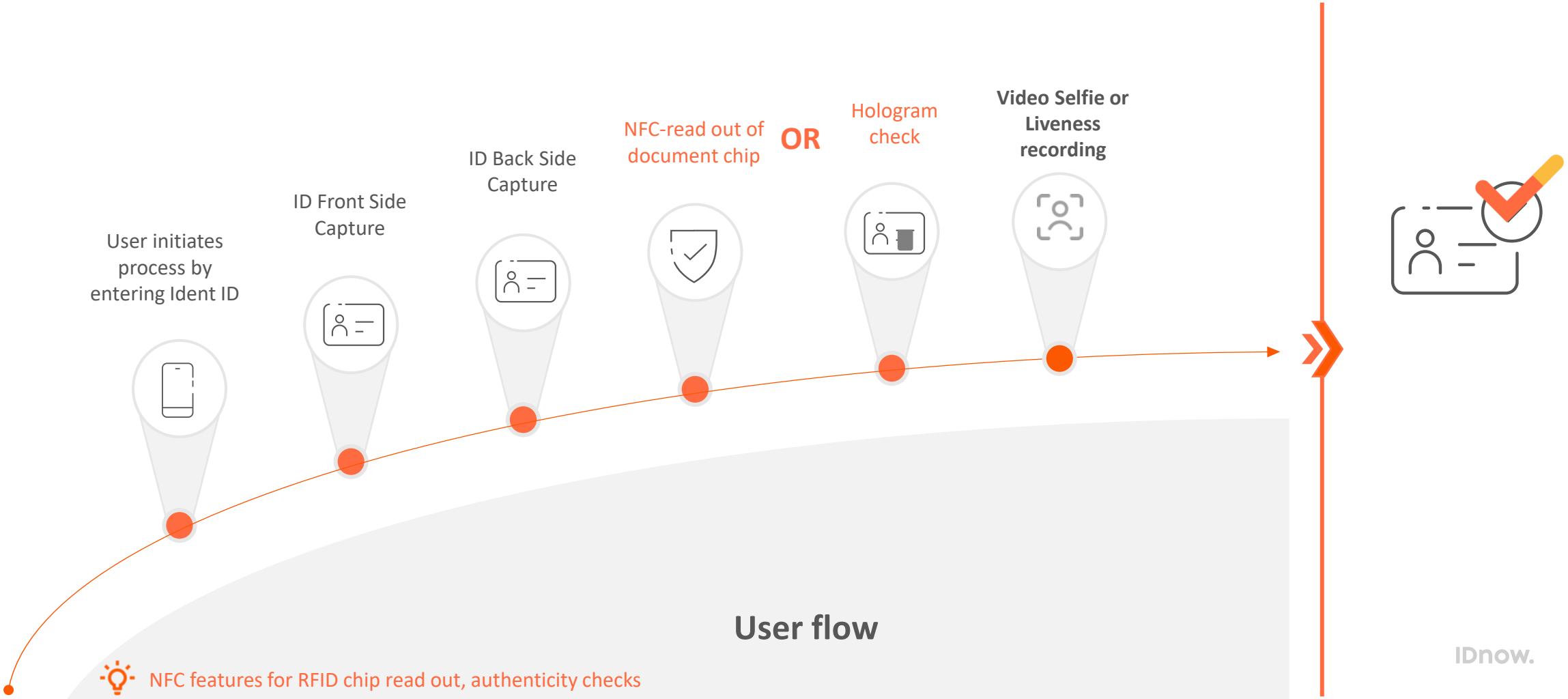
- Single API Platform – multi-client configurations
- Full Service or Self Service delivery model
- AI-algorithms trained on millions of datasets

Automation

IDnow video identification process.



IDnow automated identification process.



Remote identity attacks and fraud detection.

Types of remote identity proofing attacks.

- **Fake ID-cards**
- **Identity fraud (similarity)**
- **Presentation attacks**
  - Photo of user attack (paper, monitor or other phone)
  - Video of user attack (monitor or other phone)
  - Mask attacks (3D mask or paper mask)
- **Video injection attacks**
  - Deep fake attacks
  - Morphable avatars (advanced variant of deep fakes)
- **Social engineering**

How IDnow detects fraud.

AI-powered automatic fraud engine collects risk signals from documents, biometrics and other data sources, our own fraud detection technology.

Manual video identification in combination with AI; our solutions are also supported by highly trained agents.

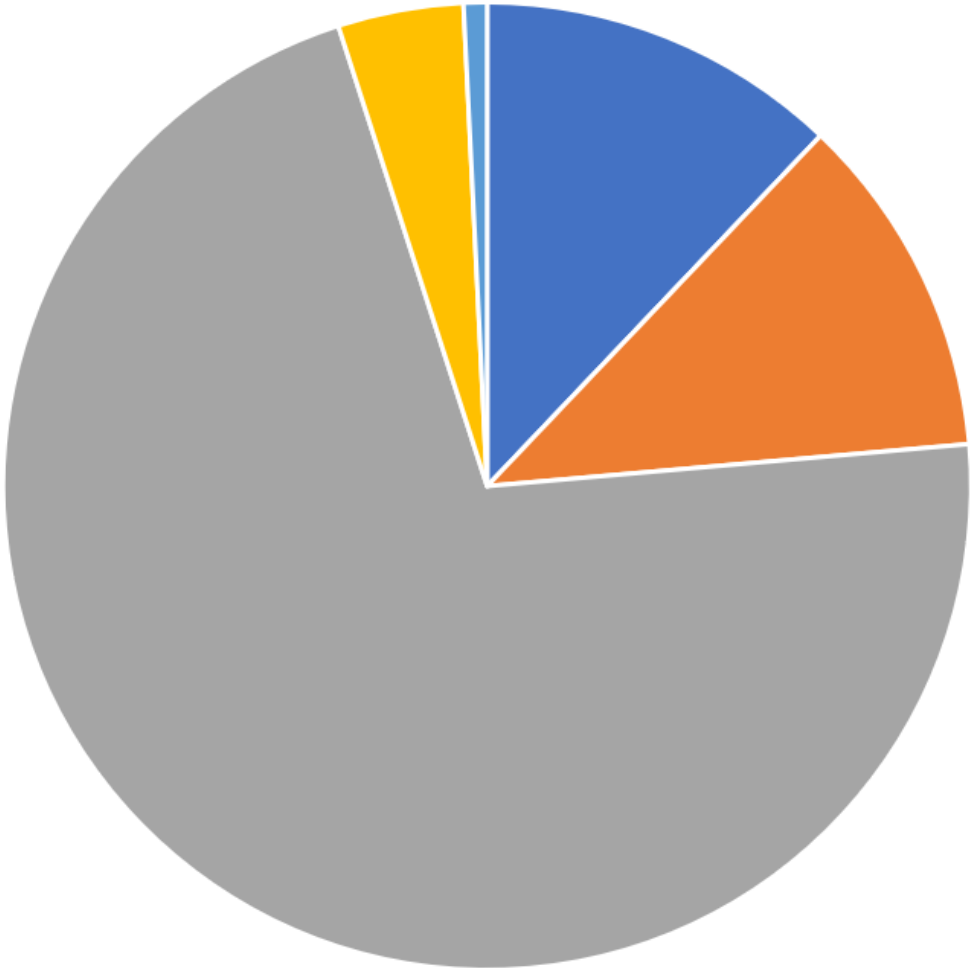
Cooperation with INTERPOL and other law enforcement agencies equips us with the expertize to keep up to date with the latest counterfeit document intelligence.

COUNTERFEIT DETECTION

- State of document
- MRZ
- Layout
- Printing technique
- Security thread
- Color
- Optical variable ink
- Optical variable device

IDnow.

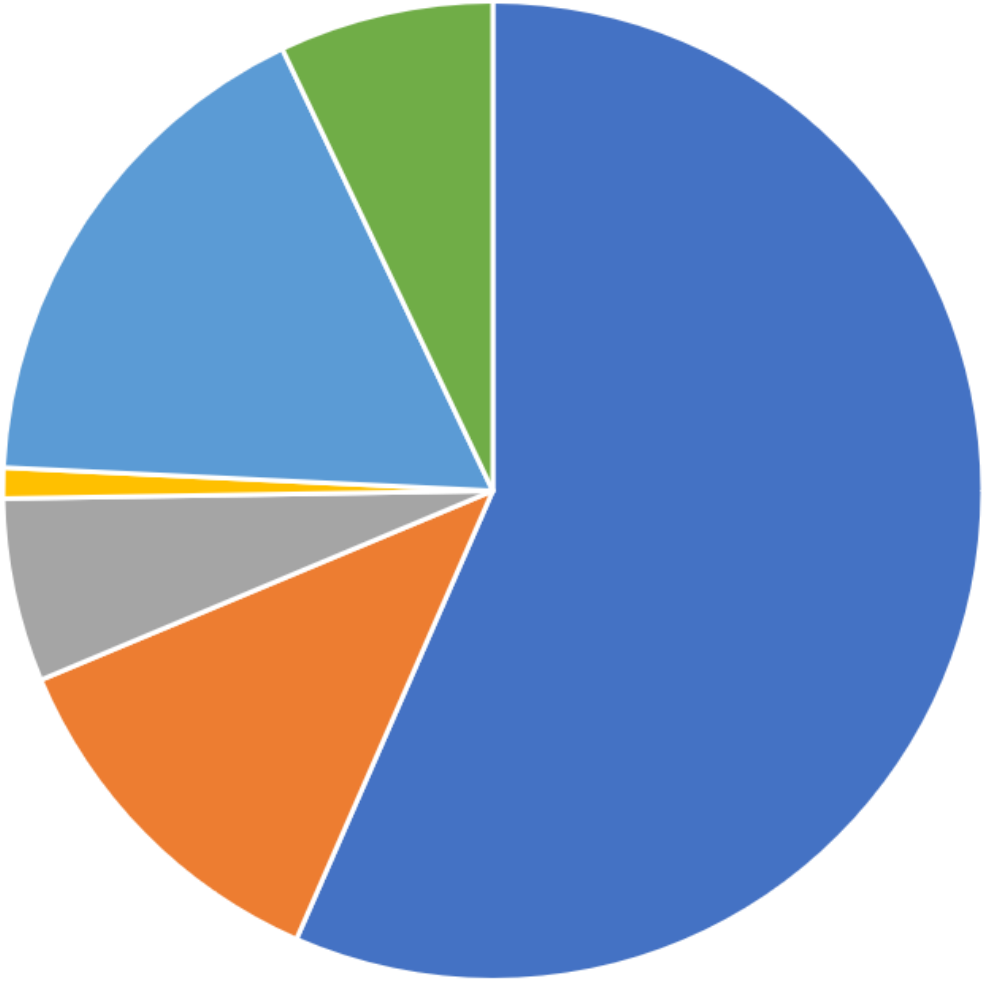
Detected frauds per attack type.



- Fake ID-document
- Identity Fraud (Similarity)
- Presentation Attacks
- Data Injection (Deep Fake)
- Social Engineering

~0,3% of all identifications are detected as attacks

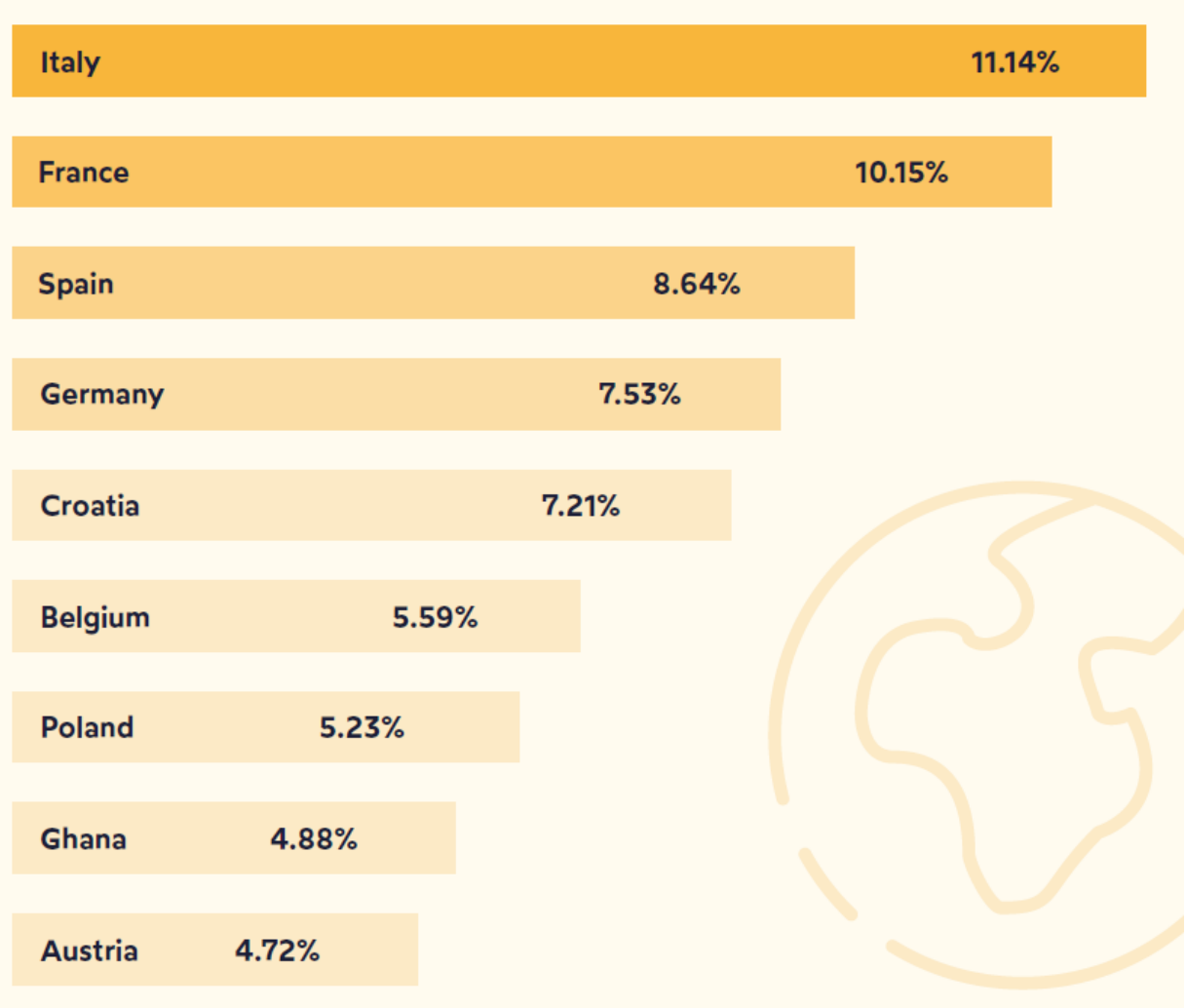
Breakdown of presentation attacks.



- Picture displayed on other phone
- Picture displayed on paper
- Picture displayed on monitor
- Paper mask
- Video displayed on other phone
- Video displayed on monitor

~75% of all detected frauds are presentation attacks

Top countries for fraudsters.



~65% of the fake ID-documents originated from the following countries

IDnow product certifications.

IDnow certifications help preventing attacks.

Existing

ISO 30107-3
ETSI EN 319 411-1 RA (NCP)
ETSI EN 319 411-2 RA (QCP)

BaFin AML Circular
Youth Protection / KJM
ETSI TS 119 461 (eIDAS art 24.1.d)

ANSSI CSPN
ETSI TS 119 461 (eIDAS art 24.1.d)

ETSI TS 119 461 (eIDAS art 24.1.d)

Sepblac AML

FINMA AML

Upcoming

ISO 27001

ANSSI PVID VideoIdent
ANSSI PVID IDcheck.io
FranceConnect Substantial

Planned

CC EAL 4+
ENISA EU-CC for the EUDI Wallet

BSI TR 03107 LoA High

ETSI TS 119 461.

- ETSI standard issued in **2021**
- Policy and security requirements for **trust services providing identity proofing**
- Focused on user identification for QTSPs issuing certificates under **eIDAS article 24.1**
- **Remote identity proofing requirements** described in eIDAS article 24.1.d
- Used in conjunction with **ETSI EN 319 411-1** (RA for normalized certificates) and **ETSI EN 319 411-2** (RA for qualified certificates)

- **IDnow products are certified** against ETSI TS 119 461 for:
  - **IDnow AutoIdent and VideoIdent** in **Germany** by TÜV-IT
  - **IDnow AutoIdent** in **France** by LSTI
  - **IDnow AutoIdent** in **Italy** by Bureau Veritas
- **Compliance with eIDAS article 24.1.d** and **ETSI EN 319 411-1/2**
- **IDnow were co-editors** of ETSI TS 119 461 v1.1.1, and are now part of the **task force for updating** ETSI TS 119 461 for eIDAS2

ISO 30107.

- ISO standard issued in **2017**
- Tests **Presentation Attack Detection (PAD)** at biometric capture during remote identity proofing
- Presentation attacks can be done through impersonation attacks or obfuscation attacks
- **Impersonation attack**: the attacker uses a false identity (either real or fake) to trick the liveness biometric capture
- **Obfuscation attack**: the attacker tries to avoid being recognized and circumvents the system

- **IDnow VideoIdent is certified against ISO 30107-3** (part 3: testing and reporting)
- **LSTI** is the CAB (Conformity Assessment Body) and main auditor of the certification
- **CLR** is the evaluation lab that performed testing against ISO 30107-3

ANSSI PVID.

- **French** certification standard for **remote identity proofing**
- Published in **2021**
- The French cybersecurity agency **ANSSI** is the certification body
- Certification levels: **substantial or high**
- PVID allows for **manual ("video") or automatic ("AI")** remote identity proofing
- Several references to **ISO 30107** for biometric verification and tests

- **IDnow VideoIdent and IDCheck.io are being certified against PVID**
- **LSTI** is the main auditor of the PVID certification
- **CLR** is the evaluation lab that performed testing against PVID
- **French police IRCGN** to run ID-document checks

Thanks!