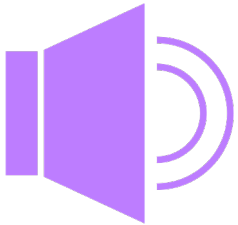
Regula

January 25, 2024

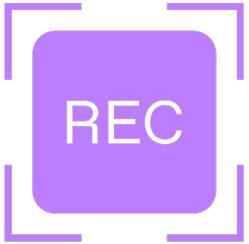
# Biometric ID Onboarding Dilemma: Fight Identity Fraud or Gain Customers?

# Housekeeping



Trouble with audio?
Try dialing in!


Submit your questions live
for our Q&A at the end




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

Name/Surname

# Henry Patishman

Business role

Executive VP of Identity Verification Solutions at Regula

Name/Surname

# Pascal Tavernier

Business role

Identity & Access Management Architect, Executive Director, UBS

Name/Surname

# Dmitry Smolyakov

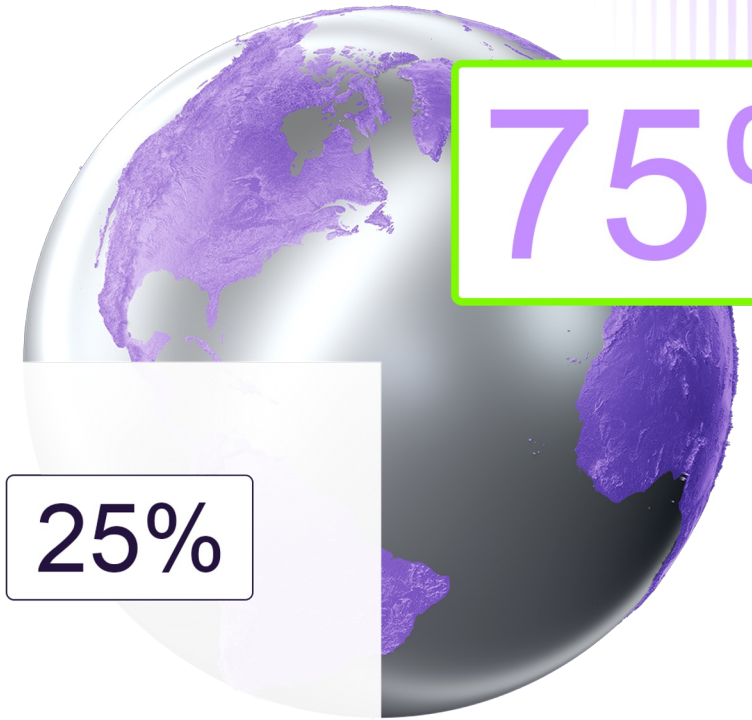
Business role

Head of Mobile and Web Development at Regula

# What Are Biometric Identity Documents?

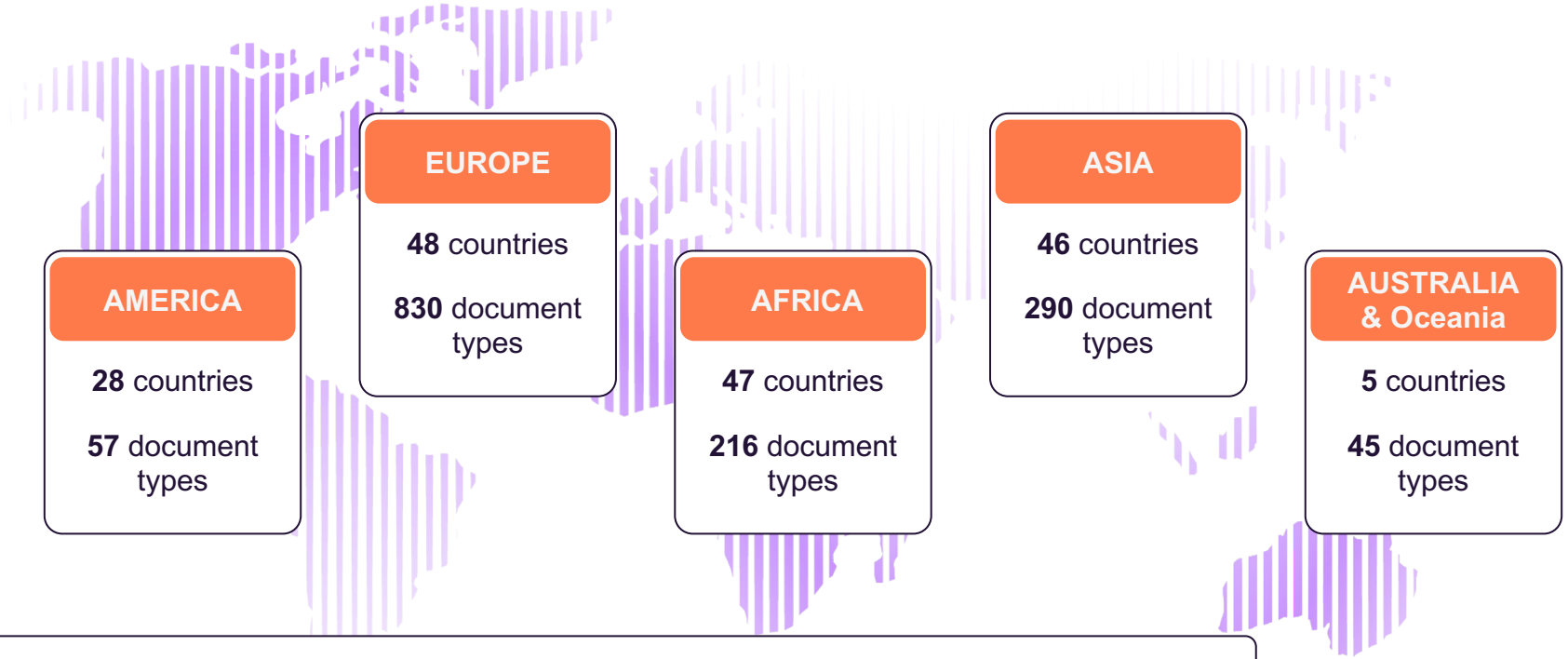
- **ICAO DOC 9303** standard: documents with an embedded contactless (NFC) chip including biographical and biometrical data stored in the chip
- **Terminology**: electronic Machine Readable Travel Document (eMRTD) ePassport, biometric passport, electronic identity card (eID)2 or biometric identity card

# Number of Biometric Documents




of countries have biometric documents

# Regula Biometric Document Coverage




But traditional documents still retain a significant share among all documents, especially for use within countries, so our document template database with more than 13,000 items is the most comprehensive and one of the largest.

# Benefits of Biometric and Limitations of Traditional Documents for Remote Verification

## Biometric Passports (eMRD)

Enhanced security against fraud and identity theft:

- An RFID chip holds data that can be read and verified with NFC-enabled smartphones and specialized IDV software - this makes counterfeiting electronic documents a harder task
- Personal Information is duplicated in different parts of the document, including the RFID chip
- RFID Chip Digital Signature

## Traditional Passports (MRP)

Limited security, can be forged by

- Personal data is much easier to be altered
- Photo replacement techniques and face morphing are evolving
- Difficult to check authenticity with the naked eye
- Increased fraud risks in remote onboarding scenarios

# Use Cases Where Biometric Documents are Crucial

Any remote interactions with the user that require identity verification when there are:

- → Self-service
- → E-signature required by regulators

**Banking & Fintech**

- Opening a bank account
- Opening an investment account
- Applying for a loan

**Government**

- Applying for documents
- Opening an account via a digital government portal
- Online tax filing
- Digital voting

**Insurance**

- Applying for insurance
- Insurance reimbursement
- Lodging an insurance claim

**Telecommunications**

- Activating a new SIM card
- Accessing account information
- Accessing online services

# Pro and Cons of Limiting Onboarding by Biometric IDs Only

Enhanced security

Streamlined onboarding process

Compliance with regulations

Improved customer experience

Cost savings by excluding manual checks

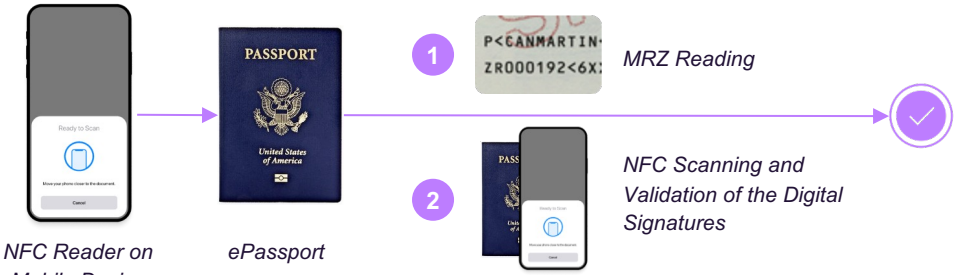
Potential revue losses

Drop in customer loyalty

Costs and implementation challenges

# Self-Service Remote Onboarding in Banks

## Digital Validation of the ePassport




## Automated Identity Verification


### Key Architecture Principles for the Mobile Device

➔Zero-Trust Model for the User's Mobile Device
➔Several Security Controls to Enforce the Zero-Trust Model
➔The User's Mobile Device is Used Only To Collect
- Information For Identity Proofing:
- Identity Document Scanning / NFC Reading
- Presence / Liveness Detection
- Face Photo / Selfie

### Key Architecture Principles for the Backend

➔Processing & Storing of Information Must Happen in a Trusted Backend Environment, i.e. Validating Document, Comparing Faces, Detecting Presence / Liveness
➔All Backend Services Designed to:
- Withstand any Cyber Security Threats – Secure by Design
- Support Various Consumers and Business Workflows
- Be Cloud Native - No Dependency on On-Prem Infrastructure

# The Technology Potential to Digitize Processes

**Digital Client Onboarding**
Digitize the prospect and client onboarding process by providing an intuitive self-service capability for the clients

**Re-Identification**
Digitize the re-identification process to renew digital signature certificates or when identity documents expired

**Personal Data Changes / Identity Document Updates**
Digitize the processes for personal data changes like name changes by providing a self-service capability to scan the new identity document

**Account Recovery**
Digitize and automate the account recovery process by providing biometric authentication and self-service identity verification

**Step Up Authentication & Identity Verification**
Automate and digitize identity verification for support or high-risk business transactions by providing biometric authentication

# Conversion Rate for Self-Service: Key Factors

1

## User Guidance: Visual, Animated Guidance Is a Must

**Most prospects/users drop out during the identity document scanning phase:** Scanning an identity document with a mobile phone camera and reading the chip data via NFC is NOT an intuitive process

2

## Error Handling: Provide Accurate, Context-Based Help

Users need crystal-clear, visual, animated instructions and real-time feedback: Failed attempts must trigger specific guidance to prevent the root cause (e.g., glare or loss of connection during NFC scan)

3

## Eligibility: Evaluate Self-Service Support at the Start of the Process

At the beginning of the process, evaluate whether a prospect is eligible for self-service to prevent frustrated users: document type, issuing country, mobile phone compatibility

### Recommendations

- ➔ Focus on Animated User Guidance and Accurate Error Handling
- ➔ Conduct as Many Usability Lab Sessions as You Can: You Have One Chance to Get it Right

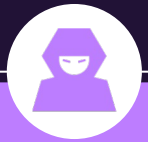
# Identity Document Validation: Evaluation Criteria

- Support of Identity documents
  - *Biometric passports and National ID*
- Usability / User Guidance / UI Customization / Error Handling Options
- Scanning & OCR Performance
  - *Older / Entry Level Phones, Poor Light Conditions, Glare*
- Server-side verification for biometric documents
- Biometric checks: Liveness detection, Face Match, Face Search
- On-premises vs SaaS: Data Privacy and Data Protection Aspects
- Size of SDK
- Developer Documentation / Code Samples for Customization
- Support for Artificial Testing Document

**Recommendations**

- Focus on User Guidance and Error Handling for Document Scanning
- Ensure that the Solution Supports Zero-Trust Model: Validation in a Trusted Environment

# Regula Addresses Customers' Requirements



## Fraud prevention

13,000+ document template database

Extra check of RFID chip on a server

Authenticity control

Document liveness

Cross-checks

Biometric checks

## Customer experience

Intuitive UI and in-built user guidance

Advanced document capture and image quality assessment

Automatic document type detection

Cross-platform support

## Implementation & integration

UI customization

Detailed developer documentation

On-premise installation

Test docs service

Adjusted size of SDK


# NFC-Based Verification - Zero Trust to Mobile

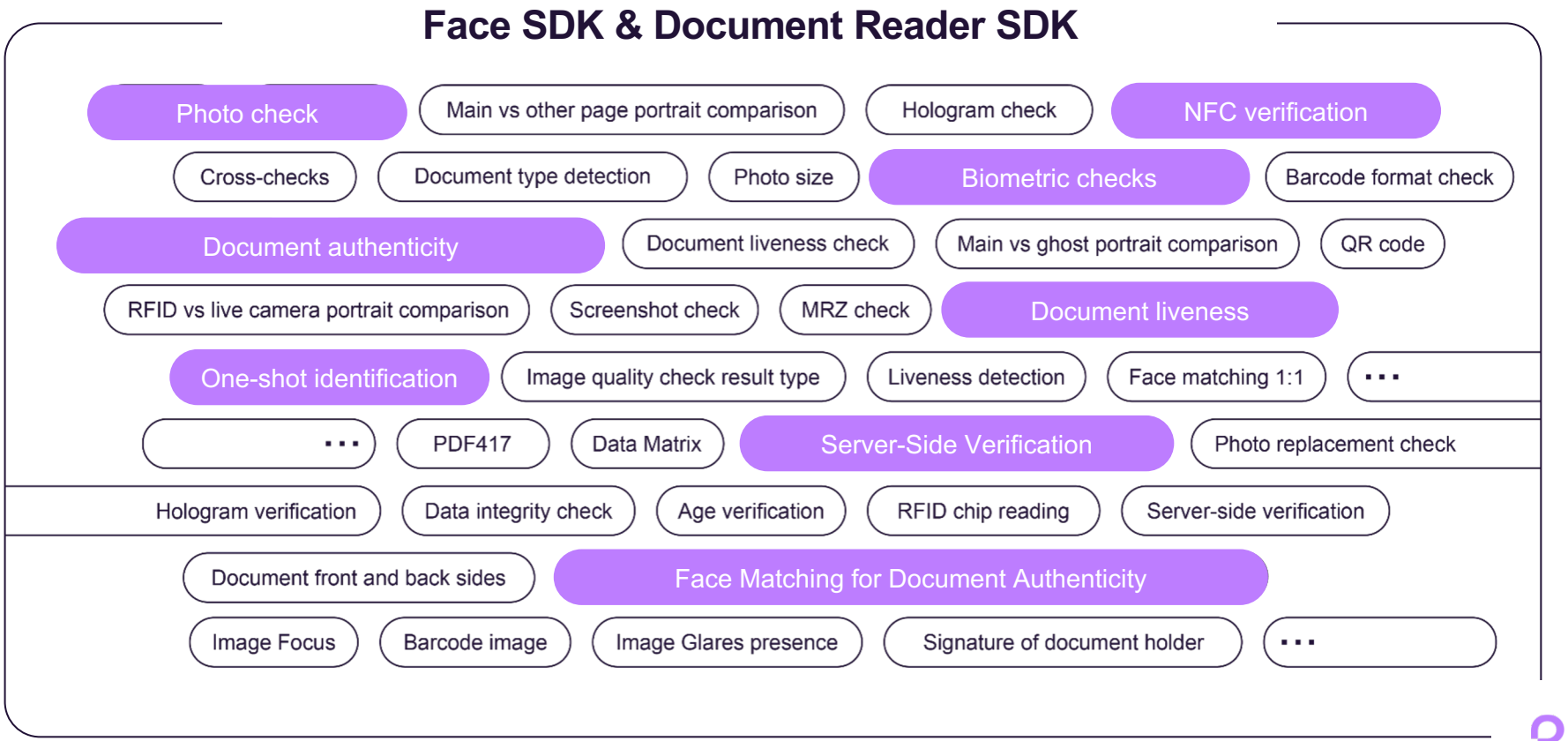
- Data from an RFID chip which is read using a mobile phone can be modified by fraudsters — therefore, mobile devices alone can't be trusted
- Data collected from mobile devices should be additionally verified on a server when a high level of protection is required

# Complete Server-Side Verification of Electronic Documents

An extra check of the RFID chip is performed, where the session is re-verified on a server for both chip and data authenticity.

This enables further reprocessing of the captured reading session in the “zero trust to mobile” model to validate the chip and its data authenticity and validity on the server side.

# Combination of Comprehensive Checks



# Testing the Solution: Challenges and Considerations

- Over 170 countries issue biometric identity documents
- Different designs, surfaces and security features
- Various races and ethnicities
- Using genuine identity documents in a development and testing environment is not a good idea, and it does not scale
- You'll need custom, artificial identity documents for testing purposes
- You should verify the testing requirements for certifications with the auditor right from the start (e.g. QES, eIDAS)

**Recommendations**

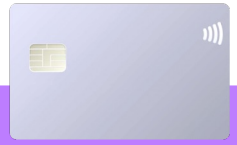
Add the Identity Document Testing Requirements to Your "Must Evaluate" Criteria

# Regula NFC TestKit Service

**Customer**


Technical specifications for testing use cases

**Regula**



Plastic cards with personalized NFC chips


Test passports with visual zone

Imitates real documents for each use case

# Regula NFC TestKit Service

## FEATURES

- Maximum similarity with original documents
- Flexible customization
- Extensive document template database
- Reliability


## Benefits for customers

- Short time to market
- Flexibility
- Efficient problem identification
- Maximum security assurance

# What’s next?

# Digital ID - Impact on Business Processes in Banks

## CHALLENGES

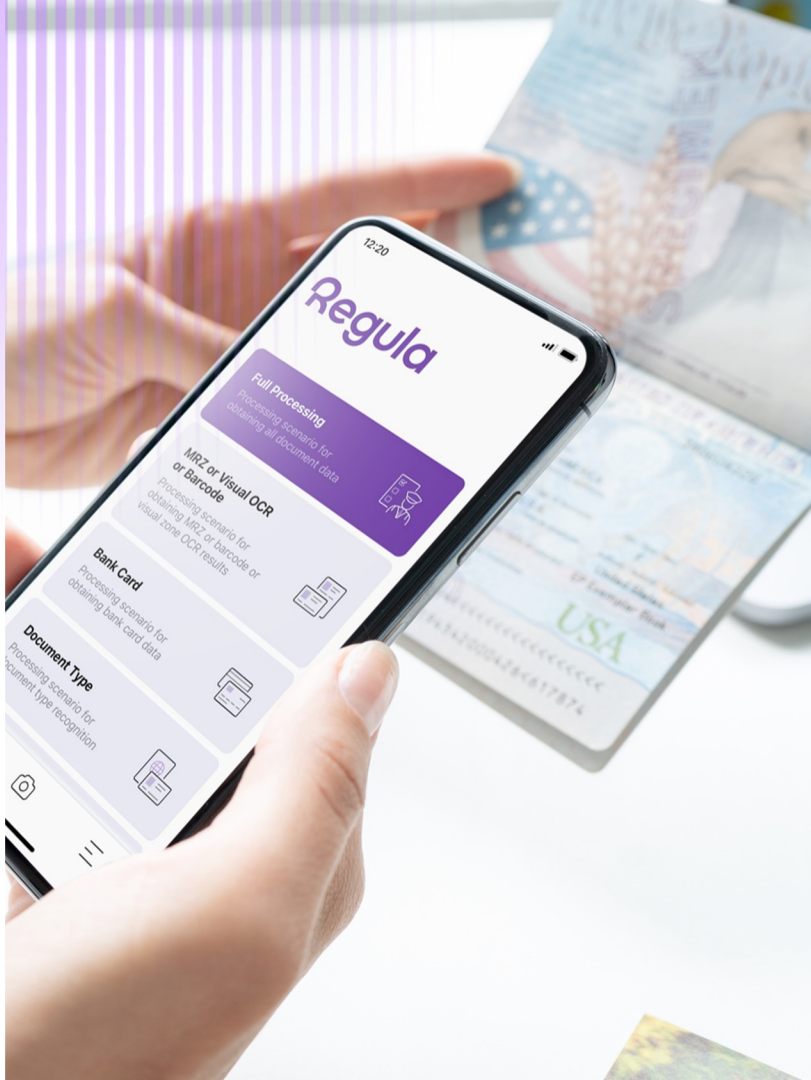
Regulatory compliance
Integration with existing systems
Security and fraud mitigation
User acceptance and adoption
Interoperability and standards
Technology infrastructure and investment
Change management

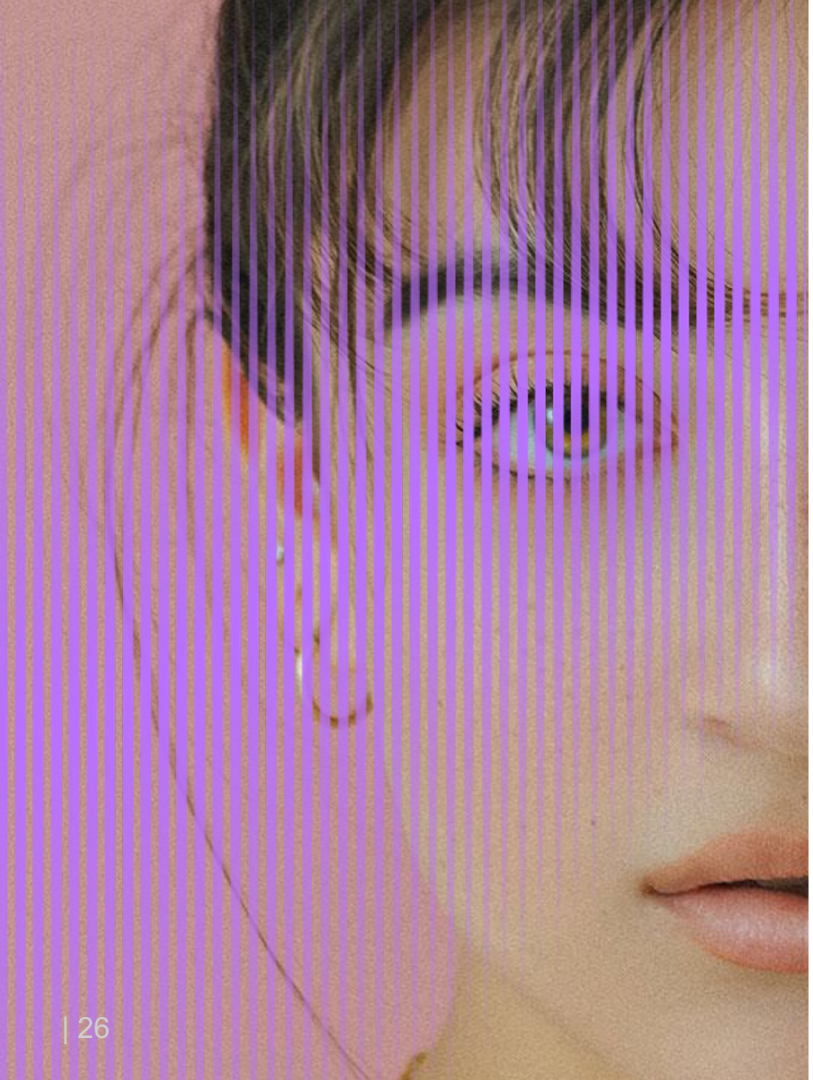
## OPPORTUNITIES

Enhanced customer experience
Streamlined onboarding and KYC processes
Improved security and fraud prevention
Expanded market reach
Data privacy and consent management
Innovation and product development
New collaboration and partnerships

# How Regula Supports Digital IDs:

- Sophisticated biometric technology
- One IDV flow supports all types of IDs: traditional (paper), biometric, and digital





# Key Takeaways

- As a business you can limit the onboarding process to biometric passports only if:
  - The penetration of biometric passports among your potential customers is high;
  - You are ready for potential negative consequences (profit reduction, reputational risk, etc.);
  - You have a robust IDV system to ensure secure and seamless remote onboarding.
- It makes sense to plan now for including digital IDs into existing onboarding processes.
- In reality, all types of documents should be supported — traditional, biometric, and digital.
- It’s critical to choose the right IDV partner.

# Questions?

# Thank you!

kate.johnson@regulaforensics.com

Regula

Decades of Forensics for Seamless Identity Verification.
Bringing together 30 years experience in forensics, border control and business, to create industry standards to trust and follow.