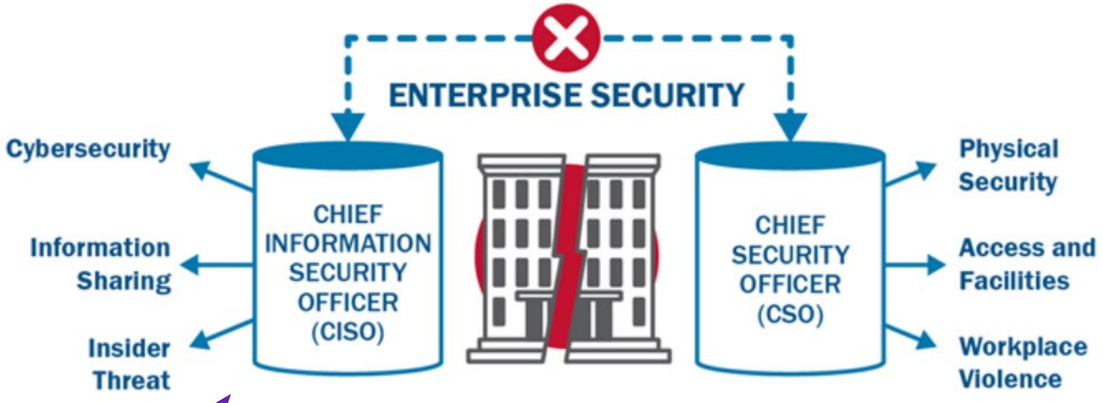
IDEMIA
PUBLIC SECURITY

What is your Roadmap for Enterprise Identity Security Convergence?

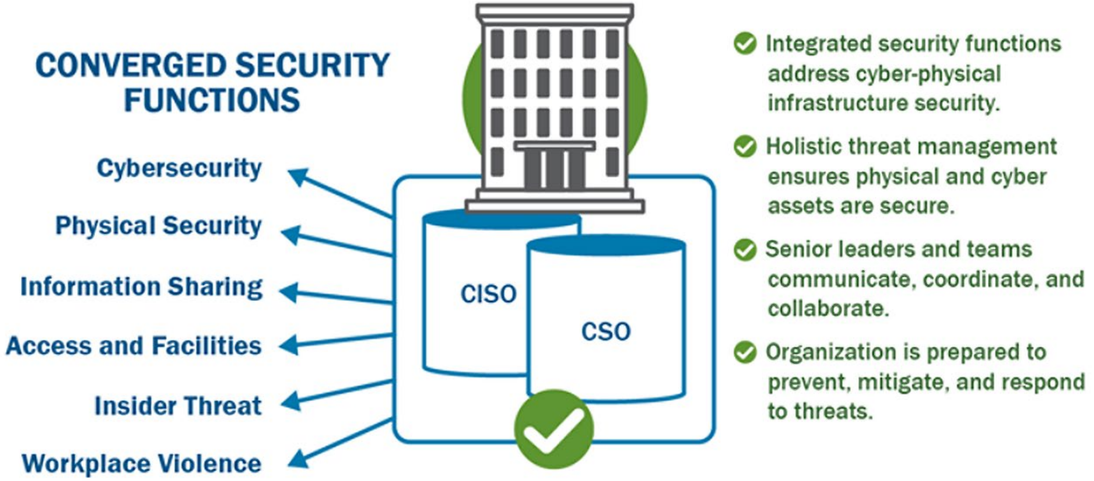
February 25, 2025

WHAT IS SECURITY CONVERGENCE?



IAM, SSO, MFA, Network Access Credentials

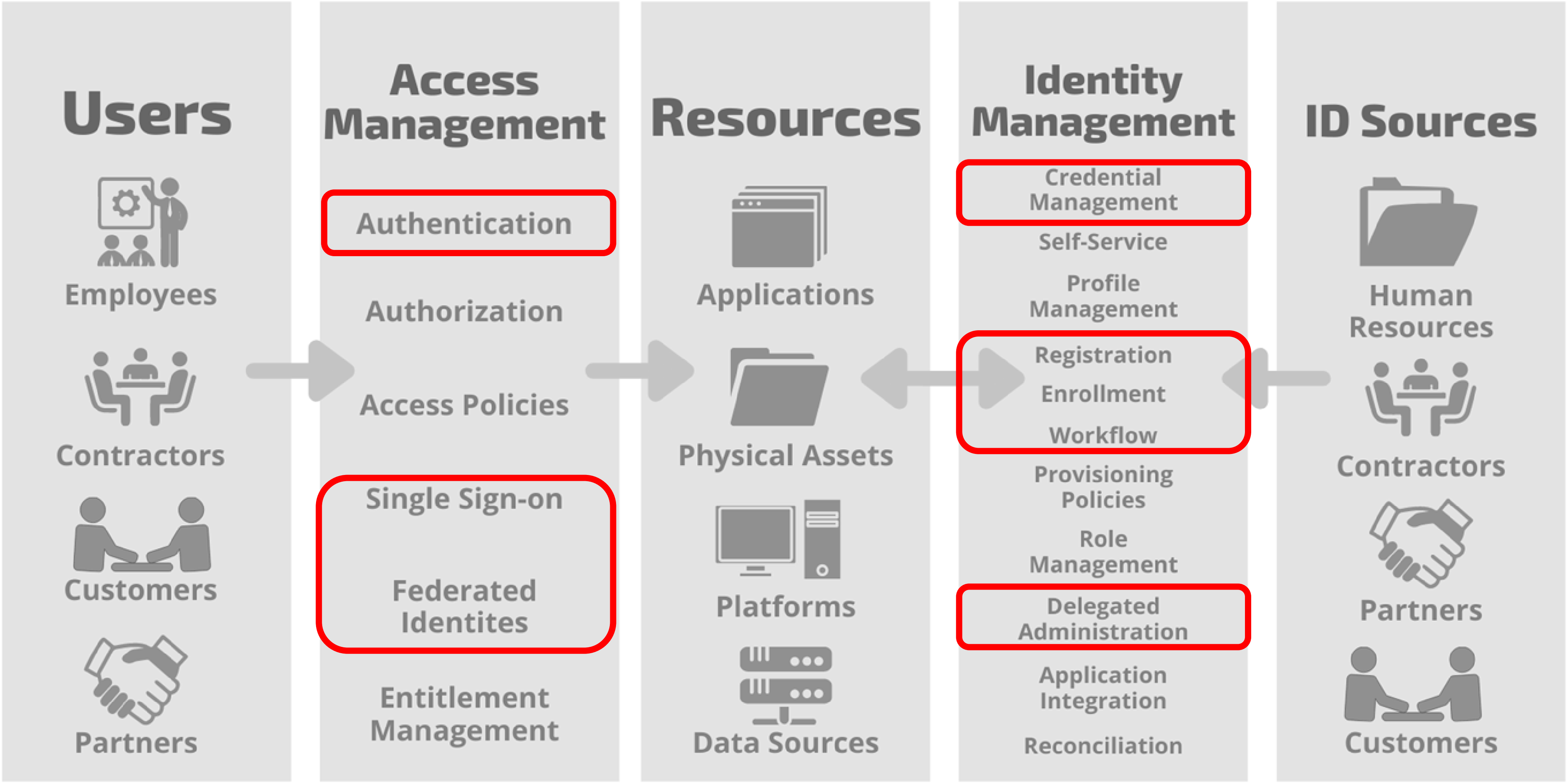
Vetting, ID Credentialing, On-/Off-boarding



- ✓ Integrated security functions address cyber-physical infrastructure security.
- ✓ Holistic threat management ensures physical and cyber assets are secure.
- ✓ Senior leaders and teams communicate, coordinate, and collaborate.
- ✓ Organization is prepared to prevent, mitigate, and respond to threats.

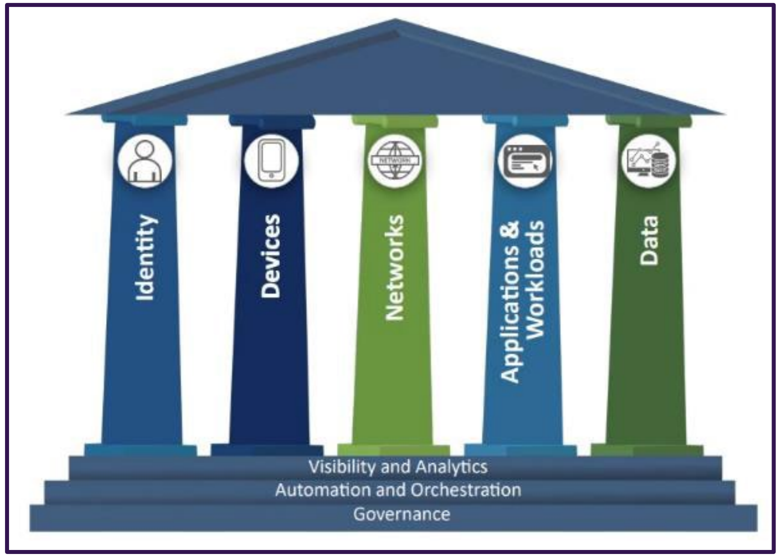
Cybersecurity and Physical Security Convergence Action Guide | CISA

IDENTITY ACCESS MANAGEMENT



[Understanding Key Identity & Access Management Components | Blog]

CHALLENGES AHEAD

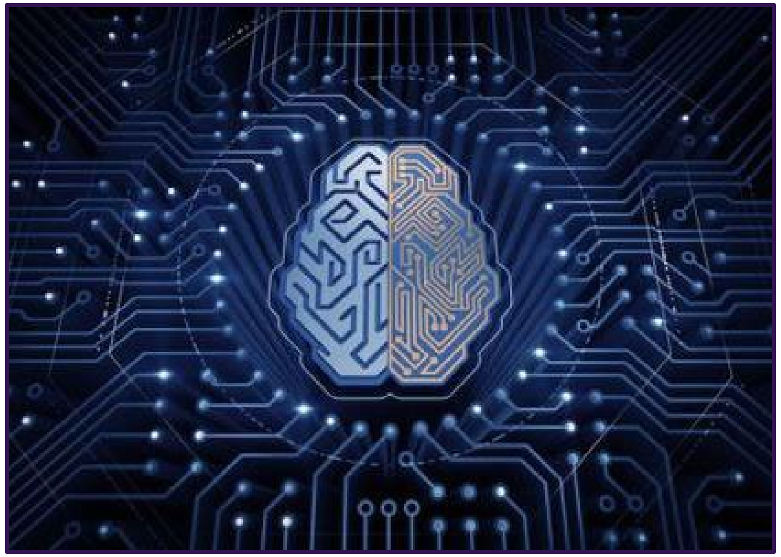


Zero Trust

- Device identification
- User identity verification and MFA
- Secure communication
- Policy enforcement & adjustment

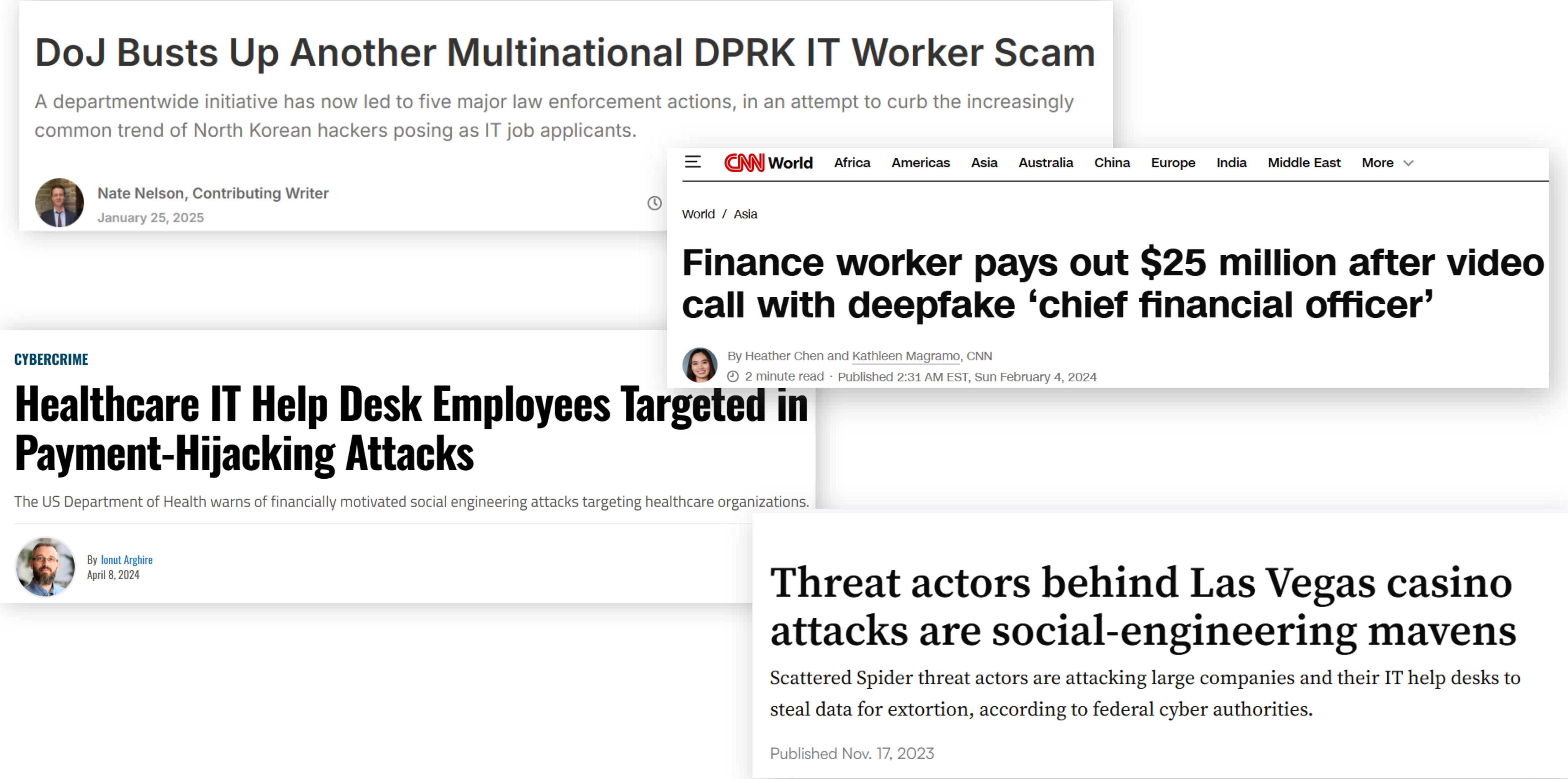
Hybrid Workforce

- Increasingly dispersed workforce
- Seasonal workforce
- Mobile devices, BYOD policies
- Interview fraud, compliance visibility



Gen AI and Quantum Agility

- Sophisticated spoofing, injection and presentation attacks
- Post-quantum computing migration yet to be planned for



DoJ Busts Up Another Multinational DPRK IT Worker Scam

A departmentwide initiative has now led to five major law enforcement actions, in an attempt to curb the increasingly common trend of North Korean hackers posing as IT job applicants.

Nate Nelson, Contributing Writer
January 25, 2025

World / Asia

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN
2 minute read · Published 2:31 AM EST, Sun February 4, 2024

CYBERCRIME

Healthcare IT Help Desk Employees Targeted in Payment-Hijacking Attacks

The US Department of Health warns of financially motivated social engineering attacks targeting healthcare organizations.

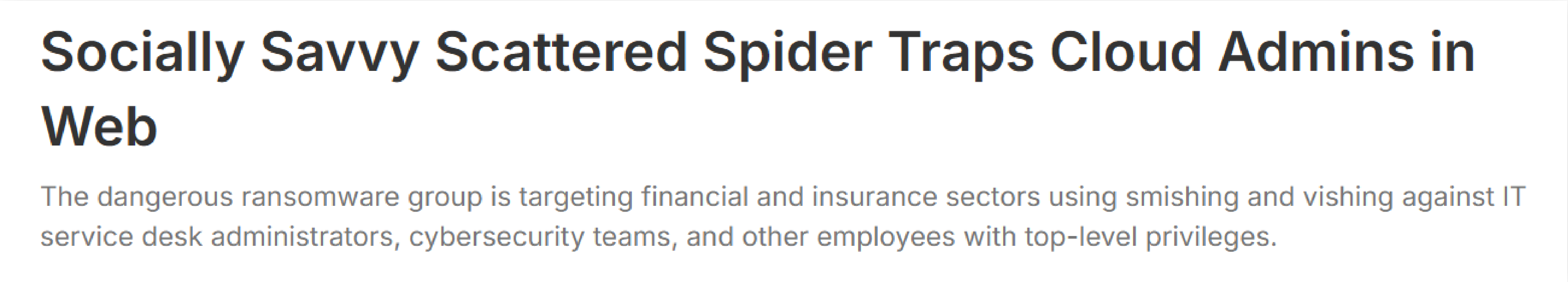
By Ionut Arghire
April 8, 2024

Threat actors behind Las Vegas casino attacks are social-engineering mavens

Scattered Spider threat actors are attacking large companies and their IT help desks to steal data for extortion, according to federal cyber authorities.

Published Nov. 17, 2023

EMPLOYEE-TARGETED ATTACKS

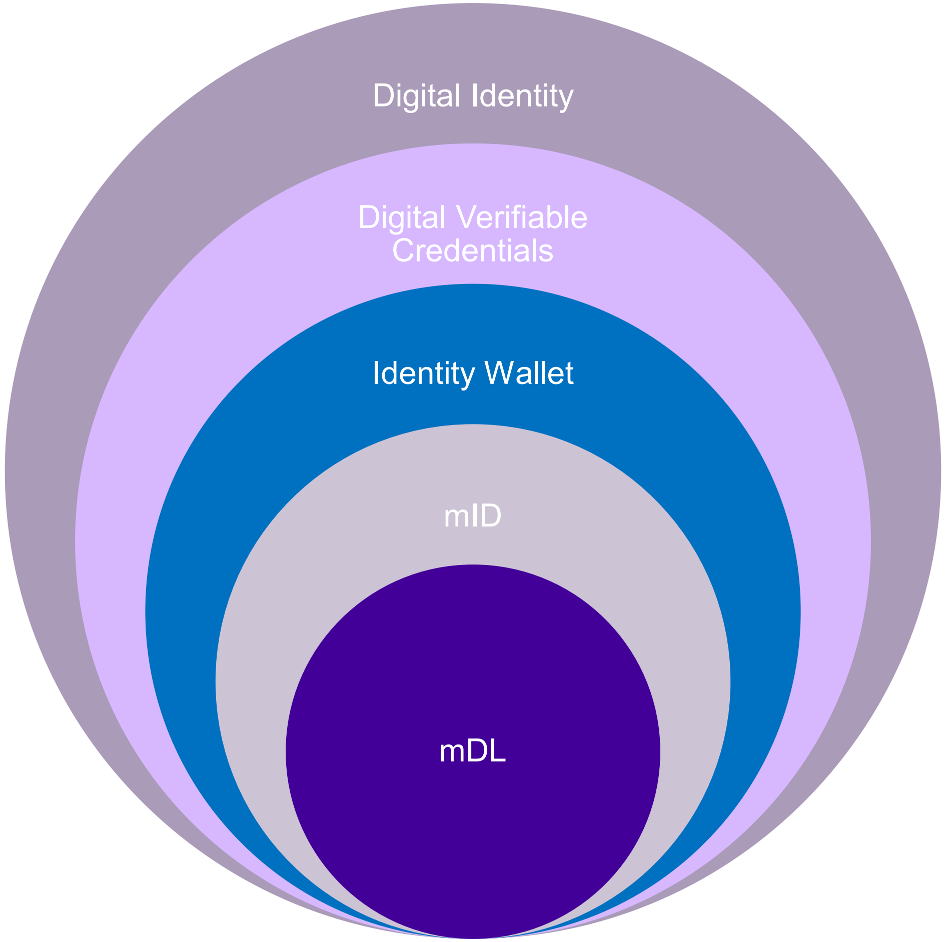


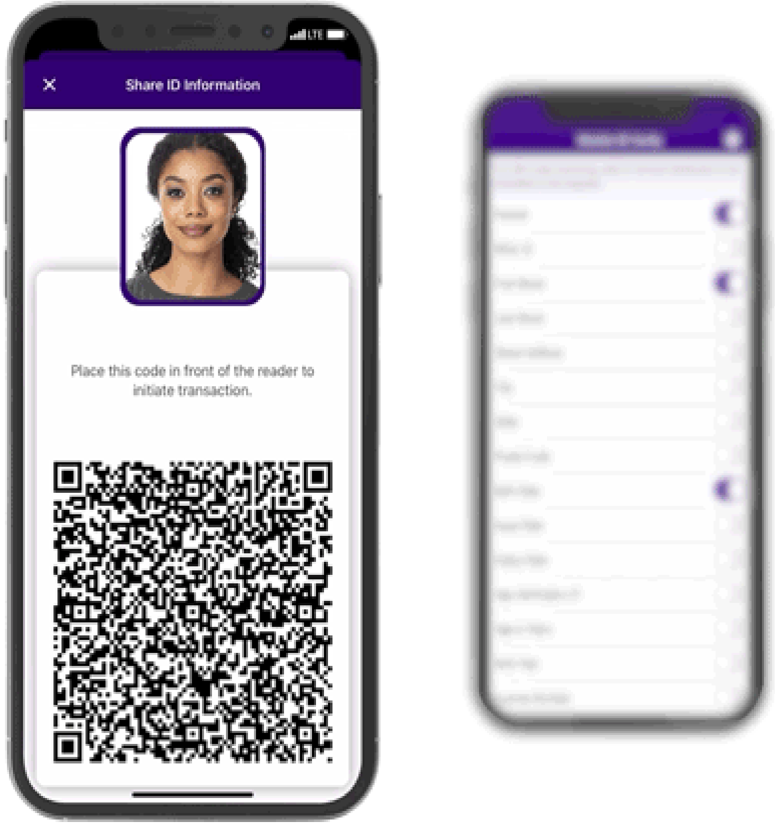
Socially Savvy Scattered Spider Traps Cloud Admins in Web

The dangerous ransomware group is targeting financial and insurance sectors using smishing and vishing against IT service desk administrators, cybersecurity teams, and other employees with top-level privileges.

Scattered Spider, a financially motivated threat actor, is infamous for gaining initial access using a variety of social engineering tactics, which include **calling employees and impersonating IT staff, using Telegram and SMS messages that redirect to phishing sites, and employing MFA fatigue.** The threat actor can also engage with the victims directly to obtain their one-time passwords (OTPs).
After gaining access, the adversary stays away from using specialized malware and favors a variety of reliable remote management tools to maintain persistent access.

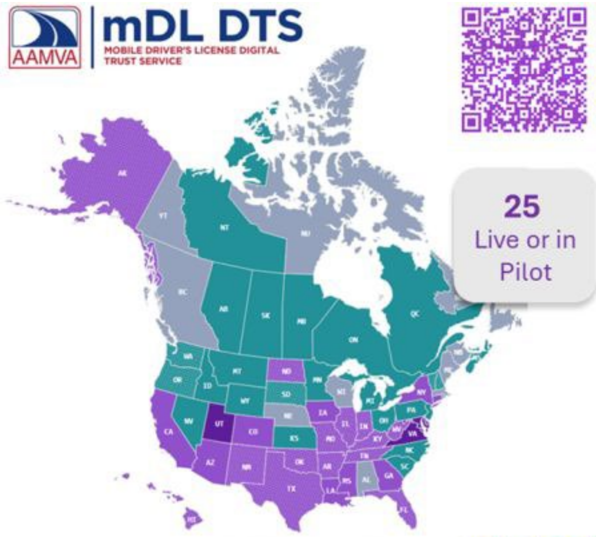
MOBILE DRIVER’S LICENSE




Share ID Information

Place this code in front of the reader to initiate transaction.

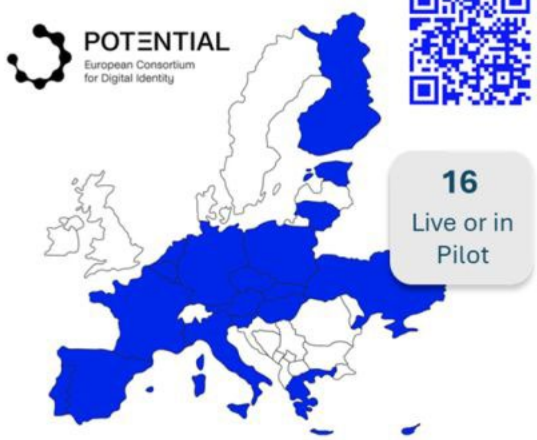
MOBILE DRIVER'S LICENSE



25
Live or in Pilot

North America mDL Implementations

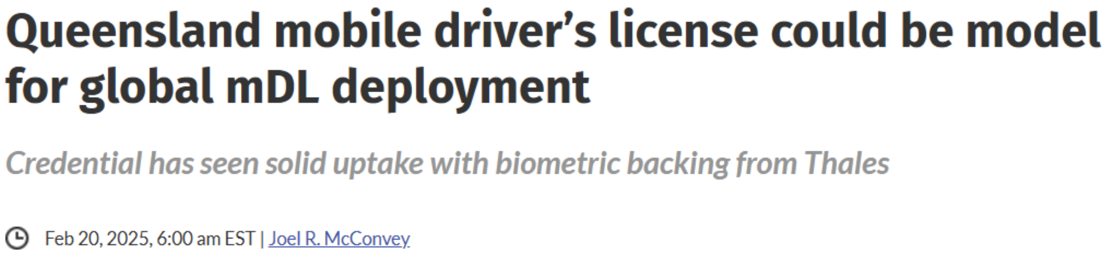
- ■ Public Key Available in Digital Trust Service
- 🟪 Interoperable implementation
- ▨ Interoperable implementation in progress
- 🟩 Legislative and/or study activity
- ▨ Attempt to execute legislative and/or study activity
- ⬜ No information available



16
Live or in Pilot

European Countries mDL Implementations

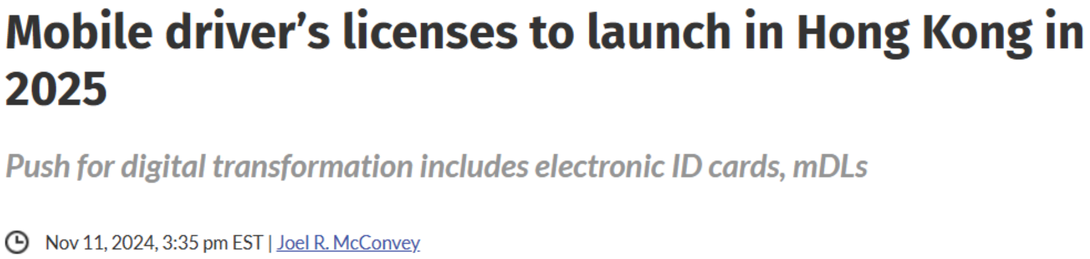
- ● Austria
- ● Belgium
- ● Cyprus
- Czechia
- ● Estonia
- ● Italy
- ● Lithuania
- ● Luxembourg
- ● Netherlands
- ● Poland
- ● Finland
- ● France Leader
- ● Germany Leader
- ● Greece
- Hungary
- ● Portugal
- ● Slovakia
- Slovenia
- ● Spain
- ● Ukraine



Queensland mobile driver's license could be model for global mDL deployment

Credential has seen solid uptake with biometric backing from Thales

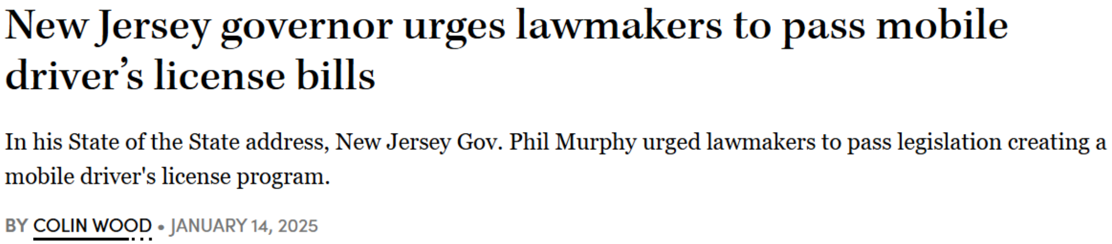
Feb 20, 2025, 6:00 am EST | Joel R. McConvey



Mobile driver's licenses to launch in Hong Kong in 2025

Push for digital transformation includes electronic ID cards, mDLs

Nov 11, 2024, 3:35 pm EST | Joel R. McConvey

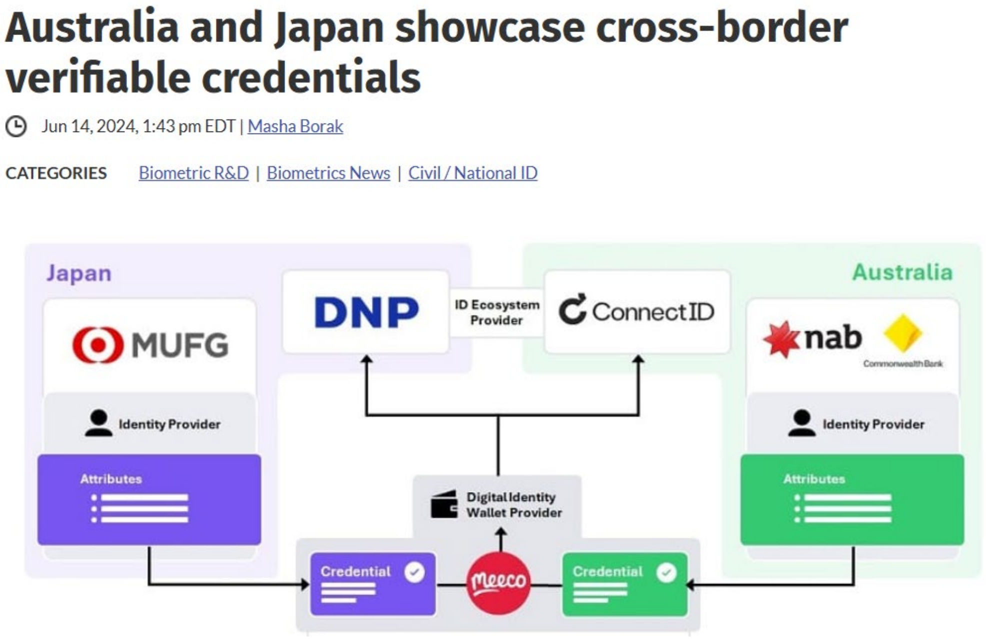


New Jersey governor urges lawmakers to pass mobile driver's license bills

In his State of the State address, New Jersey Gov. Phil Murphy urged lawmakers to pass legislation creating a mobile driver's license program.

BY COLIN WOOD • JANUARY 14, 2025

IDENTITY WALLET & DIGITAL VERIFIABLE CREDENTIALS



Australia and Japan showcase cross-border verifiable credentials

Jun 14, 2024, 1:43 pm EDT | Masha Borak

CATEGORIES Biometric R&D | Biometrics News | Civil / National ID

The Digital Identity Regulation enters into force.
REGULATION
EU
European Commission
EU Digital Identity Wallet

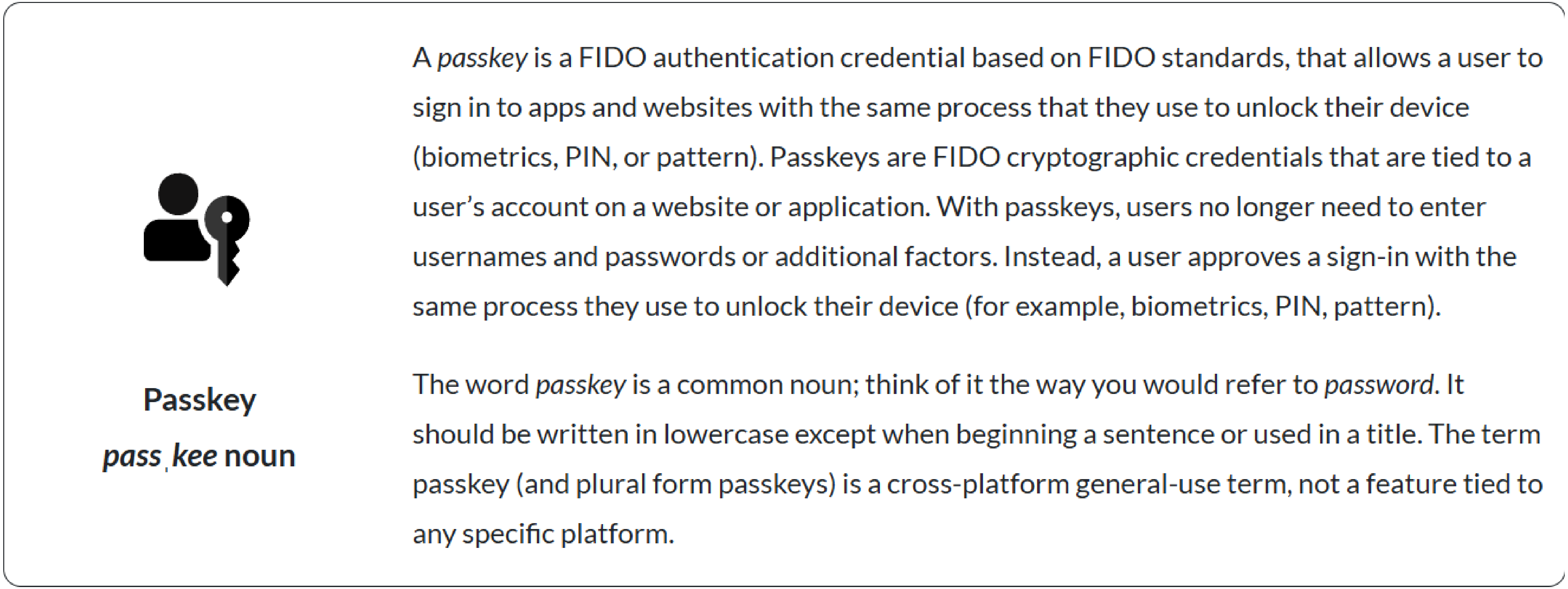
W3C®

OpenID®

OpenWallet FOUNDATION

IETF®

PASSKEY



A *passkey* is a FIDO authentication credential based on FIDO standards, that allows a user to sign in to apps and websites with the same process that they use to unlock their device (biometrics, PIN, or pattern). Passkeys are FIDO cryptographic credentials that are tied to a user's account on a website or application. With passkeys, users no longer need to enter usernames and passwords or additional factors. Instead, a user approves a sign-in with the same process they use to unlock their device (for example, biometrics, PIN, pattern).

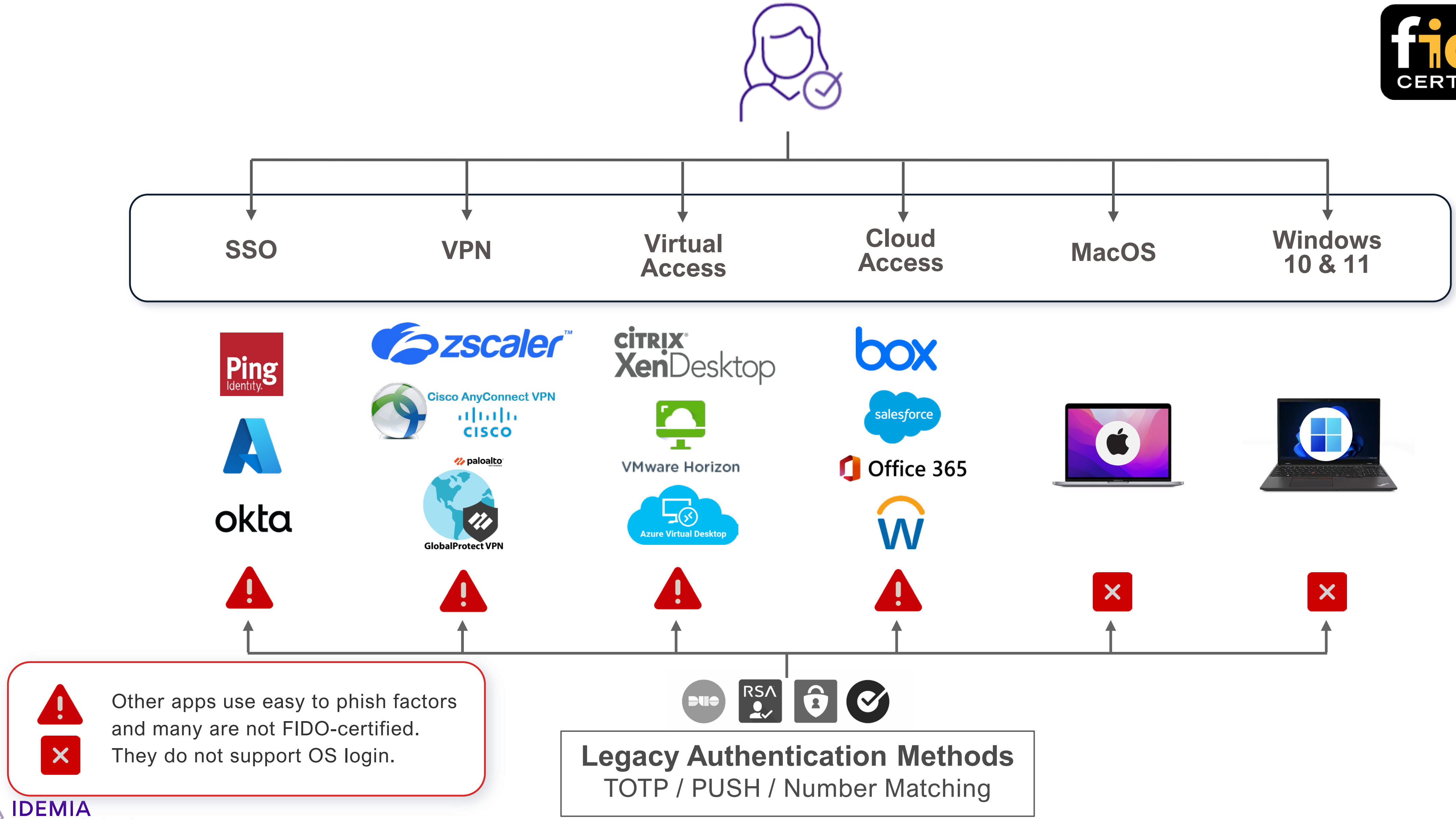
Passkey

***passˌkee* noun**

The word *passkey* is a common noun; think of it the way you would refer to *password*. It should be written in lowercase except when beginning a sentence or used in a title. The term passkey (and plural form passkeys) is a cross-platform general-use term, not a feature tied to any specific platform.

PHISHING-RESISTANT. EVERYWHERE.

fido™ CERTIFIED FIDO2



SSO

VPN

Virtual Access

Cloud Access

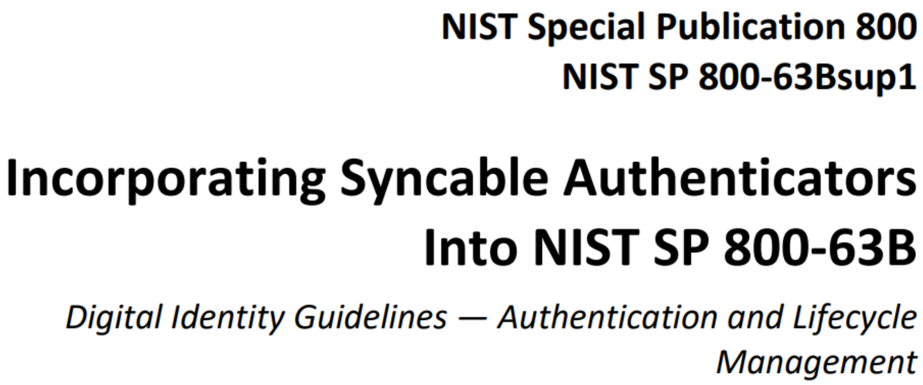
MacOS

Windows 10 & 11

⚠ ☒ Other apps use easy to phish factors and many are not FIDO-certified. They do not support OS login.

Legacy Authentication Methods
TOTP / PUSH / Number Matching

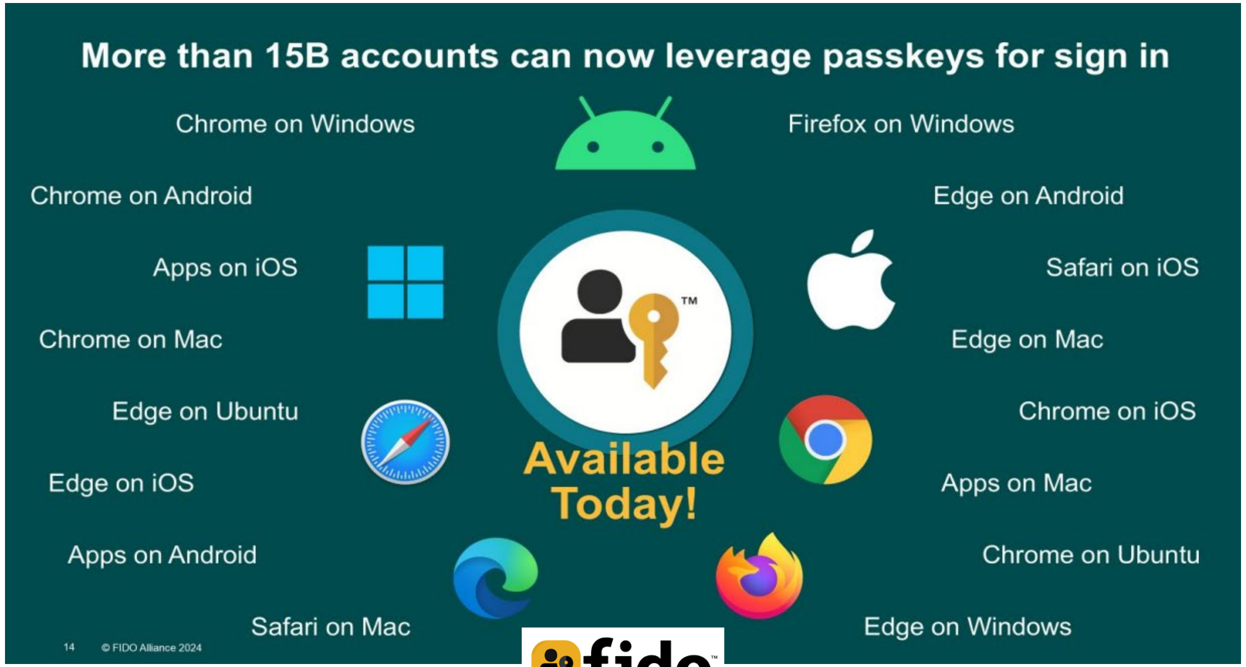
PASSKEY



NIST Special Publication 800
NIST SP 800-63Bsup1

Incorporating Syncable Authenticators Into NIST SP 800-63B

Digital Identity Guidelines — Authentication and Lifecycle Management

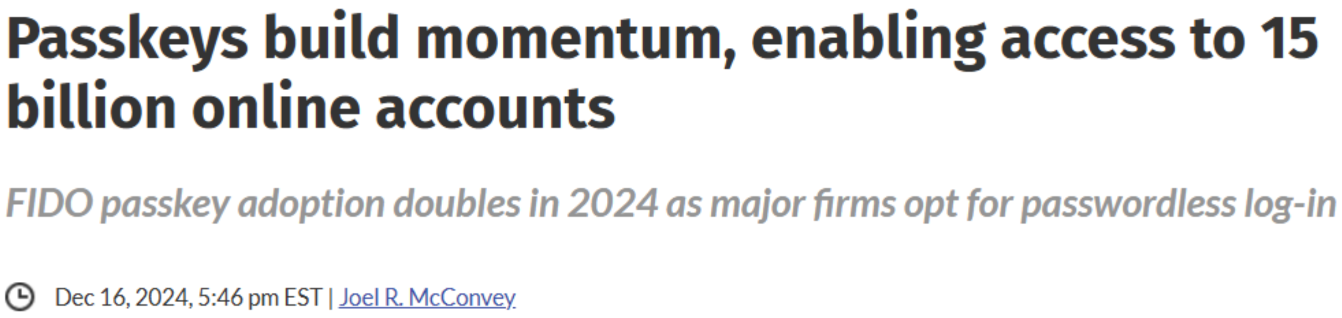


More than 15B accounts can now leverage passkeys for sign in

Chrome on Windows	Firefox on Windows
Chrome on Android	Edge on Android
Apps on iOS	Safari on iOS
Chrome on Mac	Edge on Mac
Edge on Ubuntu	Chrome on iOS
Edge on iOS	Apps on Mac
Apps on Android	Chrome on Ubuntu
Safari on Mac	Edge on Windows

14 © FIDO Alliance 2024

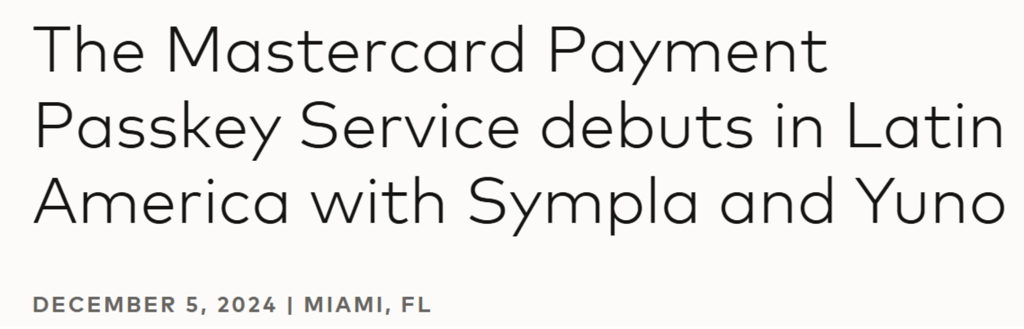
fido ALLIANCE



Passkeys build momentum, enabling access to 15 billion online accounts

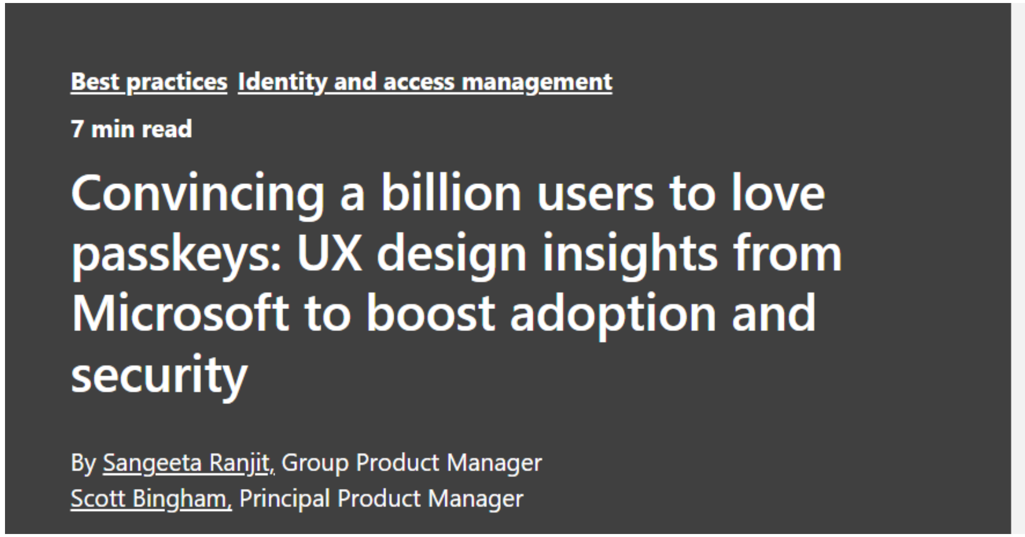
FIDO passkey adoption doubles in 2024 as major firms opt for passwordless log-in

Dec 16, 2024, 5:46 pm EST | Joel R. McConvey



The Mastercard Payment Passkey Service debuts in Latin America with Sympla and Yuno

DECEMBER 5, 2024 | MIAMI, FL



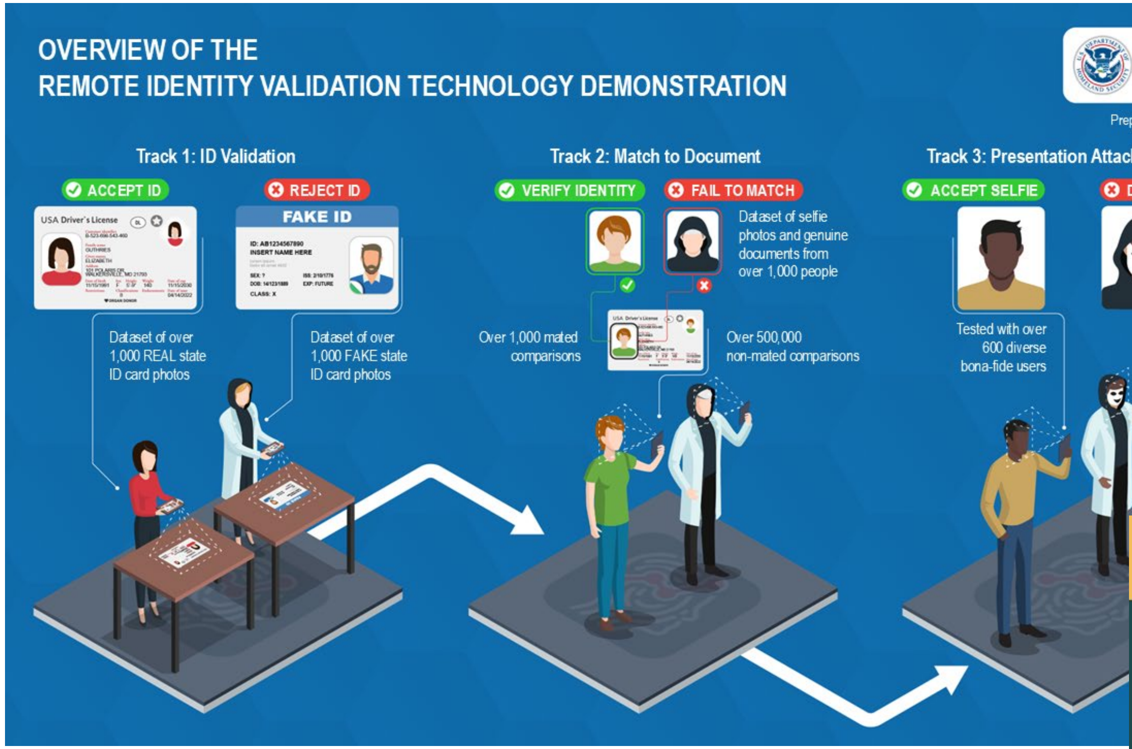
Best practices Identity and access management

7 min read

Convincing a billion users to love passkeys: UX design insights from Microsoft to boost adoption and security

By Sangeeta Ranjit, Group Product Manager
Scott Bingham, Principal Product Manager

IDENTITY VERIFICATION



OVERVIEW OF THE
REMOTE IDENTITY VALIDATION TECHNOLOGY DEMONSTRATION

Science and Technology

Prepared by the IDSL

Track 1: ID Validation

✓ ACCEPT ID

☒ REJECT ID

FAKE ID

Dataset of over 1,000 REAL state ID card photos

Dataset of over 1,000 FAKE state ID card photos

Track 2: Match to Document

✓ VERIFY IDENTITY

☒ FAIL TO MATCH

Dataset of selfie photos and genuine documents from over 1,000 people

Over 1,000 mated comparisons

Over 500,000 non-mated comparisons

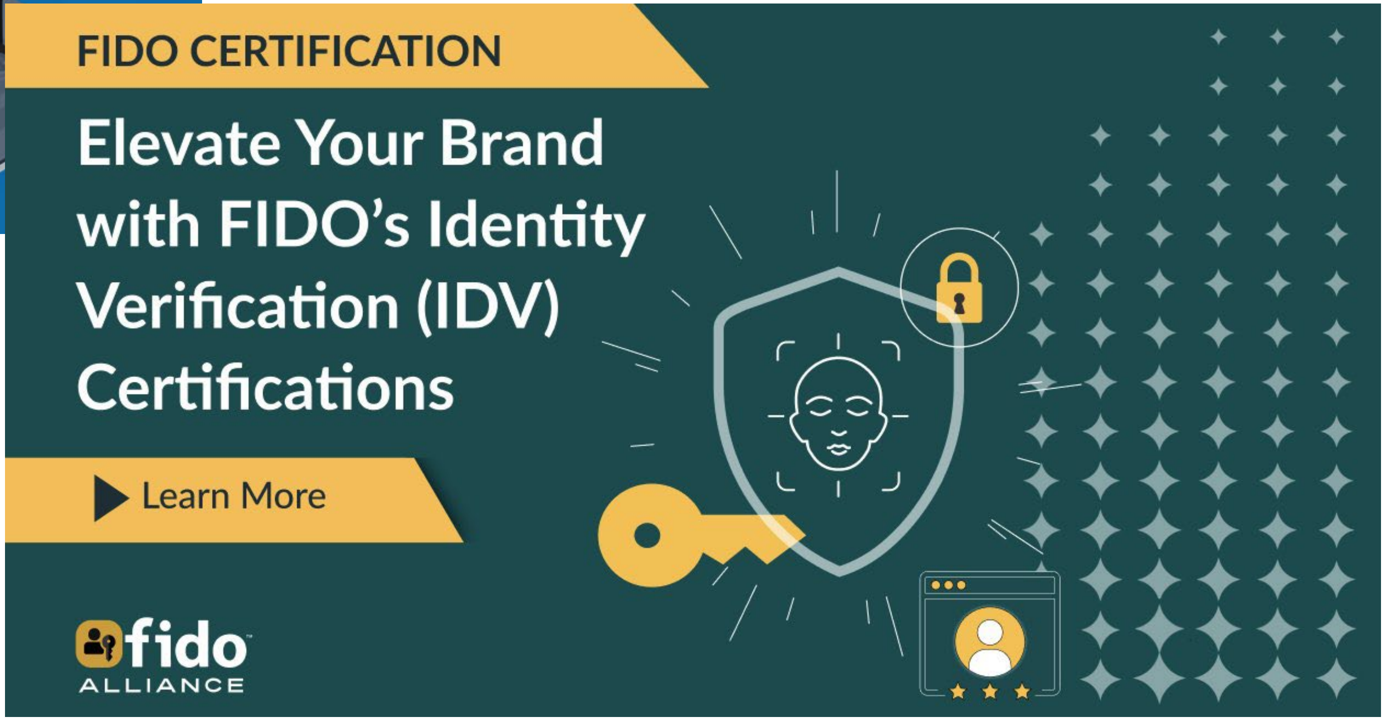
Track 3: Presentation Attack Detection

✓ ACCEPT SELFIE

☒ DETECT ATTACK

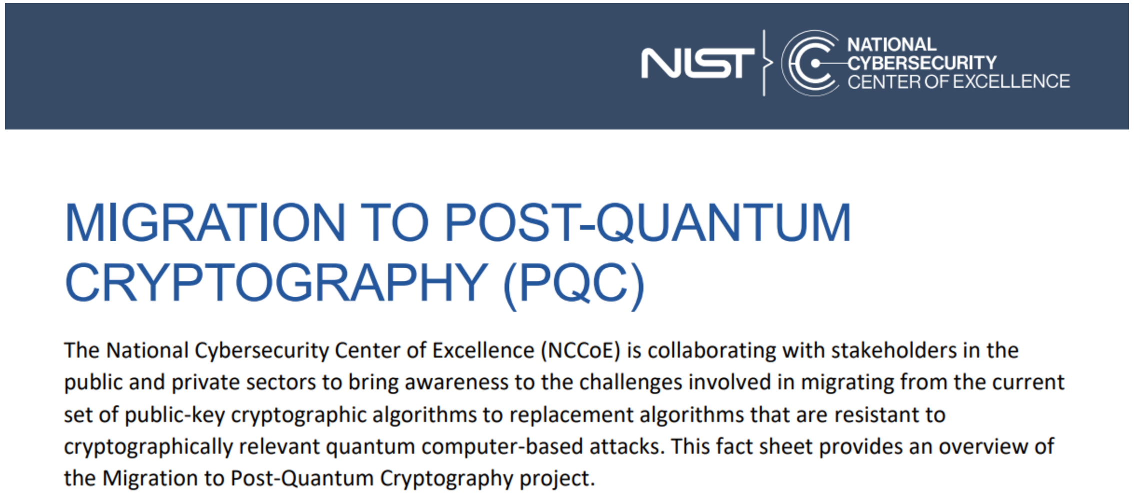
Tested with over 600 diverse bona-fide users

Tested with over 1,200 presentation attacks


FIDO CERTIFICATION
Elevate Your Brand with FIDO's Identity Verification (IDV) Certifications
Learn More
fido ALLIANCE

IDEMIA
PUBLIC SECURITY

QUANTUM COMPUTING



NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

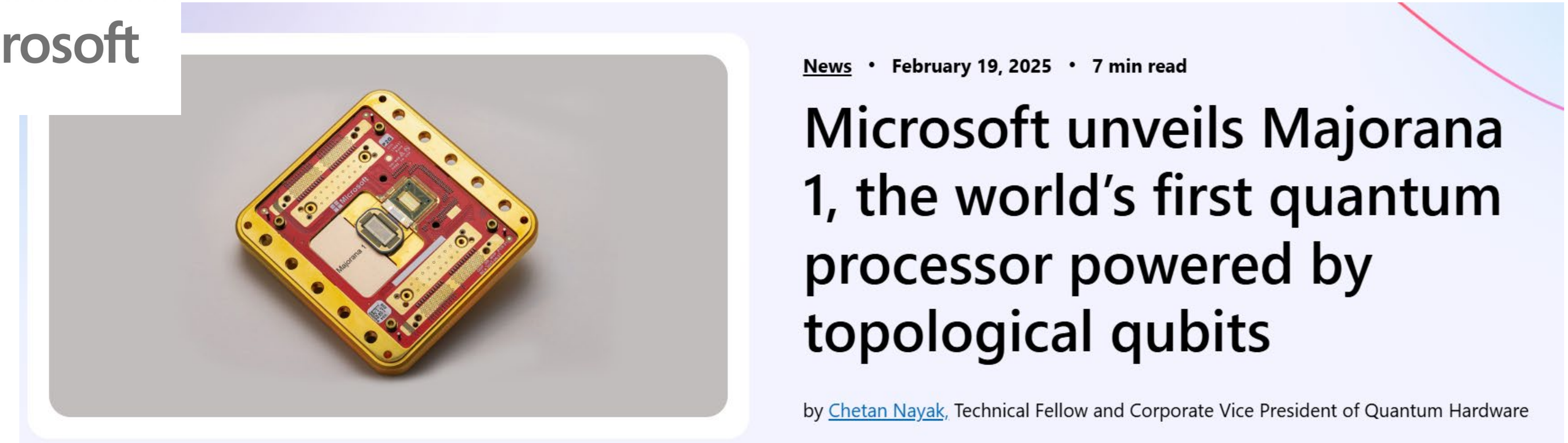
MIGRATION TO POST-QUANTUM CRYPTOGRAPHY (PQC)

The National Cybersecurity Center of Excellence (NCCoE) is collaborating with stakeholders in the public and private sectors to bring awareness to the challenges involved in migrating from the current set of public-key cryptographic algorithms to replacement algorithms that are resistant to cryptographically relevant quantum computer-based attacks. This fact sheet provides an overview of the Migration to Post-Quantum Cryptography project.

EUROPOL
EUROPEAN LAW ENFORCEMENT AGENCY

Call for action: urgent plan needed to transition to post-quantum cryptography together

Europol's Quantum Safe Financial Forum implores the financial sector to act now to combat the quantum related threat



Microsoft

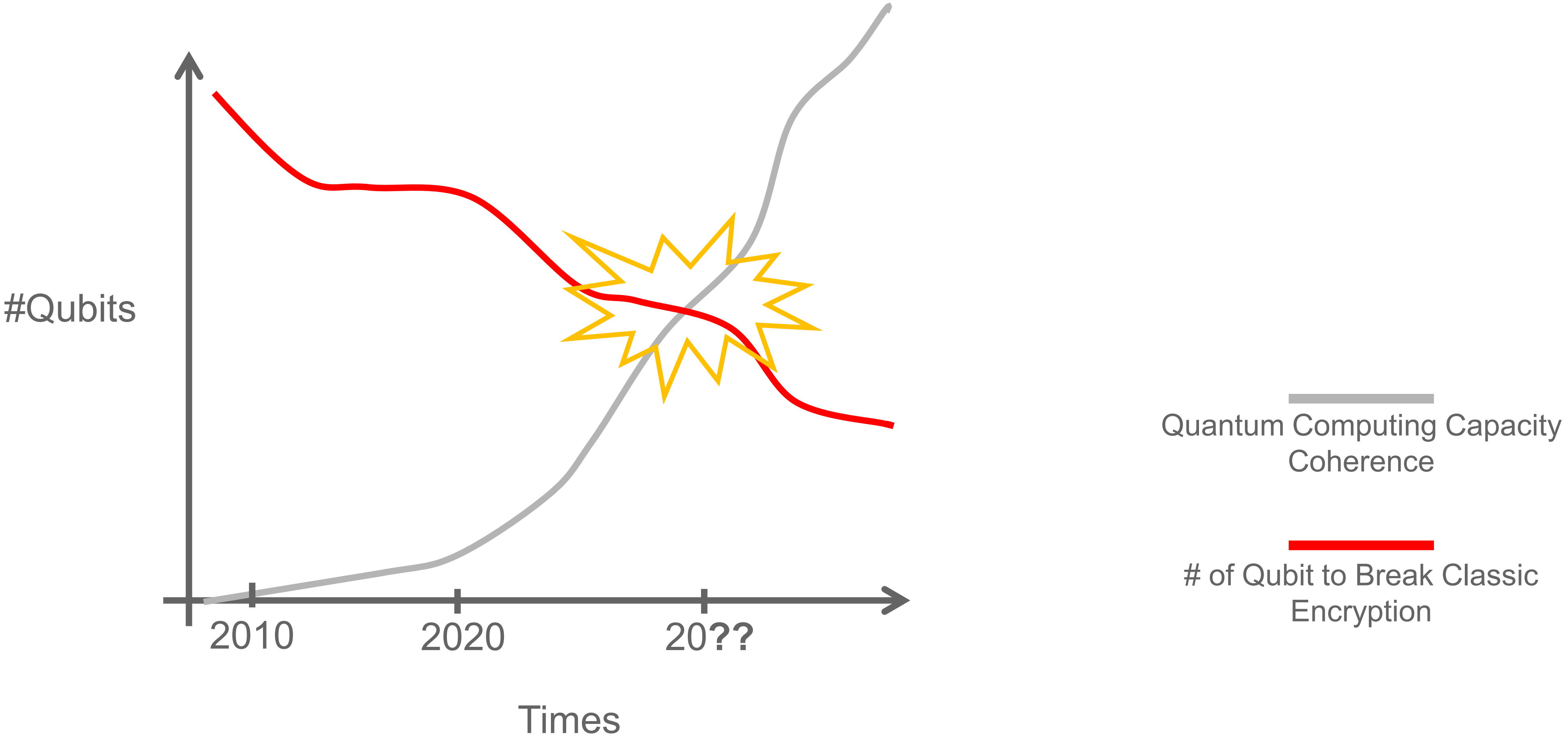
News • February 19, 2025 • 7 min read

Microsoft unveils Majorana 1, the world's first quantum processor powered by topological qubits

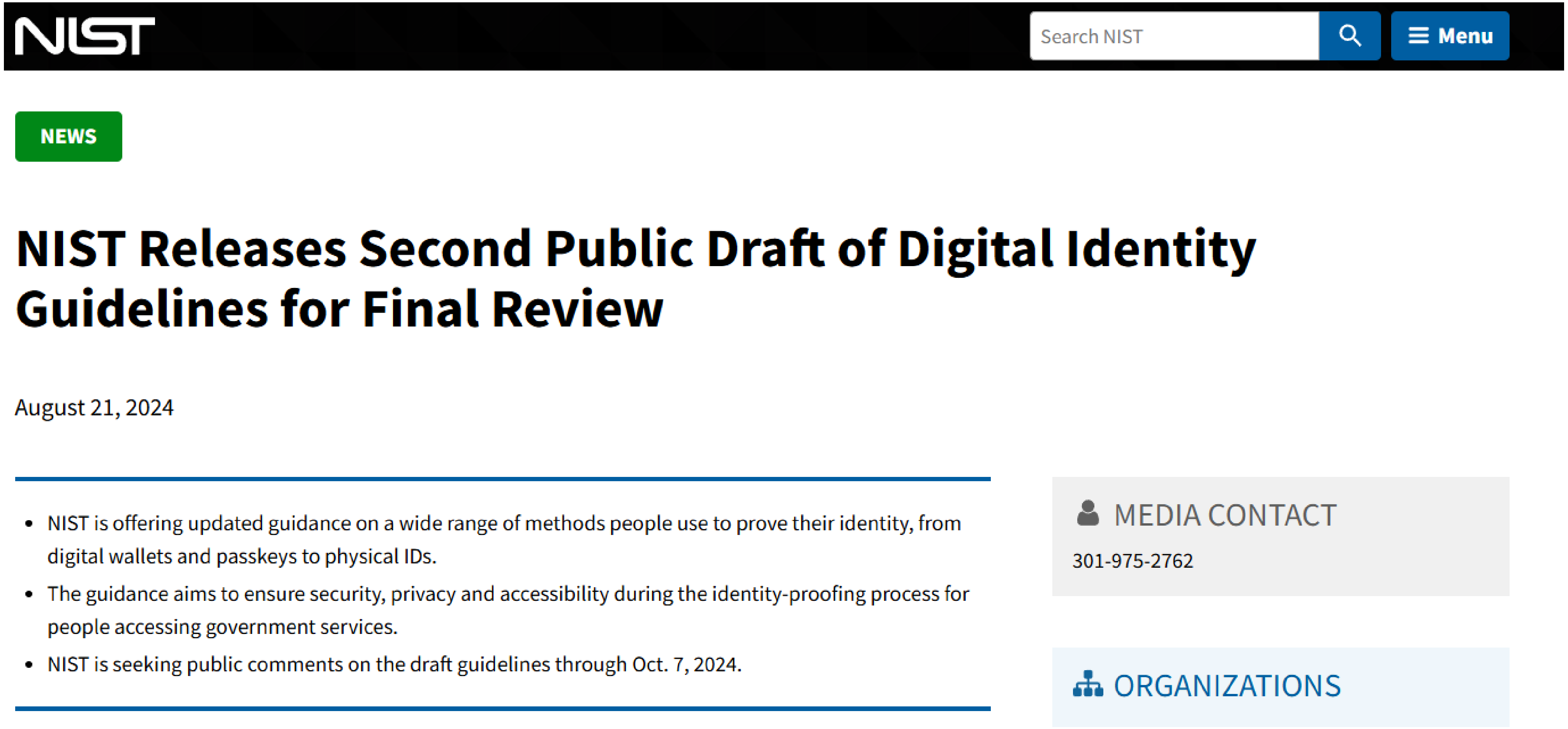
by Chetan Nayak, Technical Fellow and Corporate Vice President of Quantum Hardware

WHEN IS Q-DAY (Y2Q)?

The term "q-day" refers the day when cryptographically relevant quantum computers (crqcs) can break common (classic) cryptographic protocols using quantum algorithms.



NIST DIGITAL IDENTITY GUIDELINES….



NIST Releases Second Public Draft of Digital Identity Guidelines for Final Review

August 21, 2024

- NIST is offering updated guidance on a wide range of methods people use to prove their identity, from digital wallets and passkeys to physical IDs.
- The guidance aims to ensure security, privacy and accessibility during the identity-proofing process for people accessing government services.
- NIST is seeking public comments on the draft guidelines through Oct. 7, 2024.

MEDIA CONTACT

301-975-2762

ORGANIZATIONS

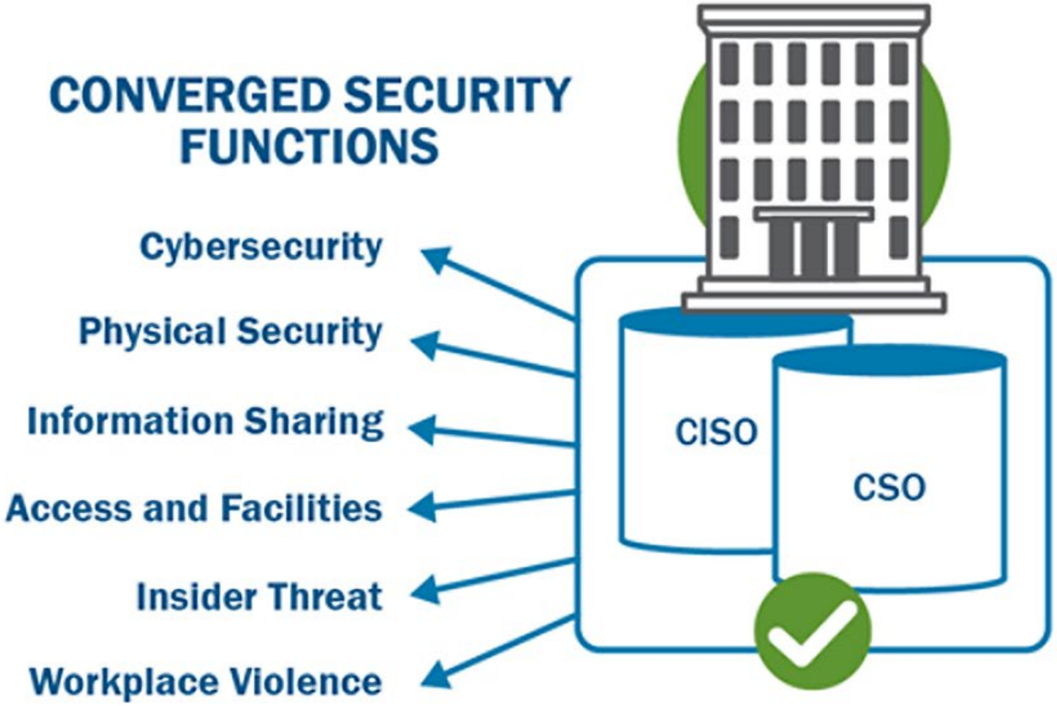
ENABLING THE CONVERGENCE

Linking Physical and Digital Identity

Multi-purpose Credential

PIV, FIDO, LEAF, NFC

Considered a **Superior** Identity Evidence

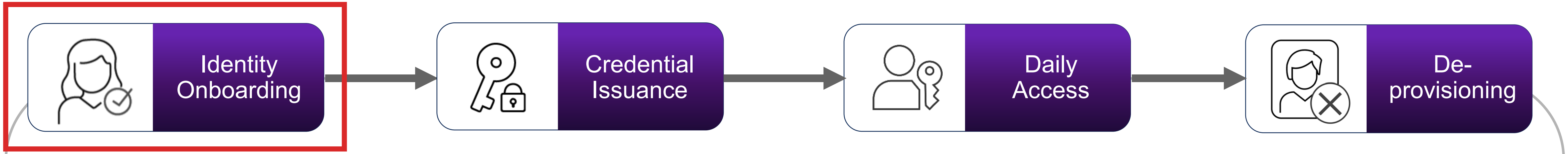


CONVERGED SECURITY FUNCTIONS

- Cybersecurity
- Physical Security
- Information Sharing
- Access and Facilities
- Insider Threat
- Workplace Violence

- ✓ Integrated security functions address cyber-physical infrastructure security.
- ✓ Holistic threat management ensures physical and cyber assets are secure.
- ✓ Senior leaders and teams communicate, coordinate, and collaborate.
- ✓ Organization is prepared to prevent, mitigate, and respond to threats.

SMART CREDENTIALS LIFECYCLE



- **Identity Verification**
- **Doc Auth**
- **Biometric Verification**
- IAL2 or IAL3
- Government issued digital credentials (ex: mDL)

- Smart Card / Badge Issuance
- Self-Service PIV Enrollment
- Passkey Enrollment (On-Device)

- Entitlements
- Physical Access Policy
- Logical Access Policy
- Risk / Threat Oriented Policies
- Account Recovery

- PIV Revocation
- Physical Access Revocation
- Passkey Revocation

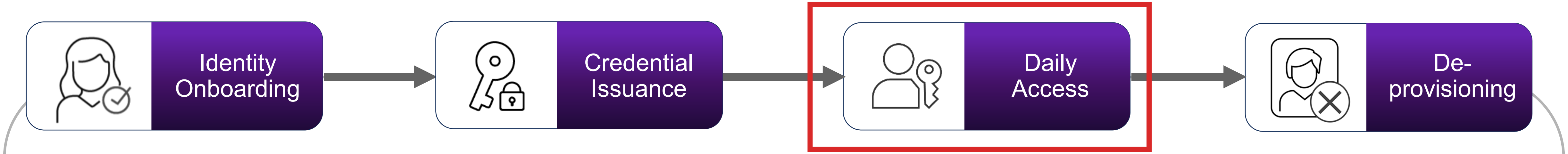
STRENGTH OF IDENTITY EVIDENCE (NIST SP 800-63)

SUPERIOR	- The issuing source of the evidence confirmed the claimed identity by following written procedures designed to enable it to have high confidence that the source knows the real-life identity of the subject. Such procedures are subject to recurring oversight by regulatory or publicly accountable institutions. - The issuing source visually identified the applicant and performed further checks to confirm the existence of that person. - The issuing process for the evidence ensured that it was delivered into the possession of the person to whom it relates. - The evidence contains at least one reference number that uniquely identifies the person to whom it relates. - The full name on the evidence must be the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names. - The evidence contains a photograph of the person to whom it relates. **- The evidence contains a biometric template (of any modality) of the person to whom it relates.** **- The evidence includes digital information, the information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the issuing source to be confirmed.** **- The evidence includes physical security features that require proprietary knowledge and proprietary technologies to be able to reproduce it.** - The evidence is unexpired.

VALIDATING IDENTITY EVIDENCE (NIST SP 800-63)

Strength	Method(s) performed by the CSP
Strong	- The evidence has been confirmed as genuine: - using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified. **OR** - by trained personnel and appropriate technologies, confirming the integrity of the physical security features and that the evidence is not fraudulent or inappropriately modified. **OR** - by confirmation of the integrity of cryptographic security features. - All personal details and evidence details have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).
Superior	**- The evidence has been confirmed as genuine by trained personnel and appropriate technologies including the integrity of any physical and cryptographic security features.** **- All personal details and evidence details from the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).**

SMART CREDENTIALS LIFECYCLE



Identity Onboarding

- Identity Verification
- Doc Auth
- Biometric Verification
- IAL2 or IAL3
- Government issued digital credentials (ex: mDL)

Credential Issuance

- Smart Card / Badge Issuance
- Self-Service PIV Enrollment
- Passkey Enrollment (On-Device)

Daily Access

- Entitlements
- Physical Access Policy
- Logical Access Policy
- Risk / Threat Oriented Policies
- **Account Recovery**

De-provisioning

- PIV Revocation
- Physical Access Revocation
- Passkey Revocation

A NEW CHALLENGE: CRYPTOAGILITY

QUANTUM-SAFE ALGORITHMS ARE YOUNG

For the next 10-15 years…

- Vulnerabilities may appear with extensive real-world deployment
- Some algorithms could prove less secure than anticipated
- Standards will be evolving

CRYPTOAGILITY

As soon as a vulnerability is discovered

- Algorithms must be updated
- Including physical credentials and devices

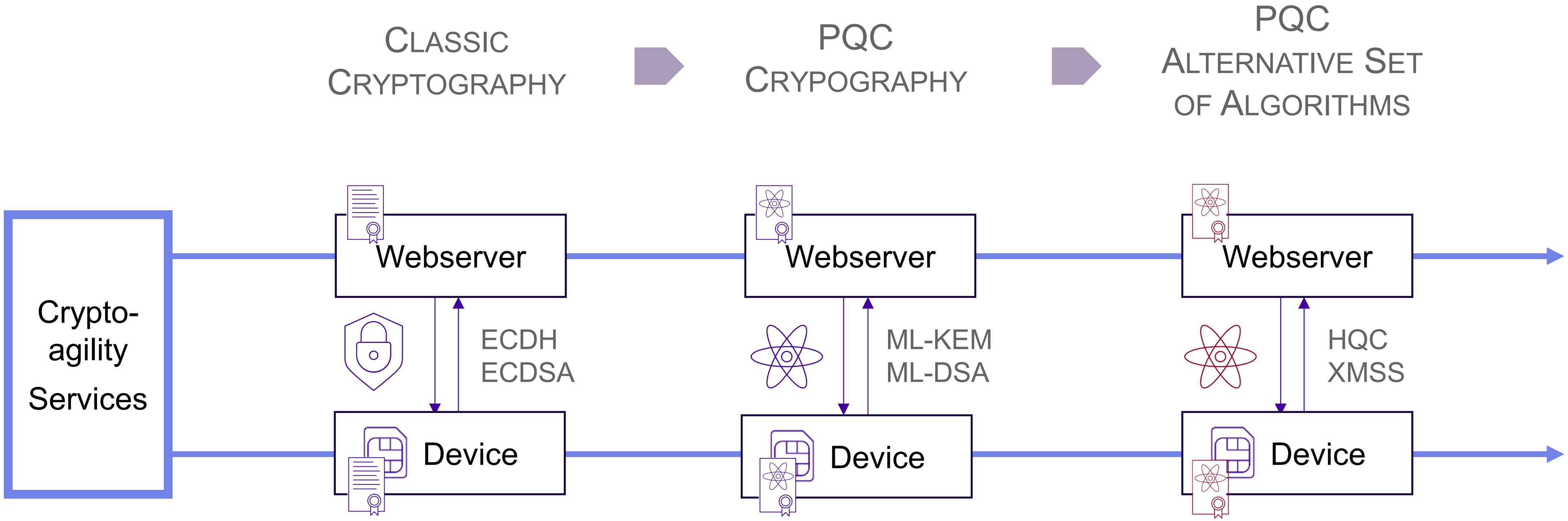
If there is a need to change algorithm

- Decouple encryption algorithms from workflows
- Protocols need to be changed everywhere <u>at the same time</u>
- Credentials must be reissued

IDEMIA
PUBLIC SECURITY

CRYPTO AGILITY FOR PHYSICAL DEVICES

Secure Communication and Authentication Using Cryptographic Modules



ROADMAP OBJECTIVES

Strengthened Posture

- Gen-AI-resilient employee on-boarding
- Eliminate passwords and legacy MFA from Desktop to Cloud
- End-point security x Identity Access Management
- Adaptive authentication continuously monitoring for increased risks

Simplified Experience

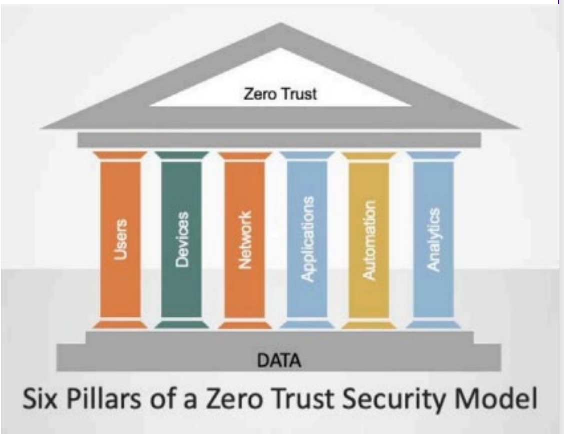
- Consistent and frictionless user experience
- Eliminate costly password resets
- Choice of hardware and software solutions with centralized management

Business Acceleration

- Accelerate business transformation by eliminating identity silos
- Smart ID as an “Anchor Credential”
- Account Recovery
- New Device Enrollment
- Re-verification
- Business Resilience with Cryptoagility

ROADMAP CONSIDERATIONS

- Interoperable: leverages industry standards
- Livessness detection
- Identity Verification enablement
- Phishing-Resistant MFA



Six Pillars of a Zero Trust Security Model

- Converged security: complete solution for physical and logical access control
- Zero trust Implementation

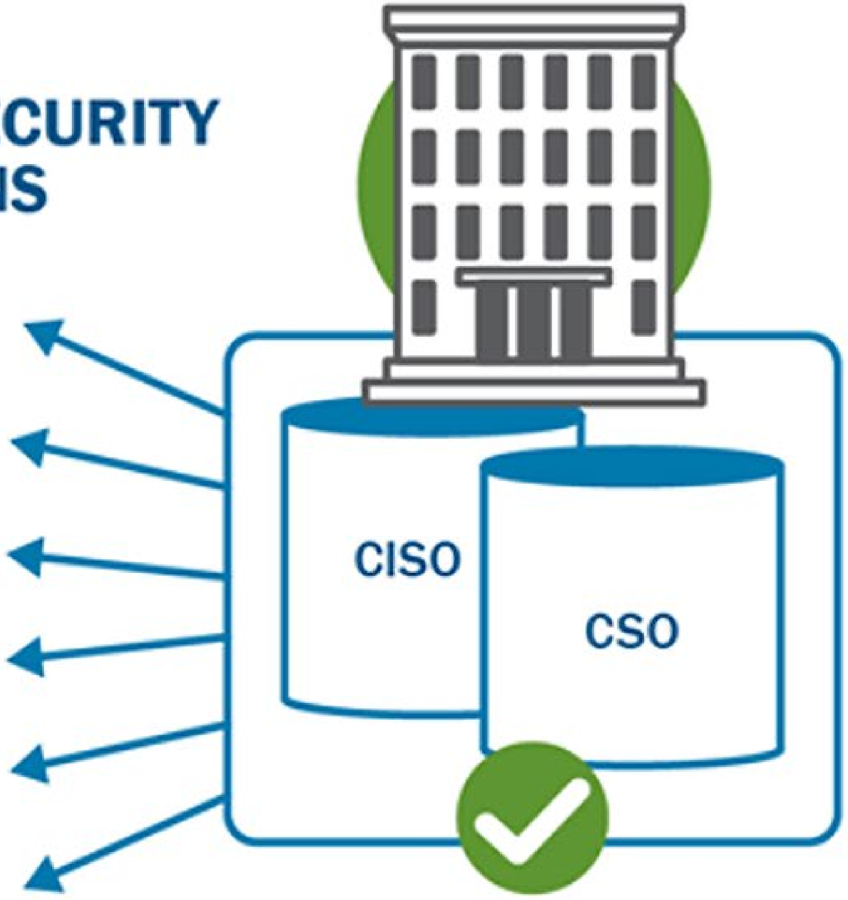
- Diverse form factors
- User choice
- Mobile & digital

QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

- Establish a PQ Readiness Roadmap
- Prepare a Cryptographic Inventory
- Engage your Cryptography Vendors on PQC
- Supply Chain Quantum Readiness

CONVERGED SECURITY FUNCTIONS

- Cybersecurity
- Physical Security
- Information Sharing
- Access and Facilities
- Insider Threat
- Workplace Violence



- ✓ Integrated security functions address cyber-physical infrastructure security.
- ✓ Holistic threat management ensures physical and cyber assets are secure.
- ✓ Senior leaders and teams communicate, coordinate, and collaborate.
- ✓ Organization is prepared to prevent, mitigate, and respond to threats.

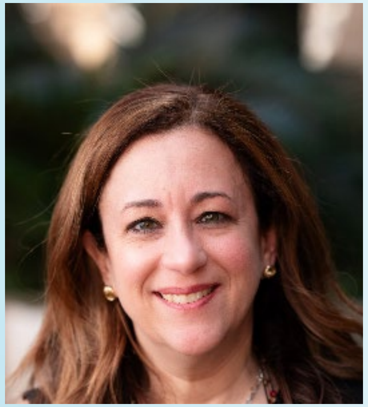
IDEMIA
PUBLIC SECURITY

CONTACT

Teresa Wu
Vice President, Smart Credentials & Access

Teresa.Wu@us.idemia.com

Challenges in Identity Verification



Frances Zelazny
Anonybit

David Kelts
DecipherID

Karan Puri
TD Bank

The Dark Side of Generative AI

Challenges for Identity Verification

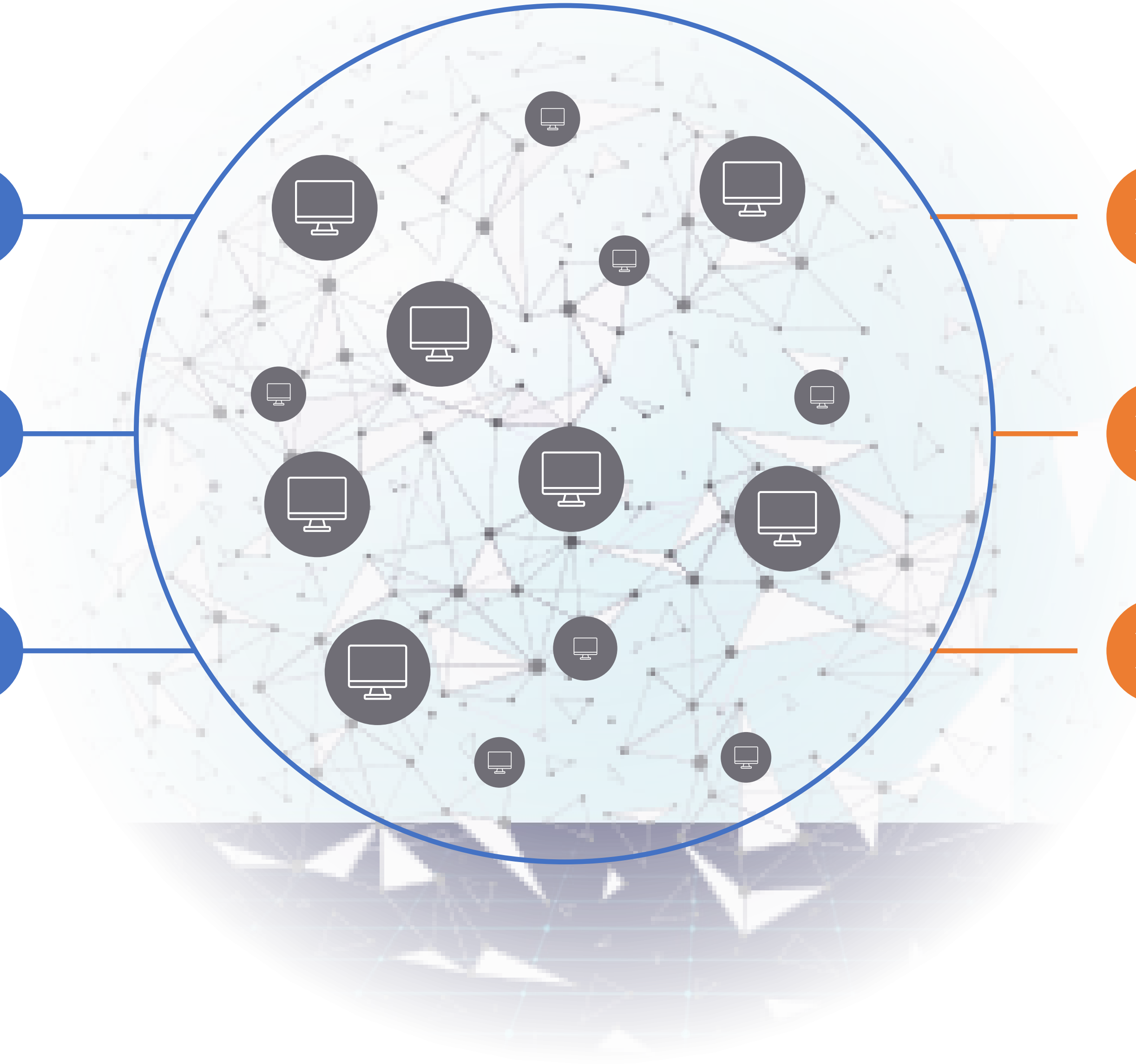
Frances Zelazny

The Future is Here and AI is Challenging Societal Assumptions

Artists embracing cloning and charging royalties for use of their voice

Companies like HourOne allow people to develop avatars for sales, product marketing, etc.

Potential to be a societal equalizer



1000:1 gap in papers on AI resource development v AI safety

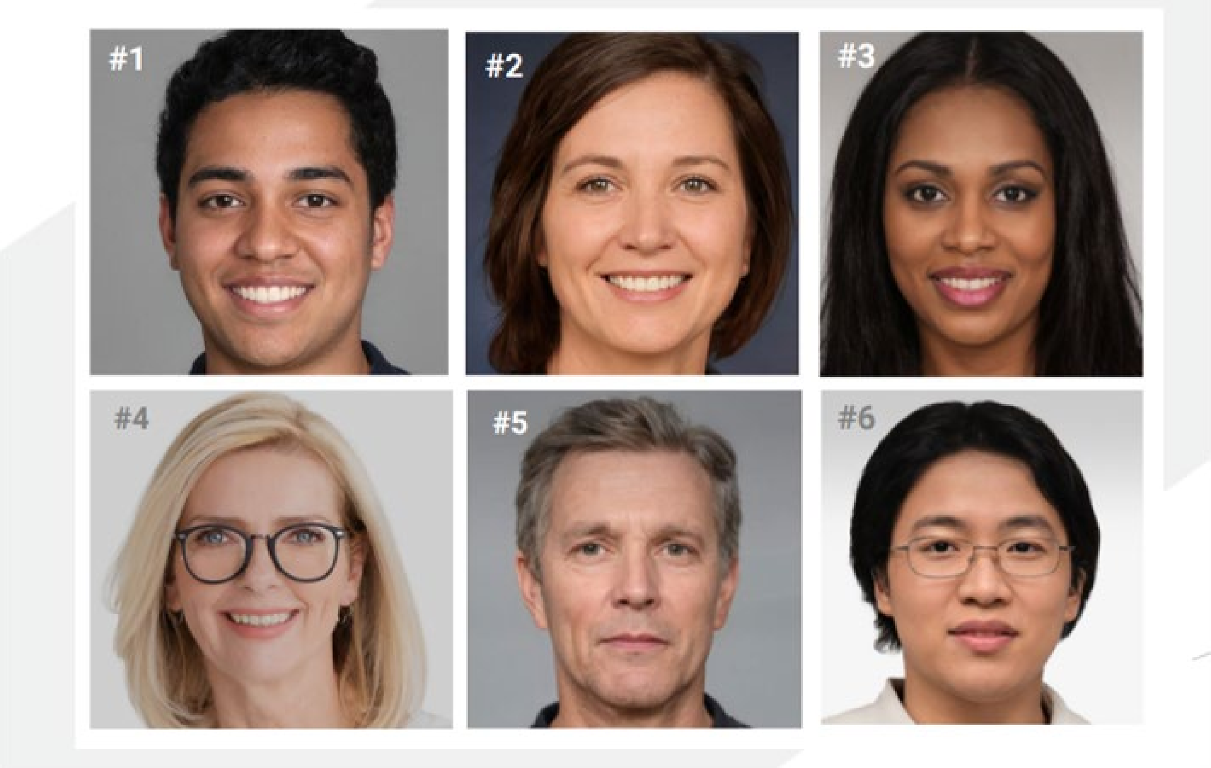
Same AI model that can give every child a biology lesson can give any terrorist a bioweapon lesson

Cyberterrorists selling AI-powered tools for $9.99/mo to enable audio clips that are tied to ransom demands.

Fact or Fiction: AI Generated Fraud

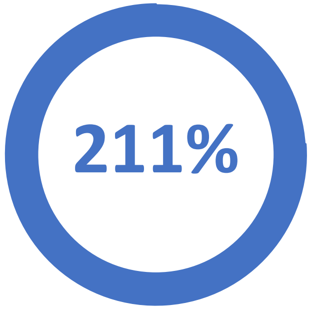
Can you spot the fakes?

Here are six headshots created with generative AI tools. Five are fake. One is real.
Can you figure it out?



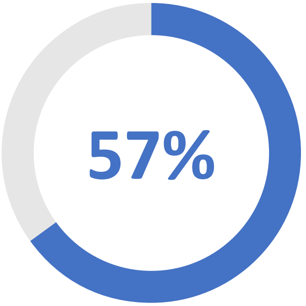
Source: AuthenticID

Even before this really takes off, we are in a fraud crisis.



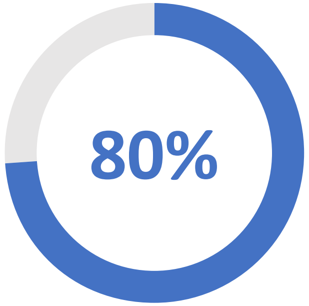
increase in victims who received breach notices

ITRC
IDENTITY THEFT RESOURCE CENTER



lost more than $500K in direct fraud

ALLOY



security incidents due to phishing

CSO

$13B

in account takeover fraud losses in 2023

AARP

$50M

lost in SIM swap attacks in 2023

FBI

The root of all fraud boils down to compromised credentials

Personal data is stored inside central honeypots that are impossible to protect

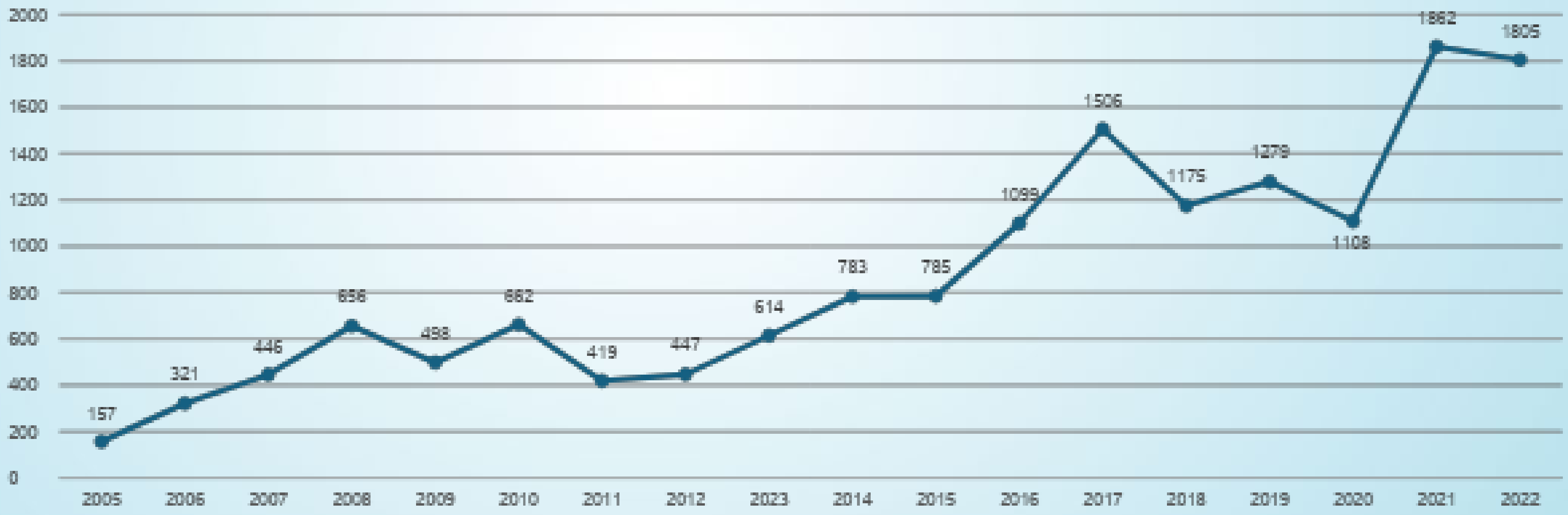
Biometric data collected in account origination is not stored because of privacy concerns

Stolen data is sold on the dark web and used for authentication

Siloed organizational processes create blind spots that attackers exploit

Many enterprises **already collect biometrics** during account origination but **don't store them for fear of data compromises**

Number of Data Compromises



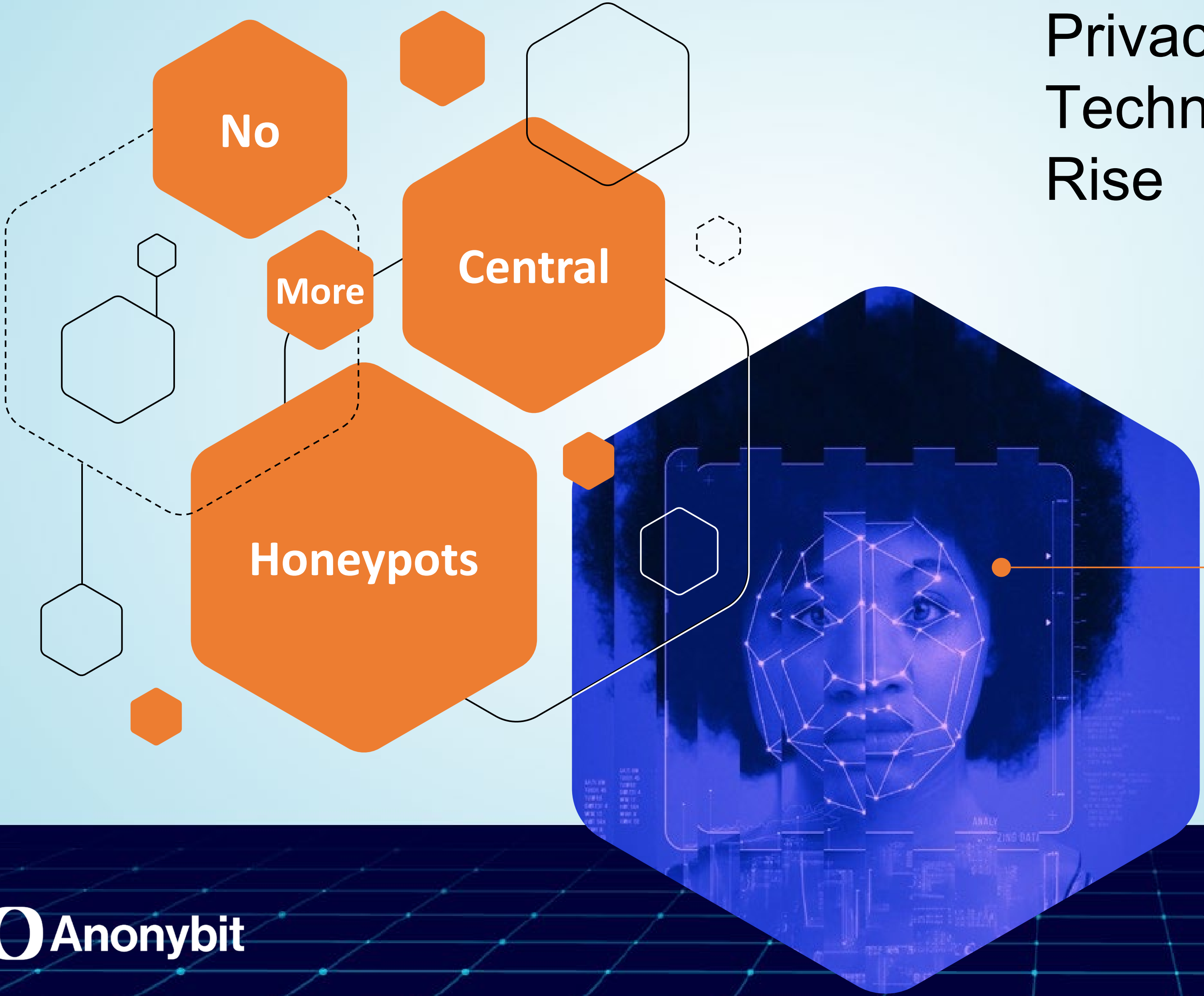
Sources: Statistica 2023, Identity Theft Resource Center, Socure

5 Steps to Combating the Risks of AI Generated Identity Theft

- **Eliminate central honeypots of personal data**
- **Use consistent biometrics across the user journey**
- Use liveness detection
- **Apply injection detection techniques**
- Augment biometric authentication mechanisms with dynamic fraud detection

Anonybit

Privacy-Enhancing Technologies (PETs) on the Rise



Approaches:

Tokenization

Homomorphic Encryption

Secure Multi Party Computation

Zero Knowledge Proofs

Considerations:

Use cases to support (1:1 v 1:N)

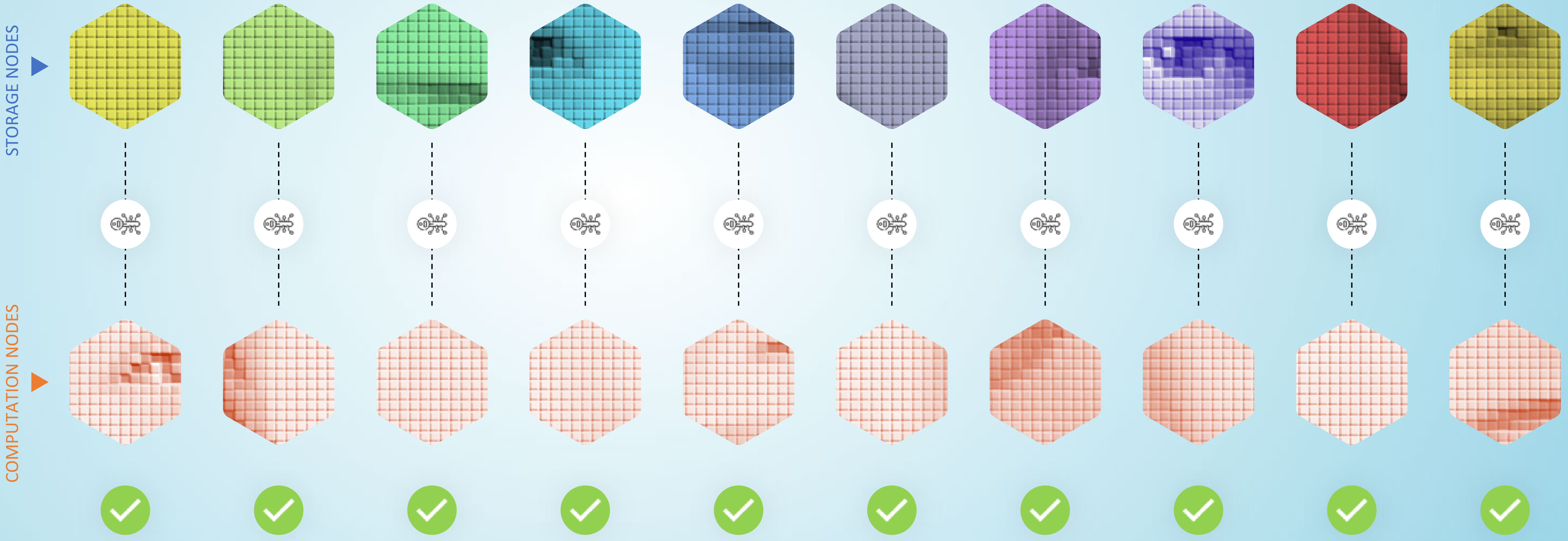
Audit and adjudication needs

Vendor lock in

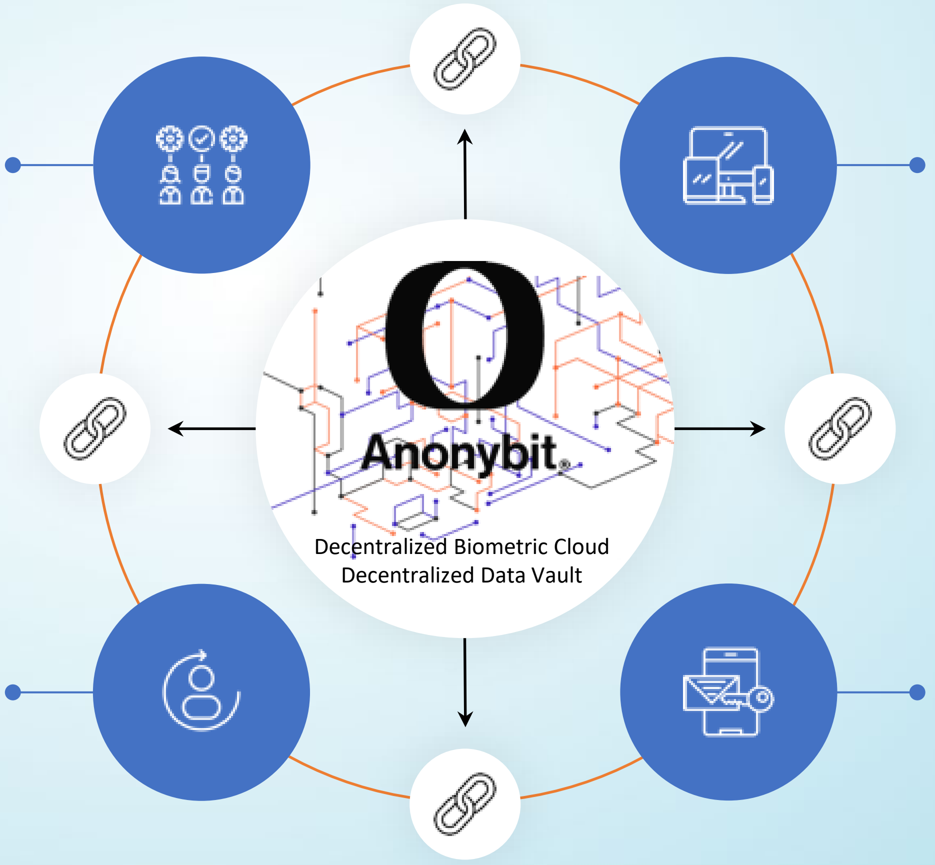
Biometric performance

Key/token management

Anonybit’s Patented Approach Leverages SMPC and ZKP



The result is a closed **circle of identity** without the gaps that attackers exploit



Digital Onboarding

Ingest biometrics and run a 1:N check to prevent duplicates, blocked identities

Binding

Once uniqueness is established, the biometric is enrolled and bound to a device/token/email or other attribute

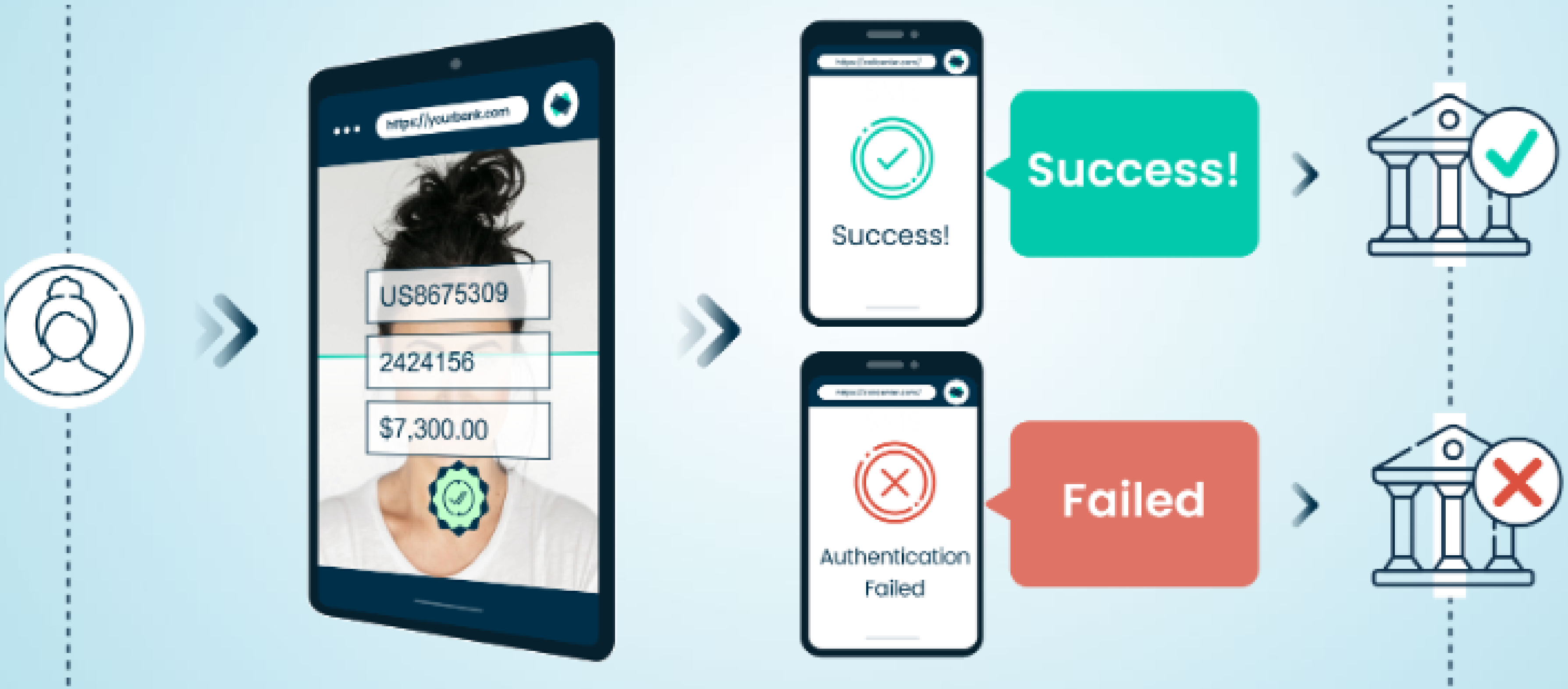
Account Recovery

Once the biometric is validated, the token or account can be reset

Authentication

Anonybit is invoked for biometric MFA across service channels/devices with no reliance on KBAs, OTPs, passwords

Combining injection detection with biometric authentication



- Ensure that the verified and authorized user is the one transacting
- Ensure that the data entered by the user is the same as what the bank has received and has not been manipulated

Source: IronVest

Anonybit

THANK YOU

Frances Zelazny
Co-Founder & CEO
frances@anonybit.io

The Experience of Identity Verification (IDV)

As it relates to provisioning a Mobile Driver’s License Accurately.

David Kelts, 2025-Feb-24

Momentum in Government Online, Digital & Mobile ID

Spots of high activity around the world and beginning to converge into global coverage

2.09 billion

people globally have a Digital Identity or Digital ID

99.4%

of all Swedish Citizens between the ages of **18-67** have a Bank ID that they use for government services

85m of 115m

people in the Philippines have ePhil ID

46%

of the **US population** lives in a state with a live mobile driver's license (**mDL**)

The **European Union** plans for **multiple wallets** and **requires** initial deployments by **2026**

1.3 billion

people covered by Aadhar in India

97%

of organizations experience **challenges** with identity verification using **physical documents** including AI generated fakes

7 States

Australia Fed Initiative deploying mDL & mID in all 7 States starting 2024

NSW: 6M drivers already installed app

Sources:
https://www.bankid.com/en/om-oss/statistic;
https://www.biometricupdate.com/;
https://hub.pingidentity.com/2024-it-pro-survey/ai-and-identity-fraud-protection-take-priority;
Trinisic.ID downloadable Digital ID Adoption Report: https://trinsic.id/adoption-report/
http://www.mdlconnection.com
Matica Technologies Group, S.A.

Who gets an ID or DL?

The universe of people who will register for mDL is larger than the set of people who get a bank account, rent a scooter, take carshare, drive carshare, rent apts.

What will happen if we don’t onboard the right person?

Adoption and trust in Mobile IDs & mDLs depends on the accuracy of onboarding at scale… **global** scale inclusive of everybody

Is remote IDV more accurate than US Postal Service delivery?

Onboarding as a Service

“Ripping IDs”

What could possibly go wrong?

Document Capture & Auth

- Steady hands for Photo of ID?
- High-Res Capture?
- Contrast for Edge-detection?
- Detect specific security features?
- UV and IR Security Features?
- Barcode generated fake data?
- AI generated Fake ID Card?
- Cropping small, obscured, overlaid face from that small captured image of the document

Face Capture for Match

- Duck Lips
- Huge Smiles on Source or Selfie?
- Angled, Distorted Selfies?
- Variable camera resolutions
- Even lighting on facial features?
- Masks, videos, sleeping people?
- AI Generated Synthetic IDs?

- And then the COST!

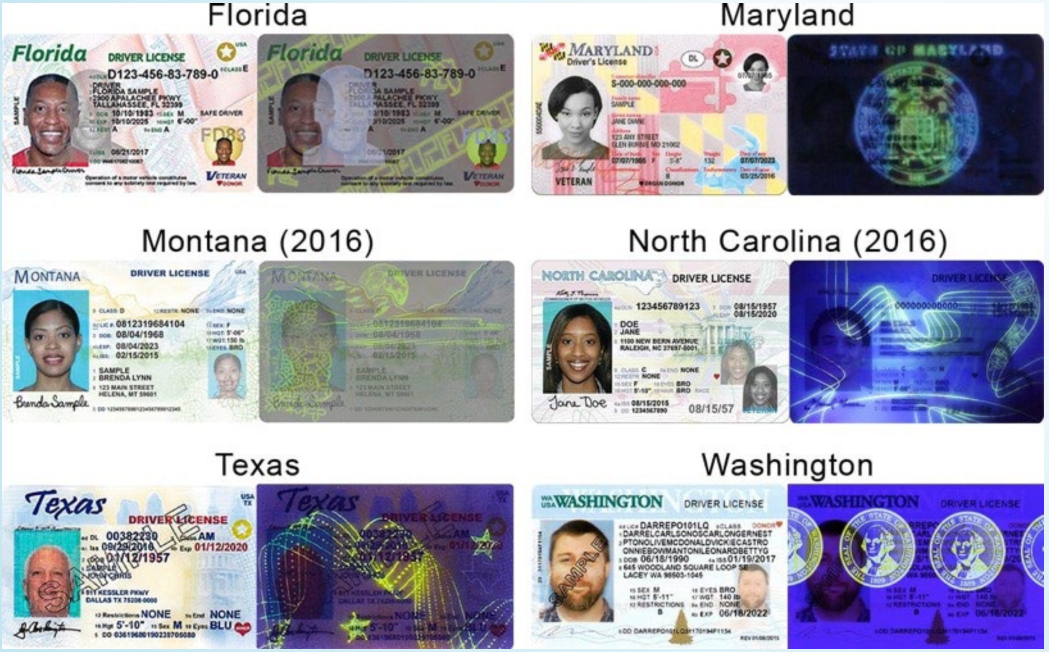
https://medium.com/@dkelts.id/ripping-ids-should-go-the-way-of-cds-49fec9206492

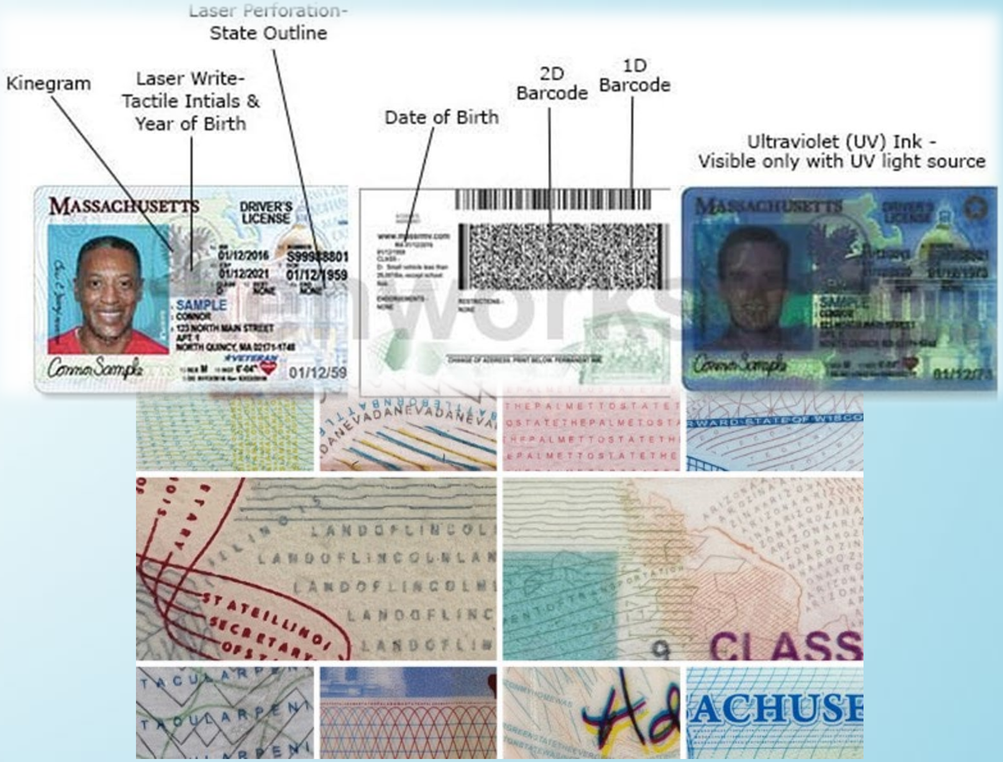
Card Capture & Document Authentication

Can we really expect a dark background? And a non-skewed capture?

We tend to consider it like this…

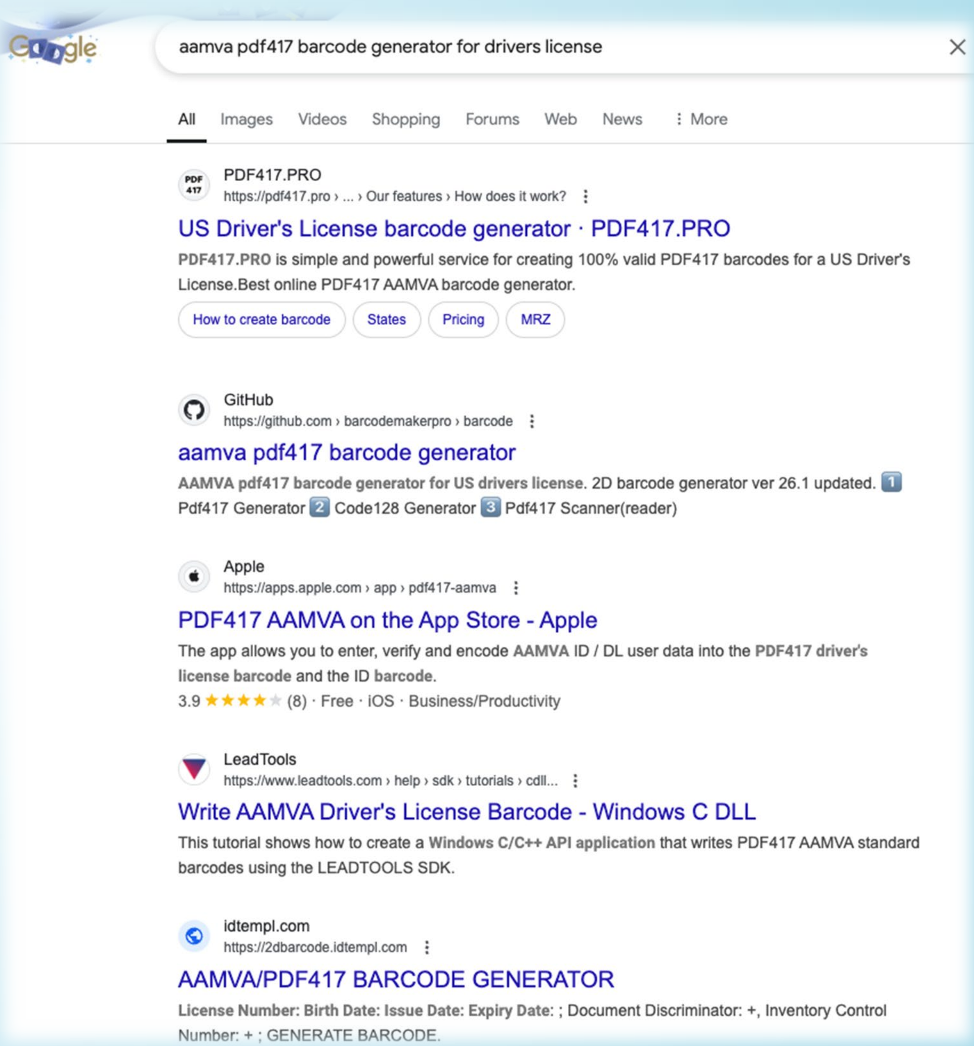
How many security features can we detect with the average phone camera?





Authenticity of Barcode Data

- Generate any data you want to lay over the existing barcode
  - Front/Back Comparison at the accuracy of OCR from beneath overlays and security line prints
- Every fake ID has a barcode that matches the front of card
  - Barcode anomaly detection as Auth
  - Digital signature in Jurisdiction specific fields (only one state)



aamva pdf417 barcode generator for drivers license

PDF417.PRO
https://pdf417.pro › ... › Our features › How does it work?

US Driver's License barcode generator · PDF417.PRO

PDF417.PRO is simple and powerful service for creating 100% valid PDF417 barcodes for a US Driver's License.Best online PDF417 AAMVA barcode generator.

GitHub
https://github.com › barcodemakerpro › barcode

aamva pdf417 barcode generator

AAMVA pdf417 barcode generator for US drivers license. 2D barcode generator ver 26.1 updated. 1️⃣ Pdf417 Generator 2️⃣ Code128 Generator 3️⃣ Pdf417 Scanner(reader)

Apple
https://apps.apple.com › app › pdf417-aamva

PDF417 AAMVA on the App Store - Apple

The app allows you to enter, verify and encode AAMVA ID / DL user data into the PDF417 driver's license barcode and the ID barcode.

3.9 ★★★★☆ (8) · Free · iOS · Business/Productivity

LeadTools
https://www.leadtools.com › help › sdk › tutorials › cdll...

Write AAMVA Driver's License Barcode - Windows C DLL

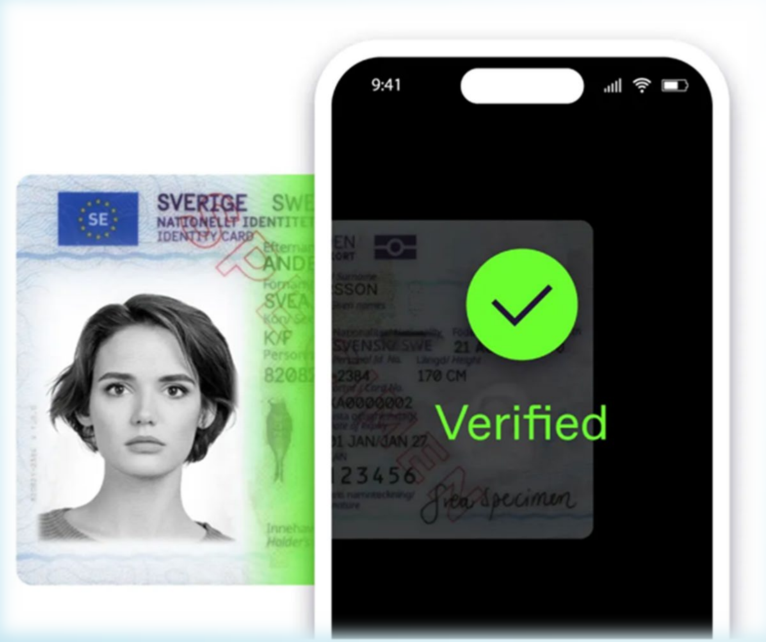
This tutorial shows how to create a Windows C/C++ API application that writes PDF417 AAMVA standard barcodes using the LEADTOOLS SDK.

idtempl.com
https://2dbarcode.idtempl.com

AAMVA/PDF417 BARCODE GENERATOR

License Number: Birth Date: Issue Date: Expiry Date: ; Document Discriminator: +, Inventory Control Number: + ; GENERATE BARCODE.

Do we have anything more accurate in the USA? Direct read from chip?



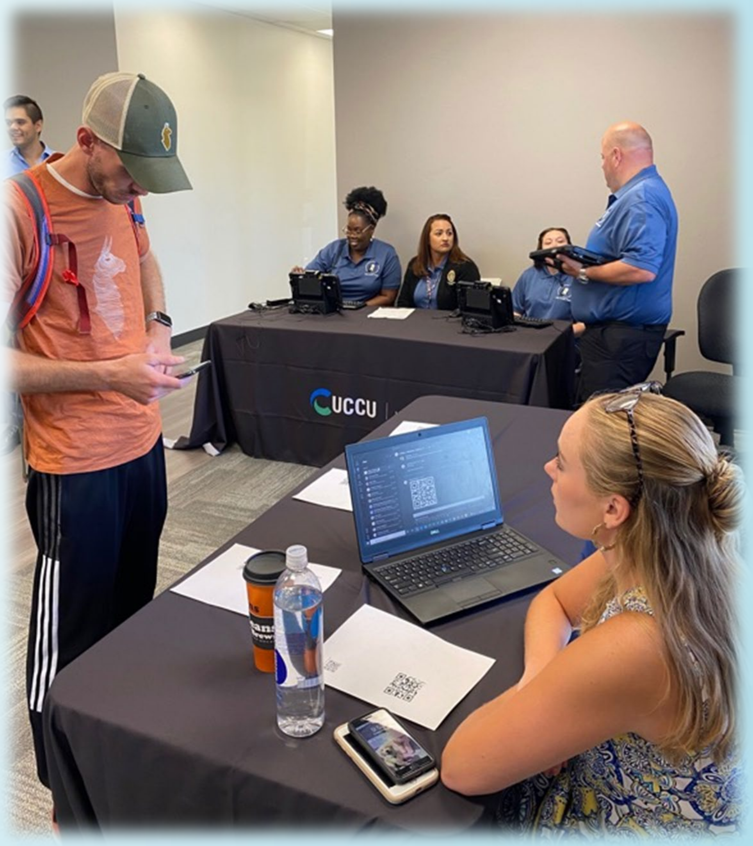
Face Capture

Liveness and Biometric face matching achieving the **expected** accuracy

How do people hold their phone to read instruction text?

- Bifocals and Progressive Lenses
  - Reading distance in lower portion
- Shielding from lit environments
- Comfortable arm positioning

- If we read instructions on a mobile app at all…

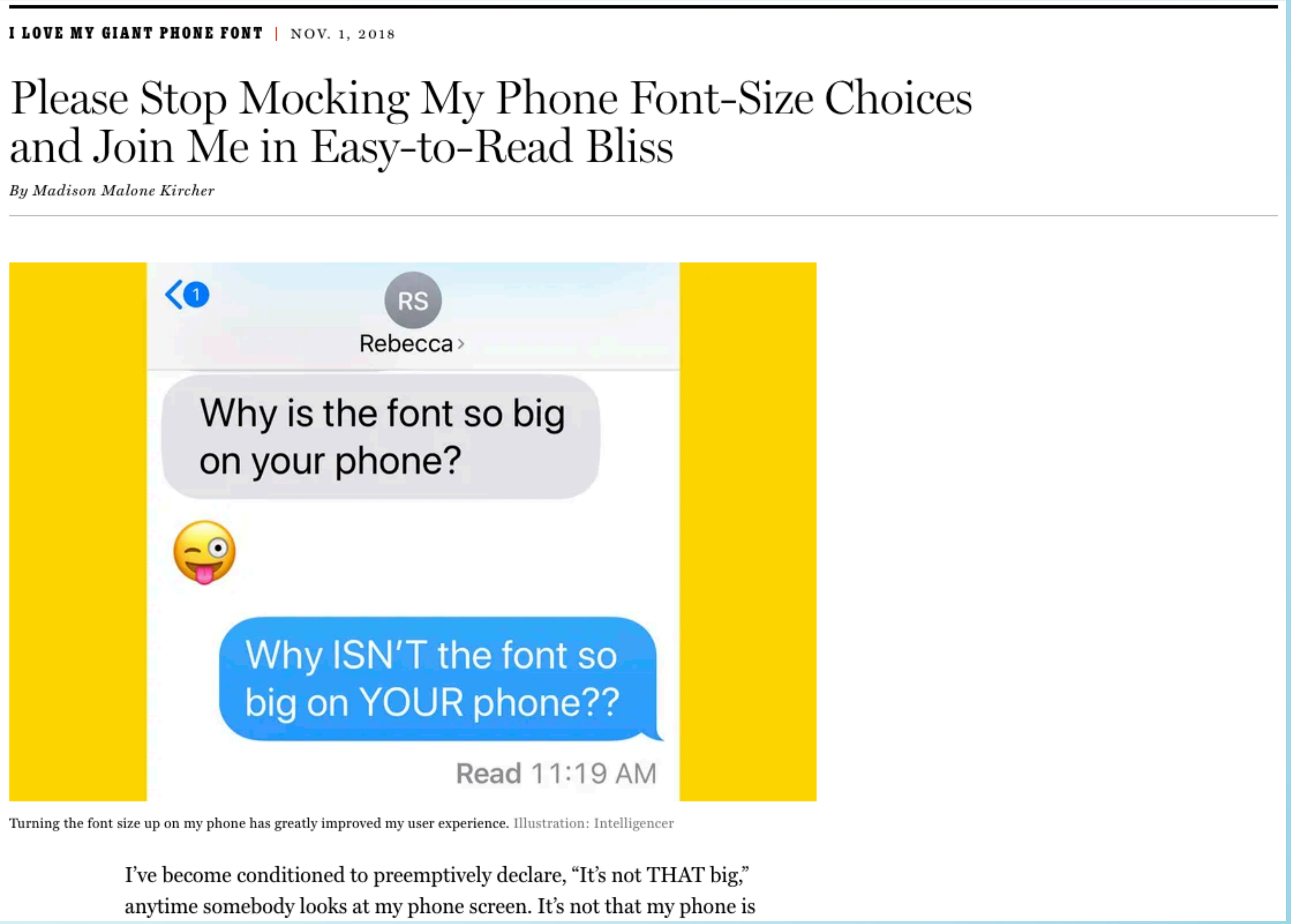


Font size defaults for vision or convenience

People set their font sizes LARGE

Are your instructions concise so that somebody could read them?

Are they in written language? Visual-only?



I LOVE MY GIANT PHONE FONT | NOV. 1, 2018

Please Stop Mocking My Phone Font-Size Choices and Join Me in Easy-to-Read Bliss

By Madison Malone Kircher

Why is the font so big on your phone?

😜

Why ISN'T the font so big on YOUR phone??

Read 11:19 AM

Turning the font size up on my phone has greatly improved my user experience. Illustration: Intelligencer

I've become conditioned to preemptively declare, "It's not THAT big," anytime somebody looks at my phone screen. It's not that my phone is

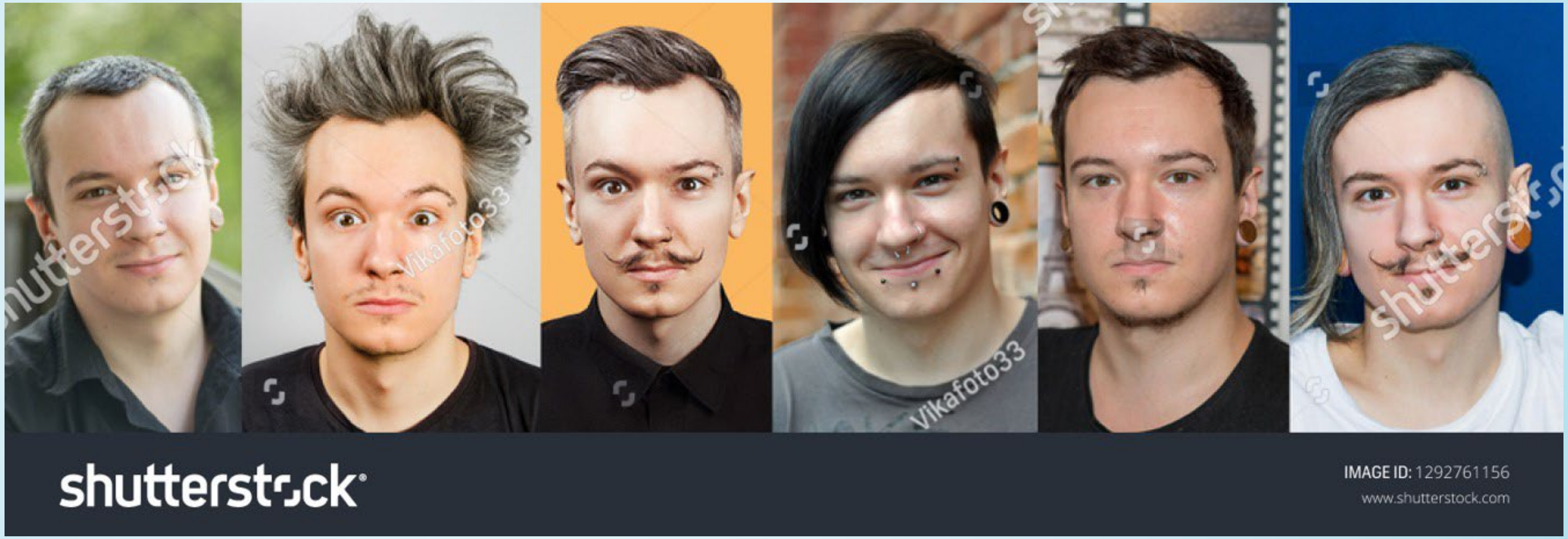
How do people take selfies?

And how do they want their picture to show on their physical card?

Where do people most often register for their Mobile Driver’s License?

How is the lighting on both sides of their face?

Social Engineering a Visual Face Match?

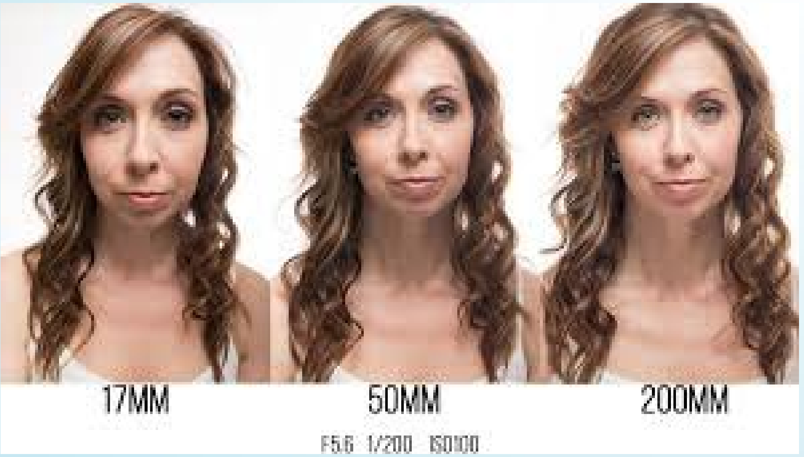


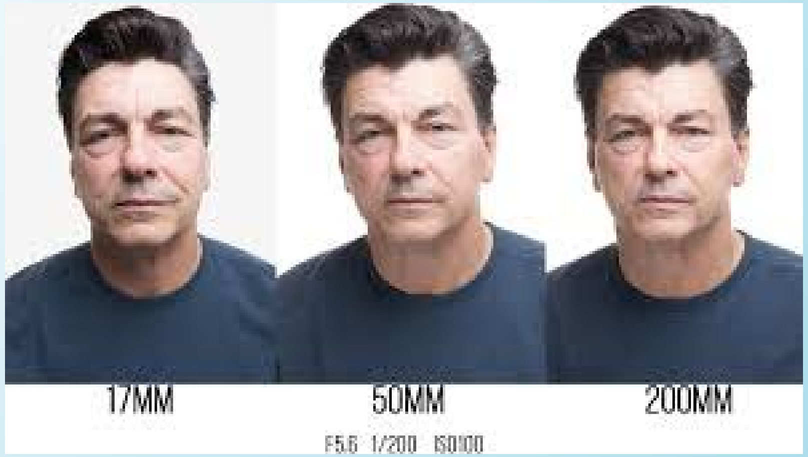
This is one way that fraudsters pass as someone else's identity for in-person transactions.

Lens or Barrel Distortion

If people in these photos had different clothes and hair, could you match them visually?

What changes in biometric measurements at different arm lengths?





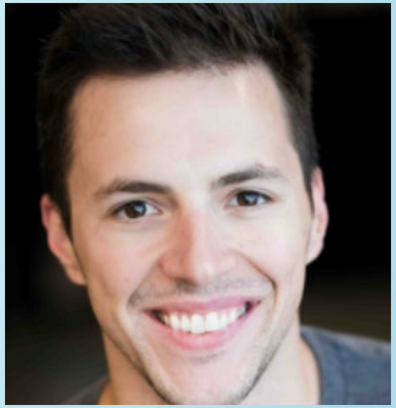
Cost

If Cardholders expect to pay nothing for their mDL, who is paying for the accuracy that we NEED to build trust in the mDL Ecosystem?

Solutions for Identity Verification

Moderator
David Kelts
DecipherID

Deepanker Saxena
Socure



Riley Hughes
Trinsic

Layered Defense against Identity Frauds

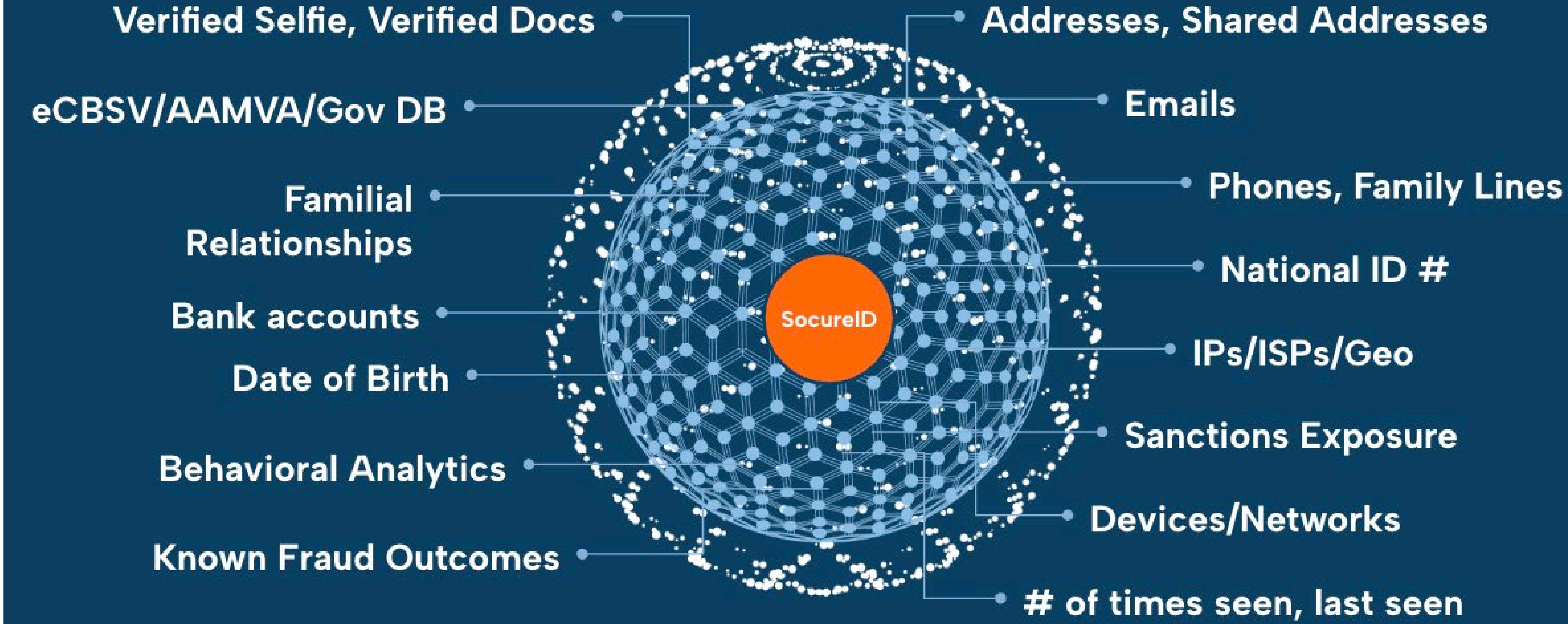
Deepanker Saxena
Socure

Our Vision

Socure will be the world's most accurate and inclusive risk and identity verification company

A developer-friendly AI platform for enterprises (and consumers) to verify, authenticate and manage identities and risk, anywhere in the world.

SocureID will be at the core of everything we do



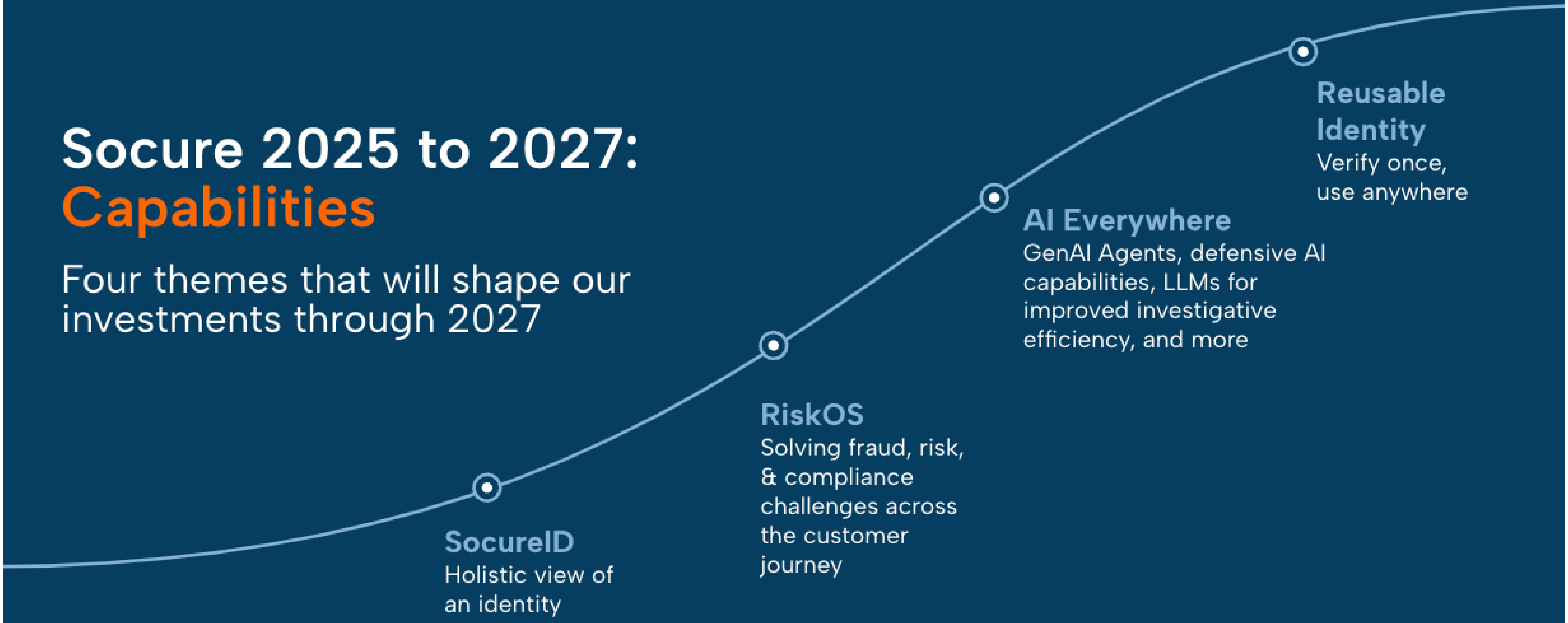
- Verified Selfie, Verified Docs
- eCBSV/AAMVA/Gov DB
- Familial Relationships
- Bank accounts
- Date of Birth
- Behavioral Analytics
- Known Fraud Outcomes
- Addresses, Shared Addresses
- Emails
- Phones, Family Lines
- National ID #
- IPs/ISPs/Geo
- Sanctions Exposure
- Devices/Networks
- # of times seen, last seen

And more!

Socure

Socure 2025 to 2027: Capabilities

Four themes that will shape our investments through 2027

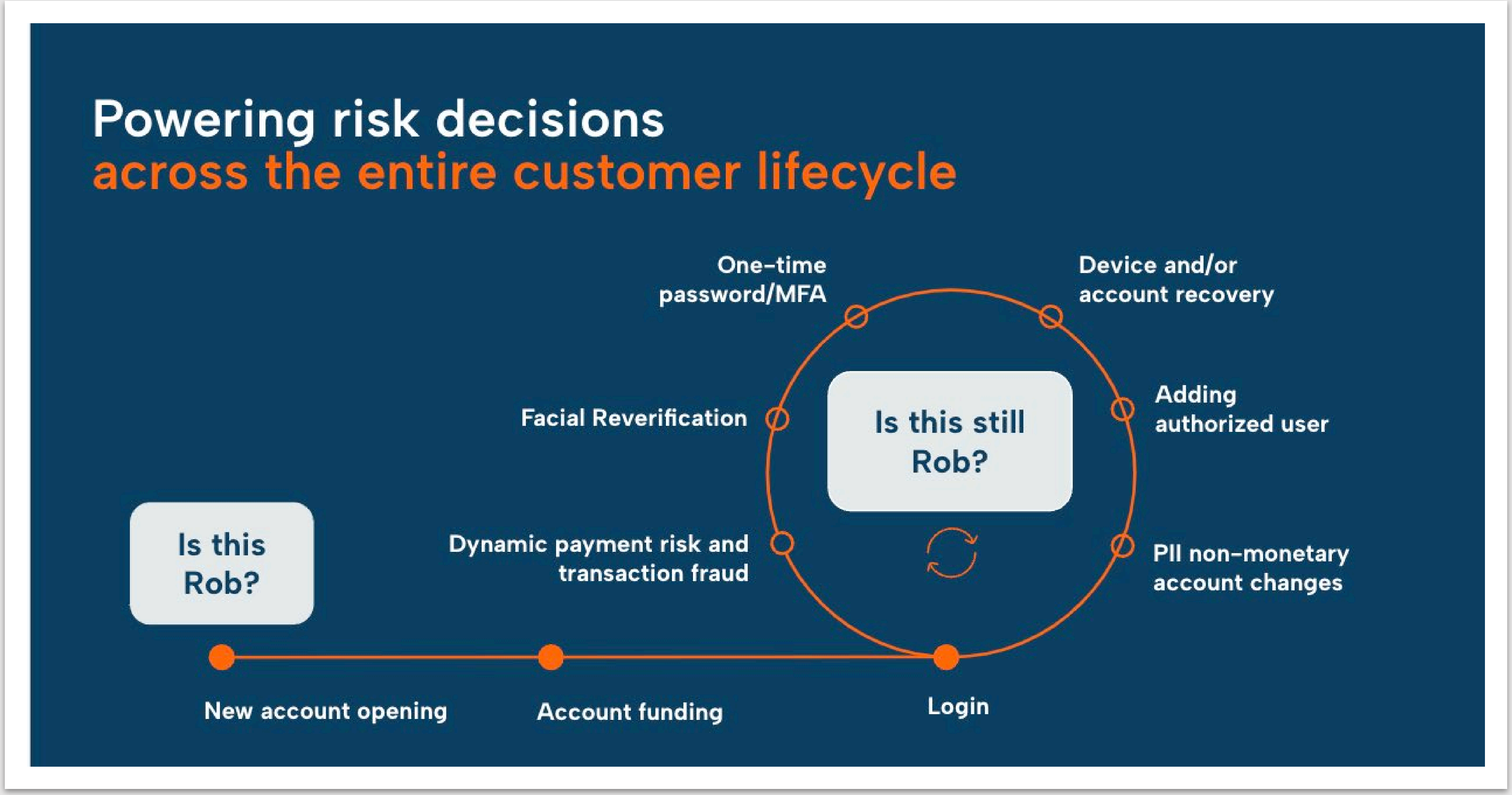


SocureID
Holistic view of an identity

RiskOS
Solving fraud, risk, & compliance challenges across the customer journey

AI Everywhere
GenAI Agents, defensive AI capabilities, LLMs for improved investigative efficiency, and more

Reusable Identity
Verify once, use anywhere



Powering risk decisions across the entire customer lifecycle

Is this Rob?

New account opening

Account funding

Login

Is this still Rob?

One-time password/MFA

Device and/or account recovery

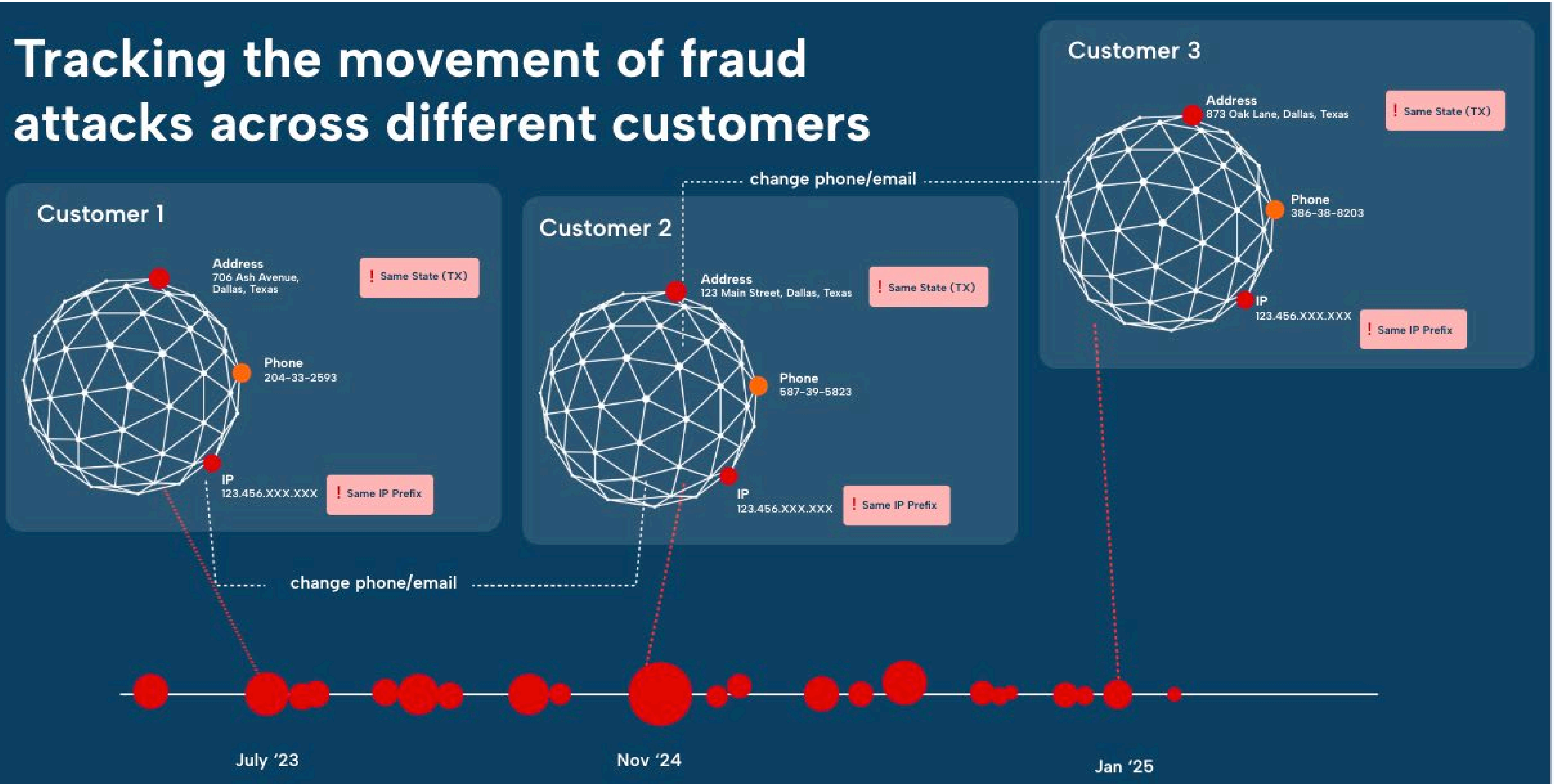
Facial Reverification

Adding authorized user

Dynamic payment risk and transaction fraud

PII non-monetary account changes

Tracking the movement of fraud attacks across different customers



Customer 1

Address
706 Ash Avenue,
Dallas, Texas

! Same State (TX)

Phone
204-33-2593

IP
123.456.XXX.XXX

! Same IP Prefix

change phone/email

Customer 2

Address
123 Main Street, Dallas, Texas

! Same State (TX)

Phone
587-39-5823

IP
123.456.XXX.XXX

! Same IP Prefix

change phone/email

Customer 3

Address
873 Oak Lane, Dallas, Texas

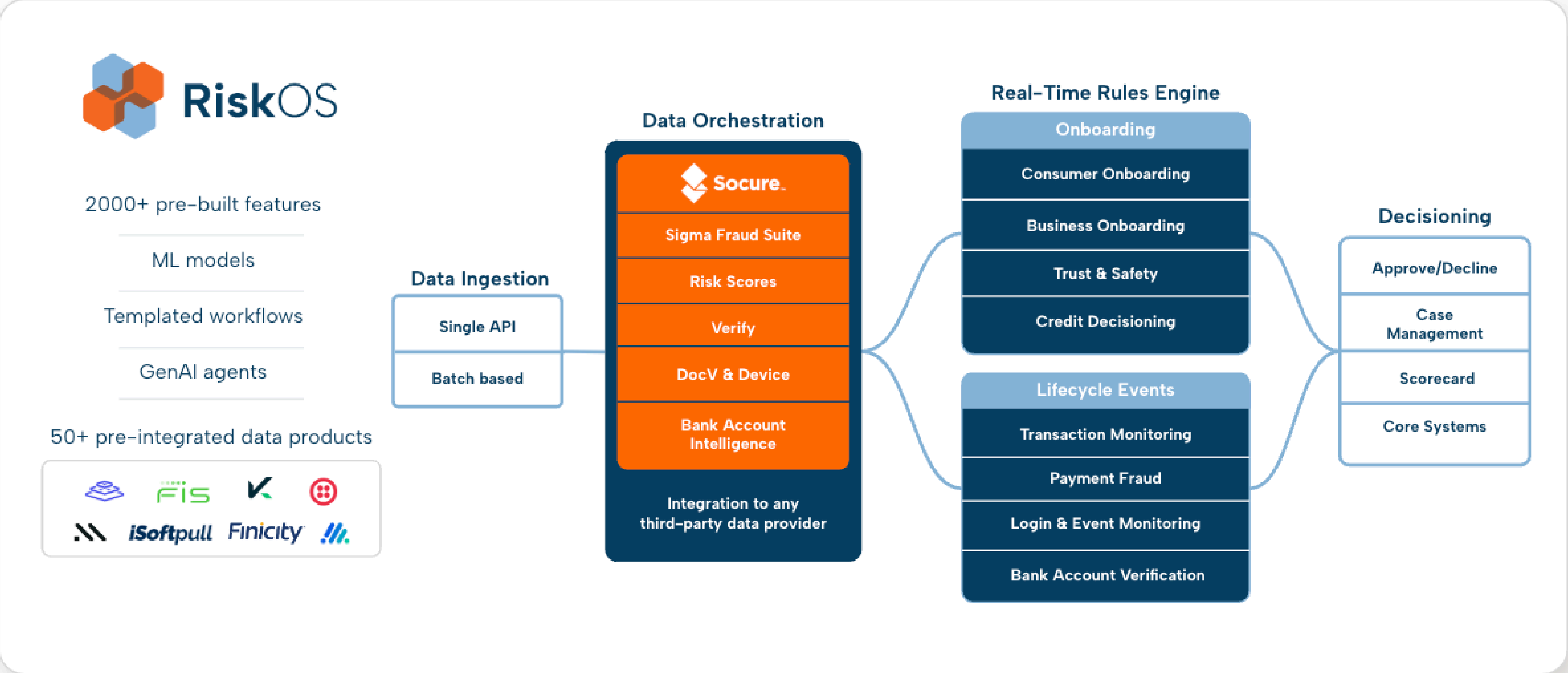
! Same State (TX)

Phone
386-38-8203

IP
123.456.XXX.XXX

! Same IP Prefix

RiskOS empowers organizations to build their own identity stack and tackle risk and trust challenges at every interaction



RiskOS

2000+ pre-built features

ML models

Templated workflows

GenAI agents

50+ pre-integrated data products

FIS iSoftpull Finicity

Data Ingestion

- Single API
- Batch based

Data Orchestration

- Socure.
- Sigma Fraud Suite
- Risk Scores
- Verify
- DocV & Device
- Bank Account Intelligence

Integration to any third-party data provider

Real-Time Rules Engine

Onboarding

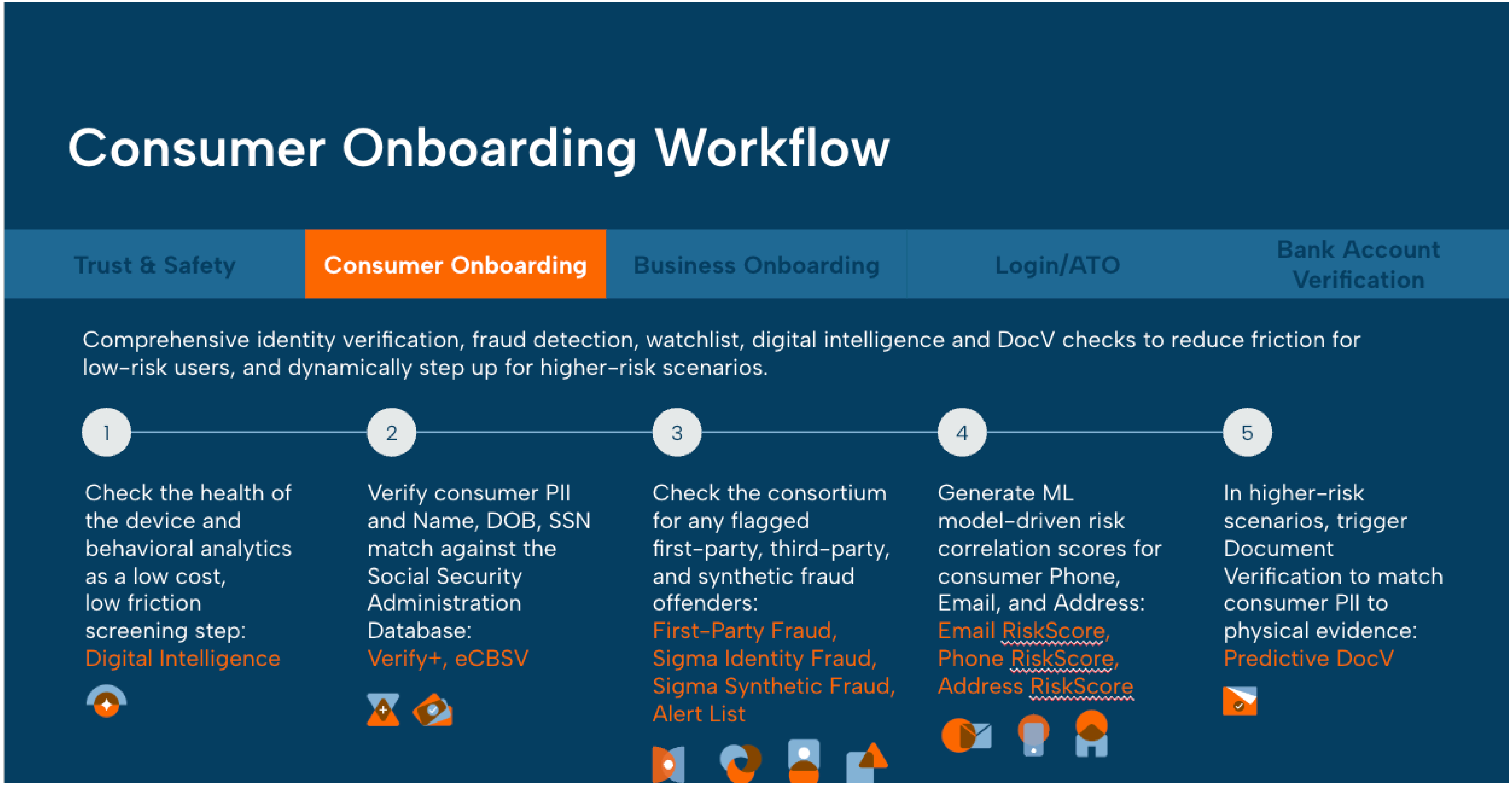
- Consumer Onboarding
- Business Onboarding
- Trust & Safety
- Credit Decisioning

Lifecycle Events

- Transaction Monitoring
- Payment Fraud
- Login & Event Monitoring
- Bank Account Verification

Decisioning

- Approve/Decline
- Case Management
- Scorecard
- Core Systems



Consumer Onboarding Workflow

Trust & Safety | **Consumer Onboarding** | Business Onboarding | Login/ATO | Bank Account Verification

Comprehensive identity verification, fraud detection, watchlist, digital intelligence and DocV checks to reduce friction for low-risk users, and dynamically step up for higher-risk scenarios.

1. Check the health of the device and behavioral analytics as a low cost, low friction screening step: Digital Intelligence

2. Verify consumer PII and Name, DOB, SSN match against the Social Security Administration Database: Verify+, eCBSV

3. Check the consortium for any flagged first-party, third-party, and synthetic fraud offenders: First-Party Fraud, Sigma Identity Fraud, Sigma Synthetic Fraud, Alert List

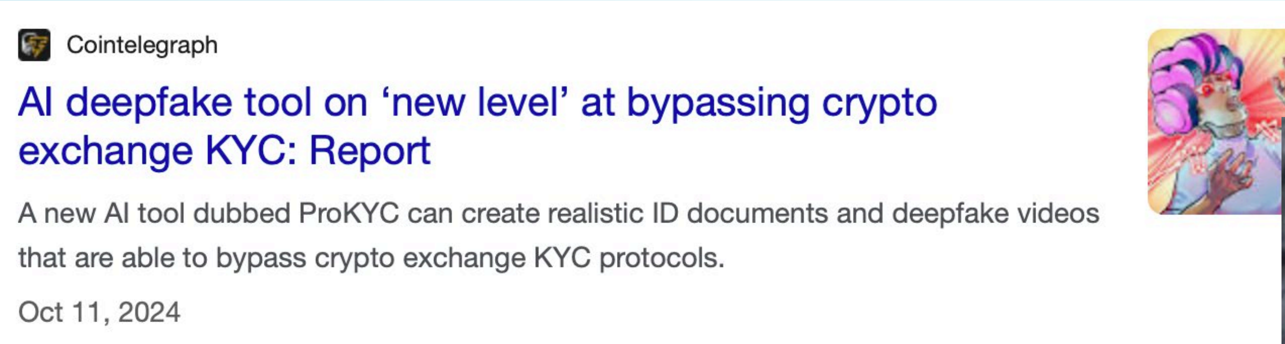
4. Generate ML model-driven risk correlation scores for consumer Phone, Email, and Address: Email RiskScore, Phone RiskScore, Address RiskScore

5. In higher-risk scenarios, trigger Document Verification to match consumer PII to physical evidence: Predictive DocV

Solutions for IDV

Riley Hughes, co-founder and CEO of Trinsic

trinsic

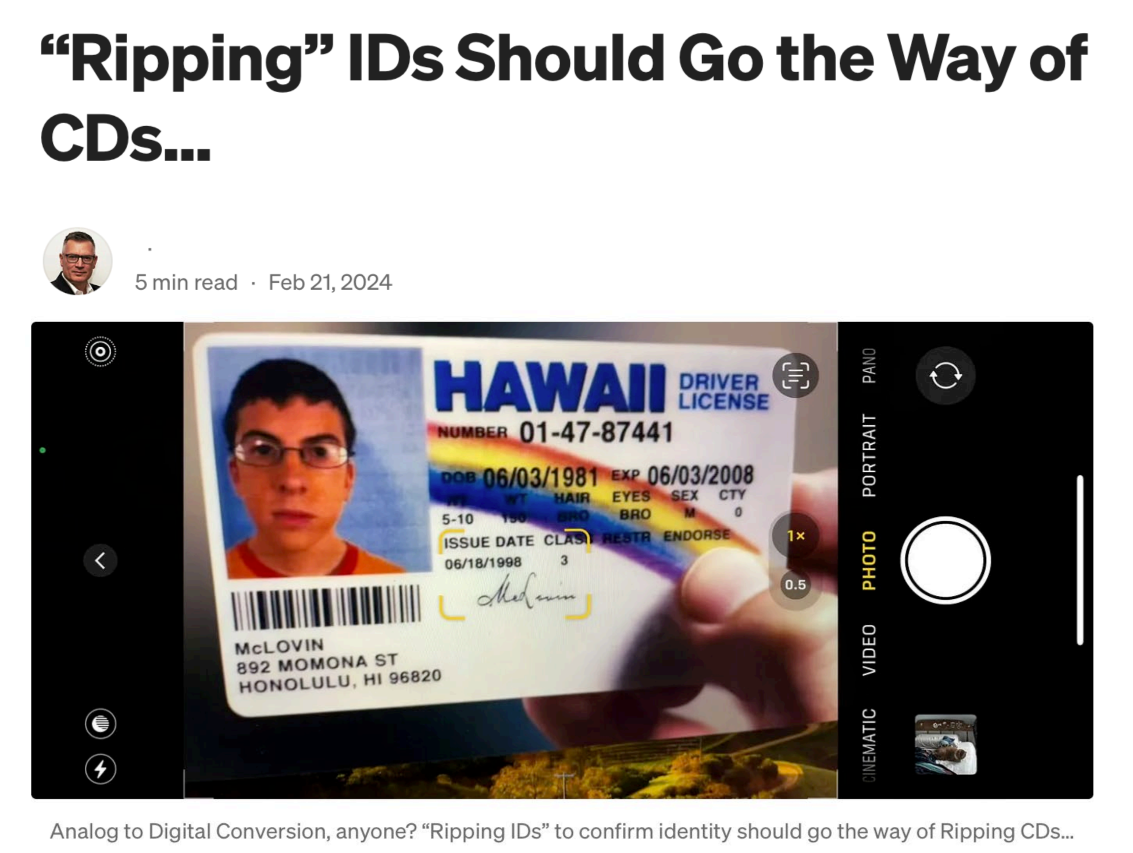


Cointelegraph

AI deepfake tool on ‘new level’ at bypassing crypto exchange KYC: Report

A new AI tool dubbed ProKYC can create realistic ID documents and deepfake videos that are able to bypass crypto exchange KYC protocols.

Oct 11, 2024

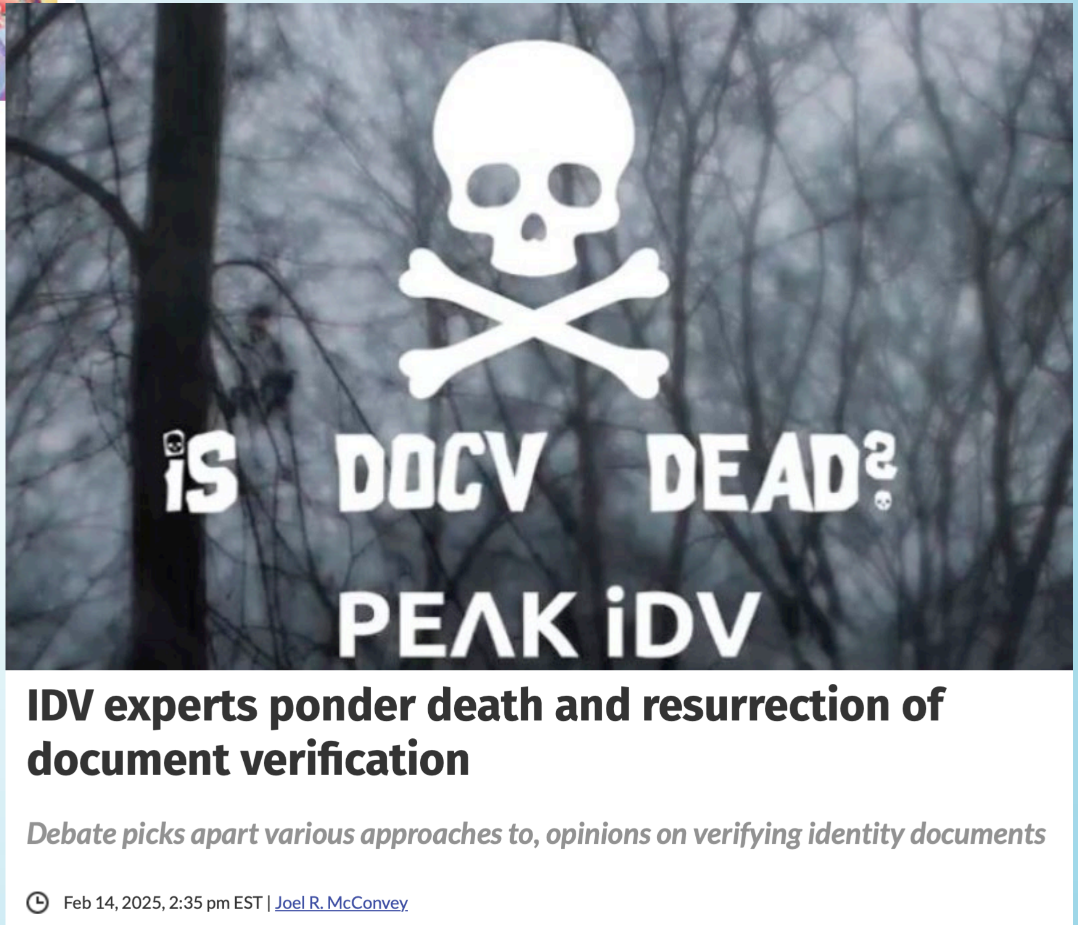


“Ripping” IDs Should Go the Way of CDs…

·

5 min read · Feb 21, 2024

Analog to Digital Conversion, anyone? “Ripping IDs” to confirm identity should go the way of Ripping CDs…

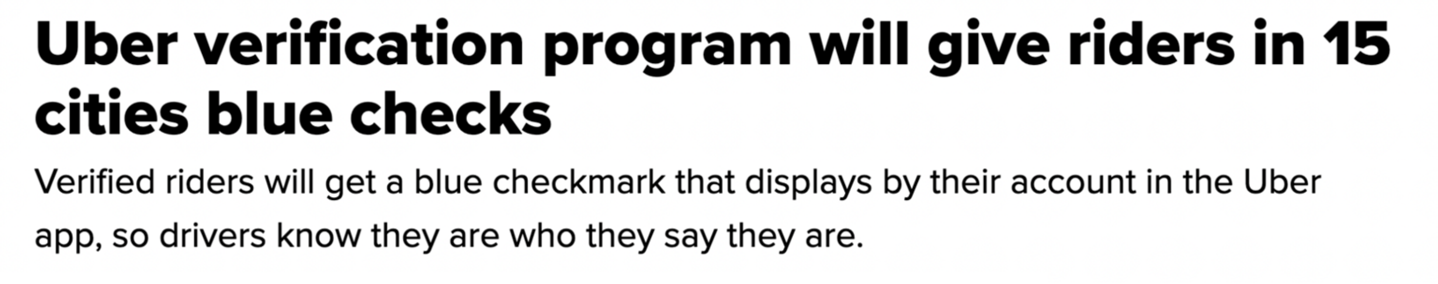


IDV experts ponder death and resurrection of document verification

Debate picks apart various approaches to, opinions on verifying identity documents

Feb 14, 2025, 2:35 pm EST | Joel R. McConvey

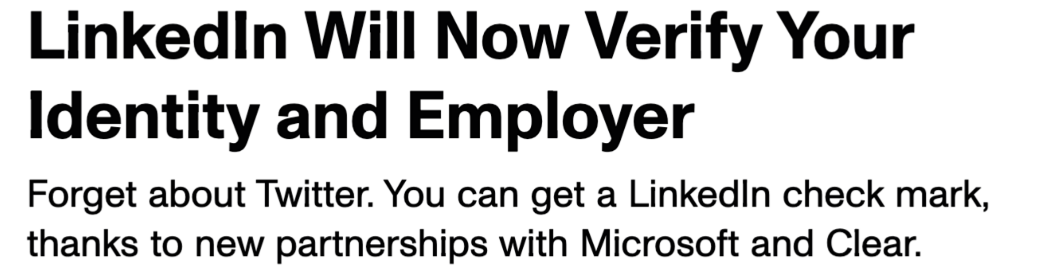
Uber



Uber verification program will give riders in 15 cities blue checks

Verified riders will get a blue checkmark that displays by their account in the Uber app, so drivers know they are who they say they are.

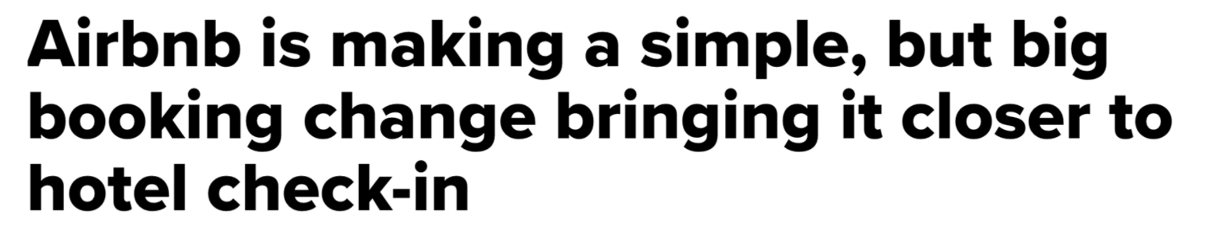
LinkedIn



LinkedIn Will Now Verify Your Identity and Employer

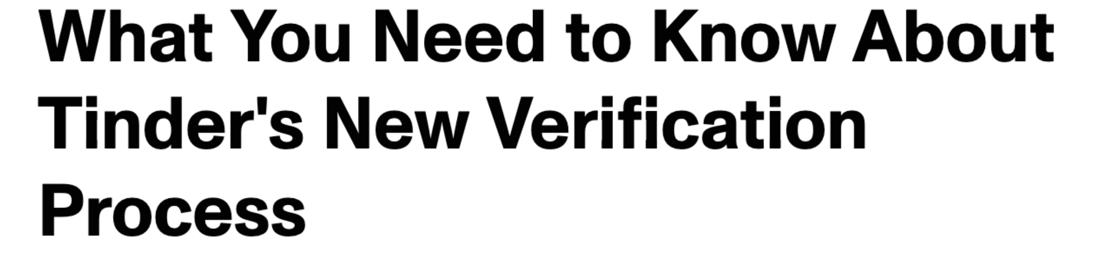
Forget about Twitter. You can get a LinkedIn check mark, thanks to new partnerships with Microsoft and Clear.

airbnb



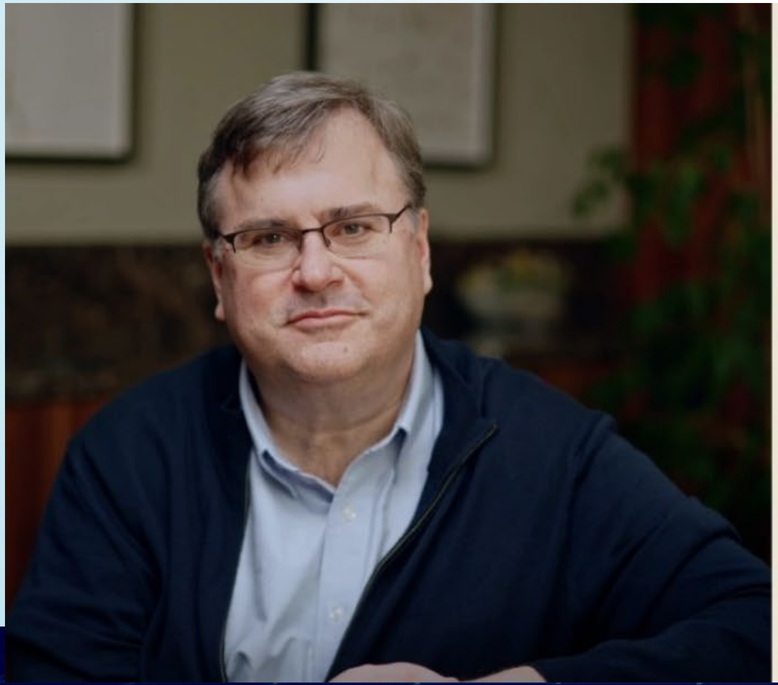
Airbnb is making a simple, but big booking change bringing it closer to hotel check-in

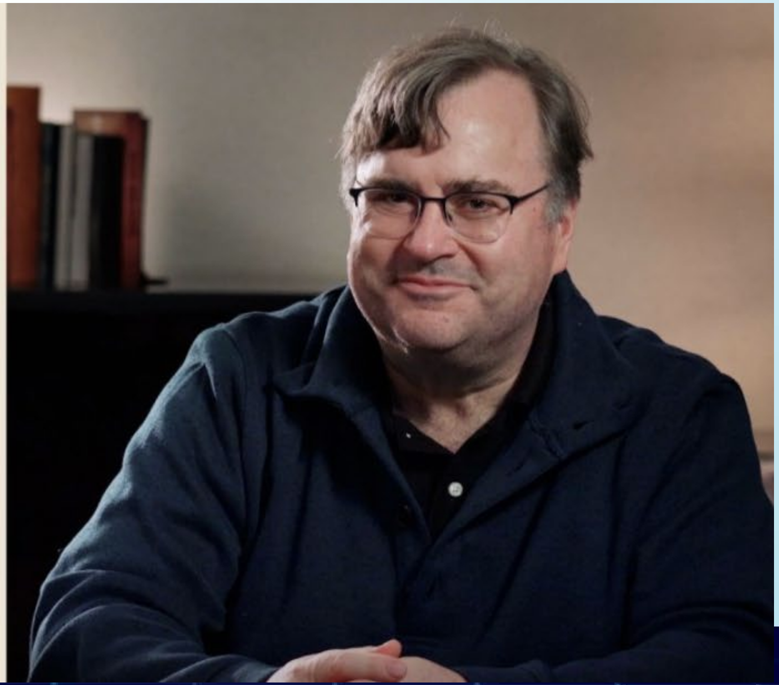
tinder®



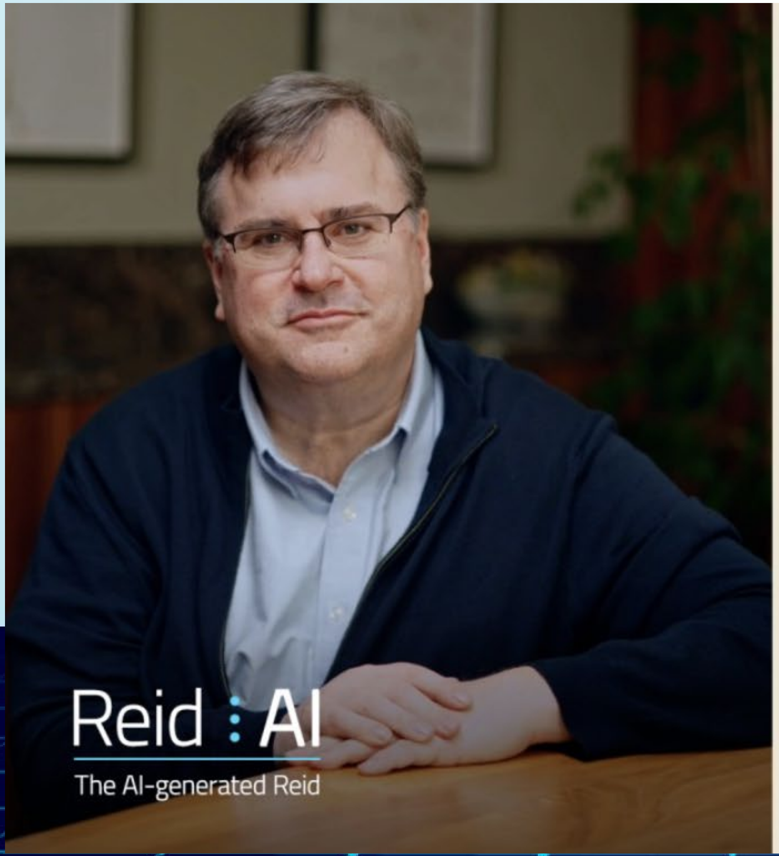
What You Need to Know About Tinder's New Verification Process

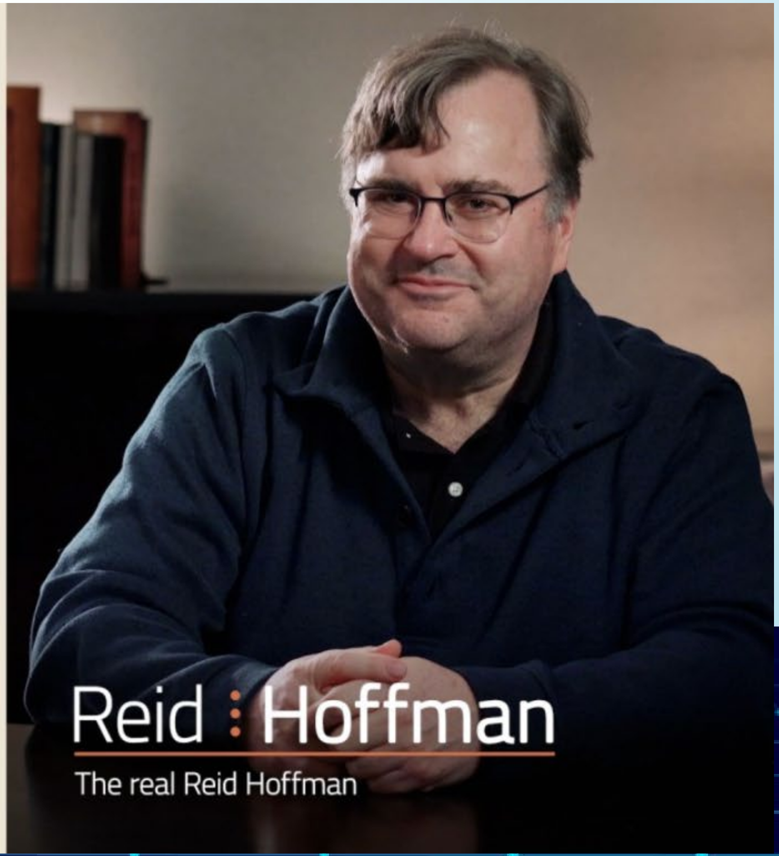
Which image was generated with AI?





Which image was generated with AI?

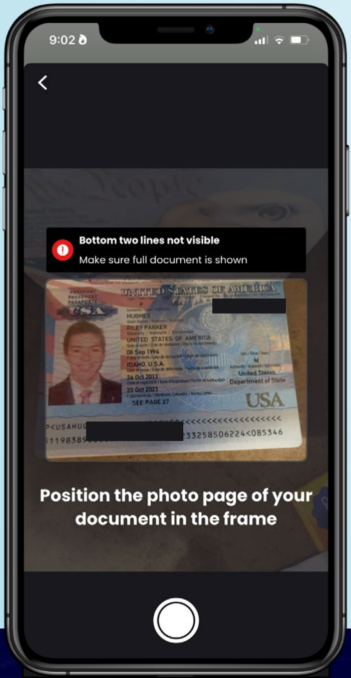




Billions of synthetic identities & agents

Time to re-verify on every platform

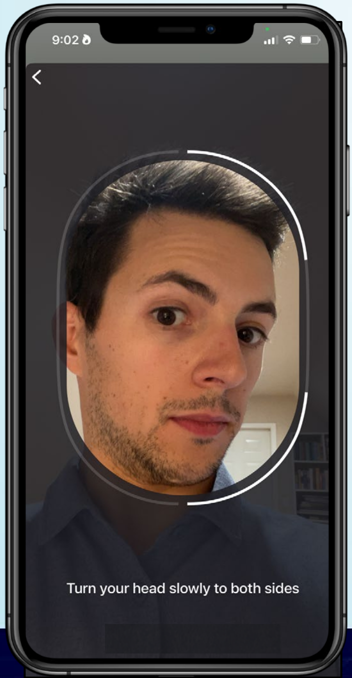
Uber


9:02

Bottom two lines not visible

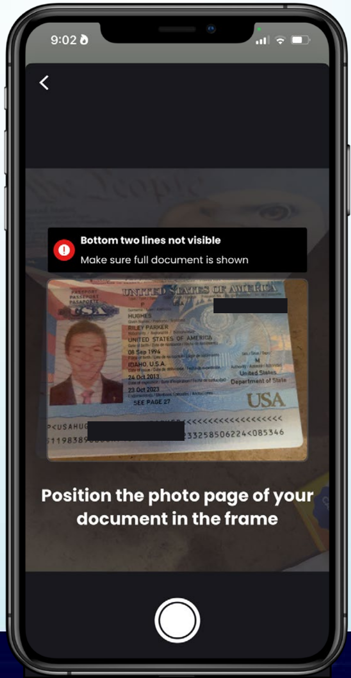
Make sure full document is shown

Position the photo page of your document in the frame


9:02

Turn your head slowly to both sides

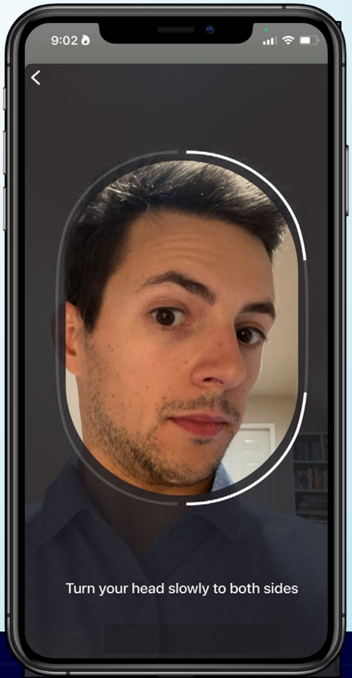
airbnb


9:02

Bottom two lines not visible

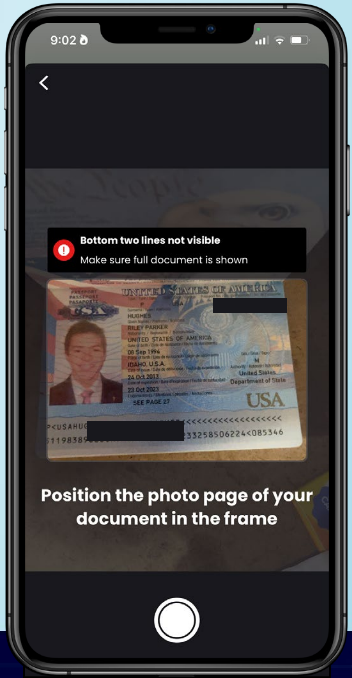
Make sure full document is shown

Position the photo page of your document in the frame


9:02

Turn your head slowly to both sides

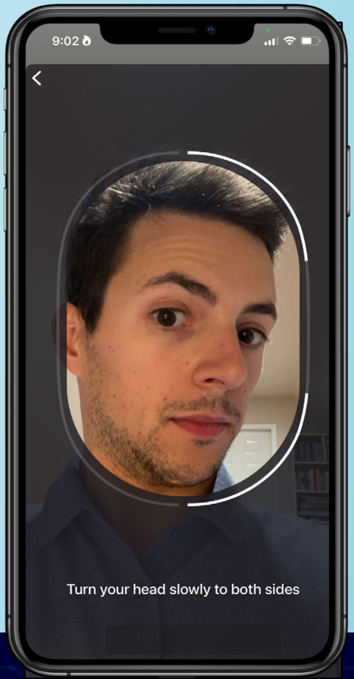
LinkedIn


9:02

Bottom two lines not visible

Make sure full document is shown

Position the photo page of your document in the frame


9:02

Turn your head slowly to both sides

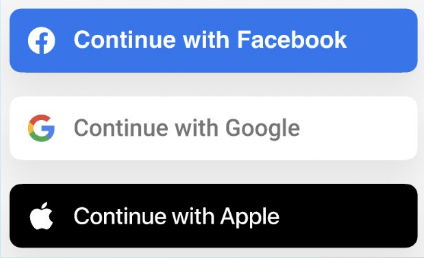
	Before	After
Retail		

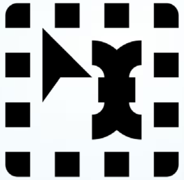
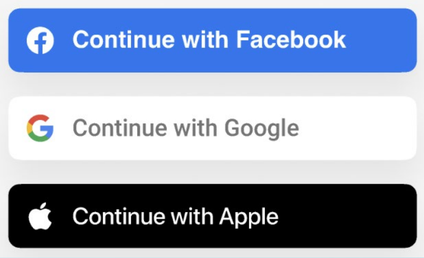
	Before	After
Retail		

	Before	After
Retail		
eComm		

	Before	After
Retail		💳
eComm		Pay shop Pay

	Before	After
Retail		💳
eComm		Pay shop Pay
Login	***	

	Before	After
Retail		
eComm		Pay shop Pay
Login	***	 Continue with Facebook Continue with Google Continue with Apple

	Before	After
Retail		
eComm		Pay shop Pay
Login	✱✱✱	 Continue with Facebook Continue with Google Continue with Apple
IDV		?

The market is quickly shifting to digital IDs

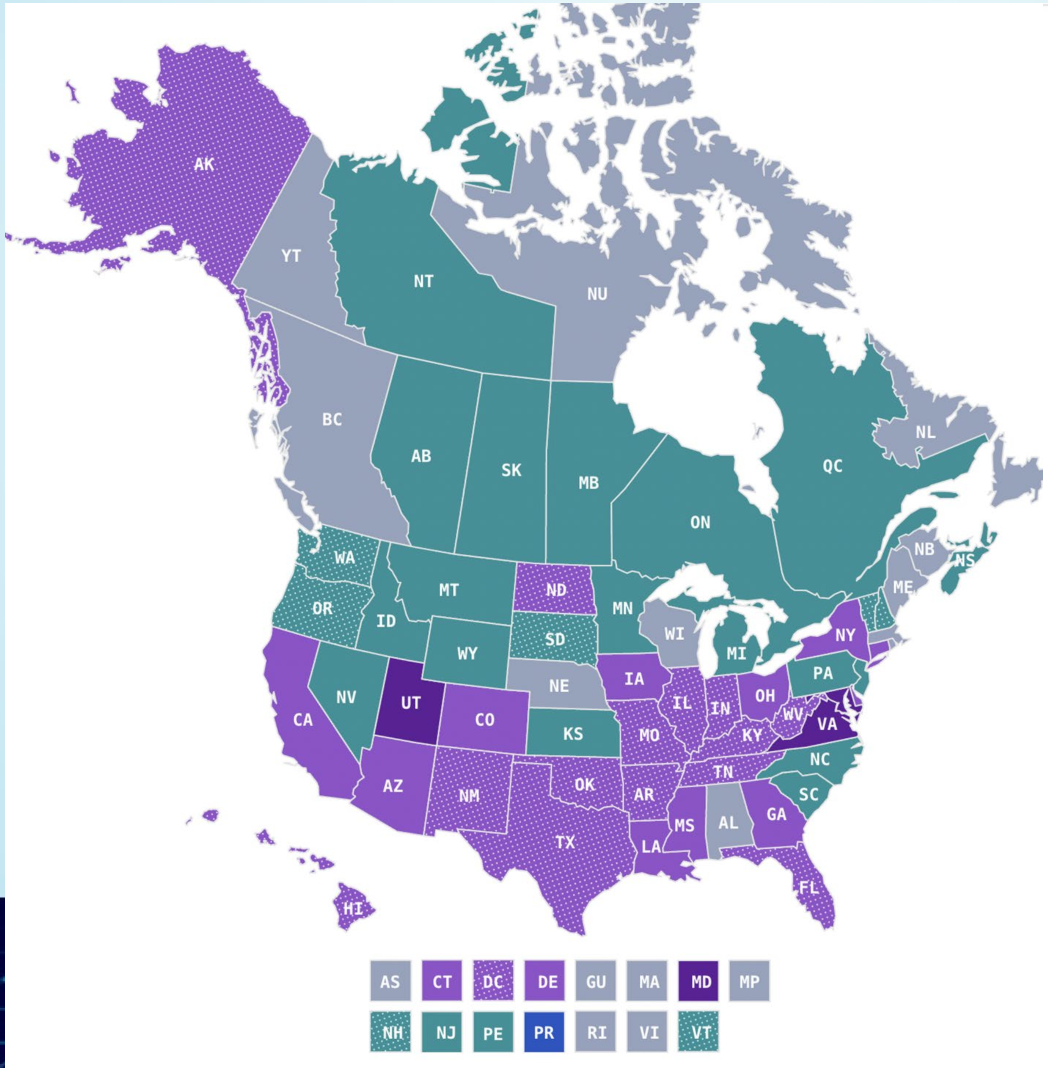
Mobile Driver's License Launches by Year

🇺🇸 **United States** • 27 states

2018	2019	2020	2021	2022	2023	2024	2025
						PR	IL
						WV	MT
						NM	TN
			CO		MO*	HI	NJ
			IA	DE	GA	NY	ND
			FL*	MD	MS	OH	WY
LA		AZ	UT	OK*	CA	VA	NC

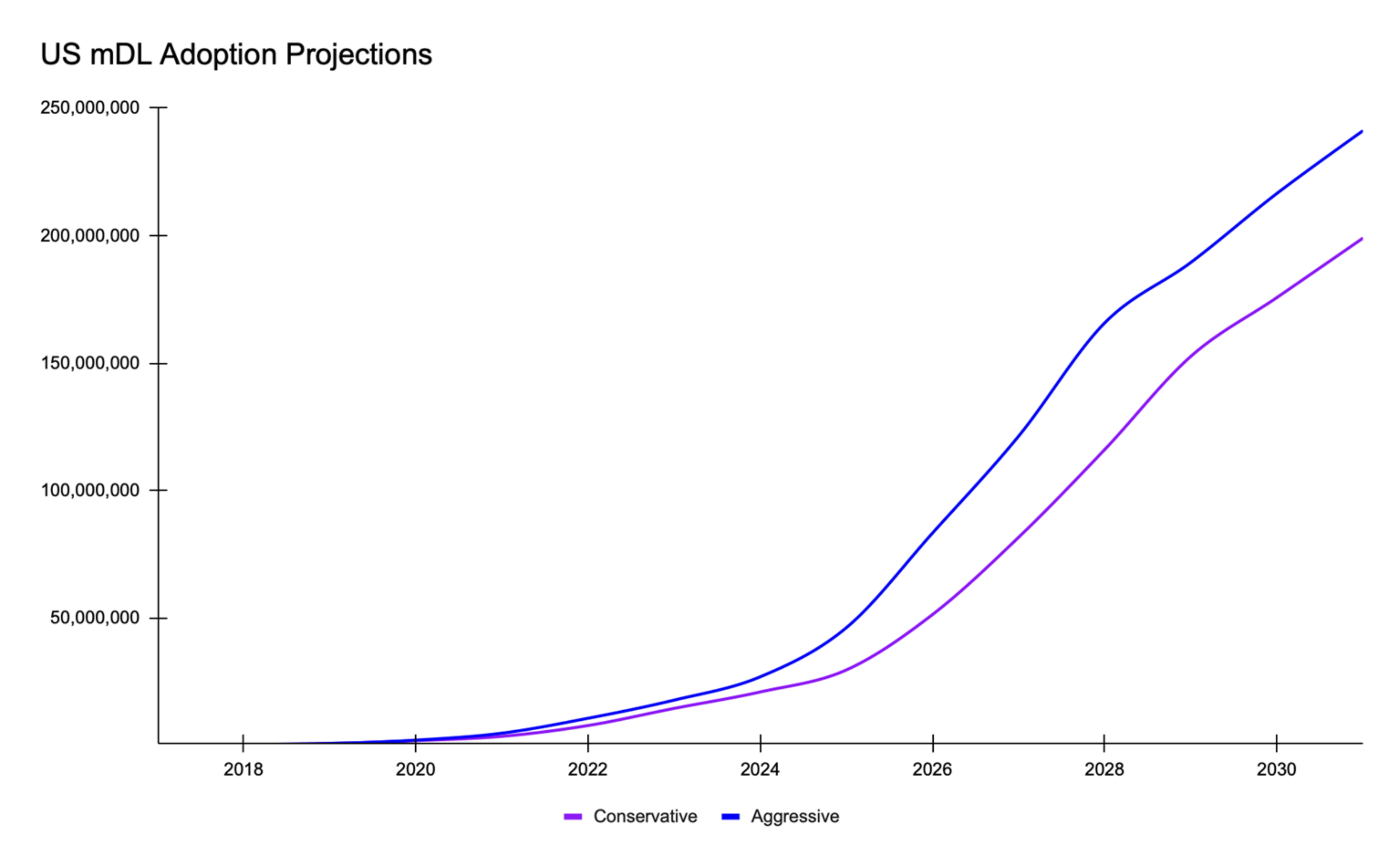
* temporarily suspended, relaunching soon

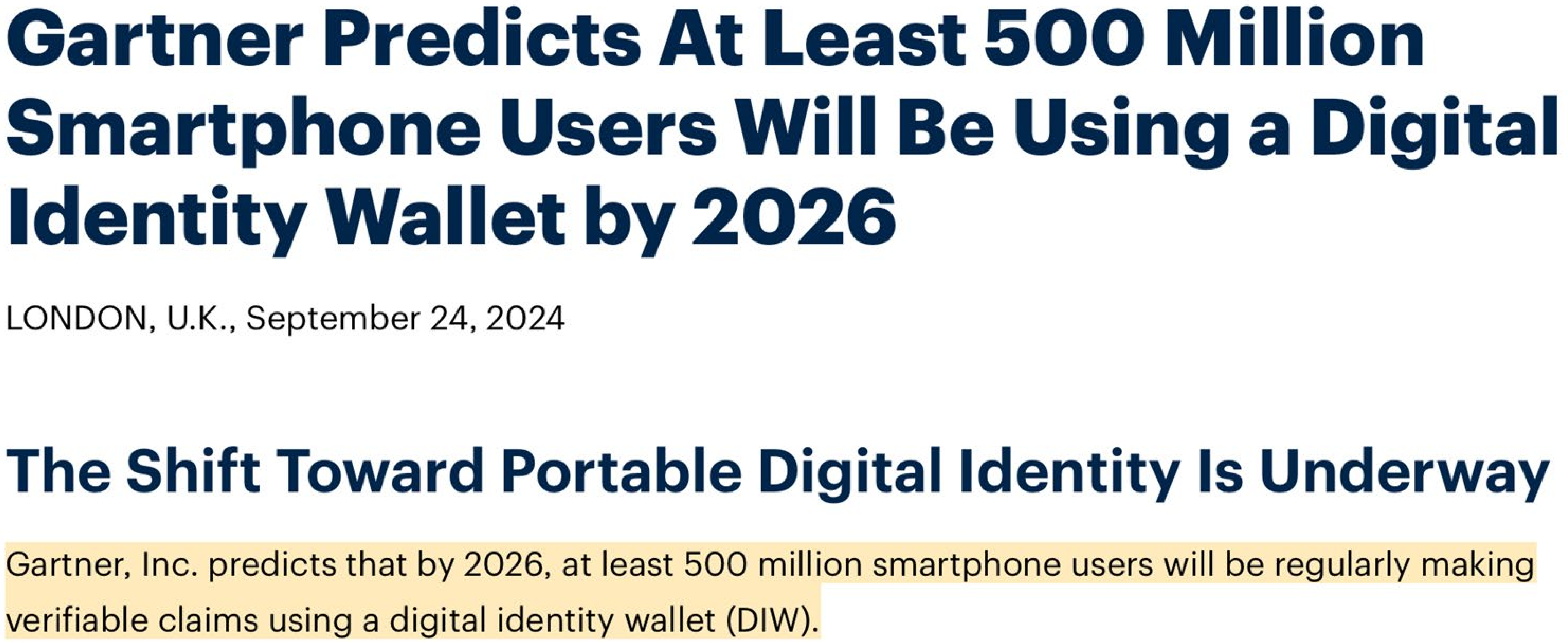
mDLs in development for 75% of Americans



- ■ Public Key Available in Digital Trust Service
- ■ Interoperable implementation
- ▨ Interoperable implementation in progress
- ■ Legislative and/or study activity
- ▨ Attempt to execute legislative and/or study activity
- ■ No information available
- ■ Jurisdiction specific implementation

100m state-issued mDLs by 2026





Gartner Predicts At Least 500 Million Smartphone Users Will Be Using a Digital Identity Wallet by 2026

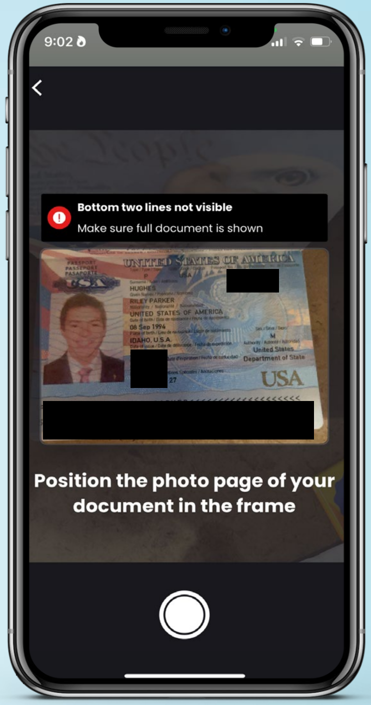
LONDON, U.K., September 24, 2024

The Shift Toward Portable Digital Identity Is Underway

Gartner, Inc. predicts that by 2026, at least 500 million smartphone users will be regularly making verifiable claims using a digital identity wallet (DIW).

DocV Market Size

⏱ ~50 seconds



Bottom two lines not visible

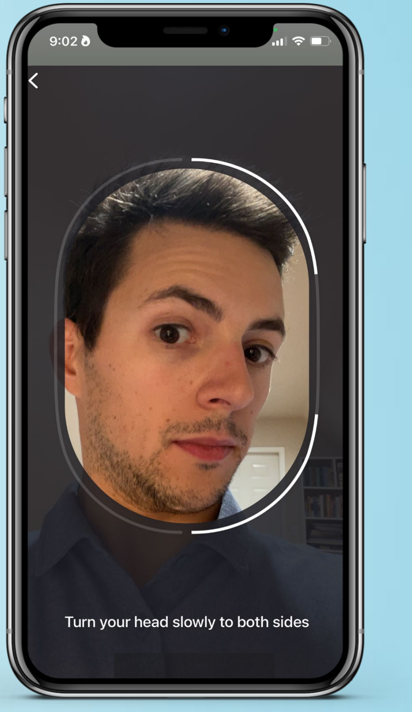
Make sure full document is shown

[redacted]

[redacted]

[redacted]

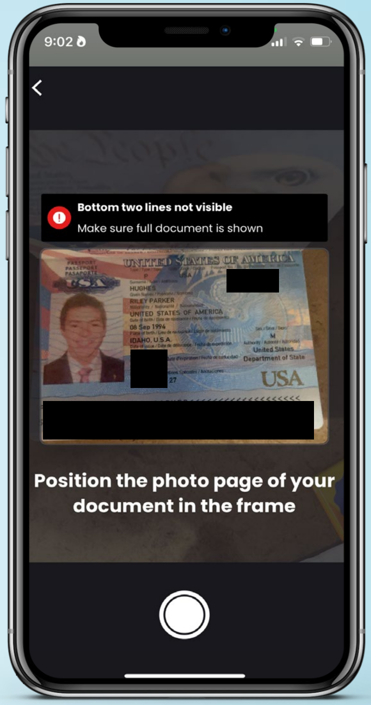
Position the photo page of your document in the frame



Turn your head slowly to both sides

DocV Market Size

⏱ ~50 seconds



9:02

Bottom two lines not visible

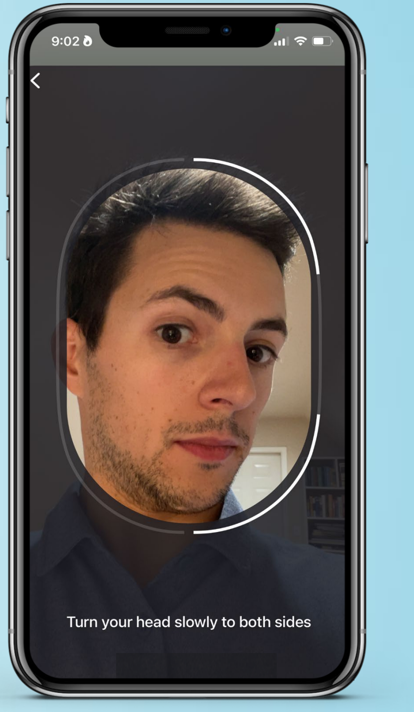
Make sure full document is shown

[redacted]

[redacted]

[redacted]

Position the photo page of your document in the frame



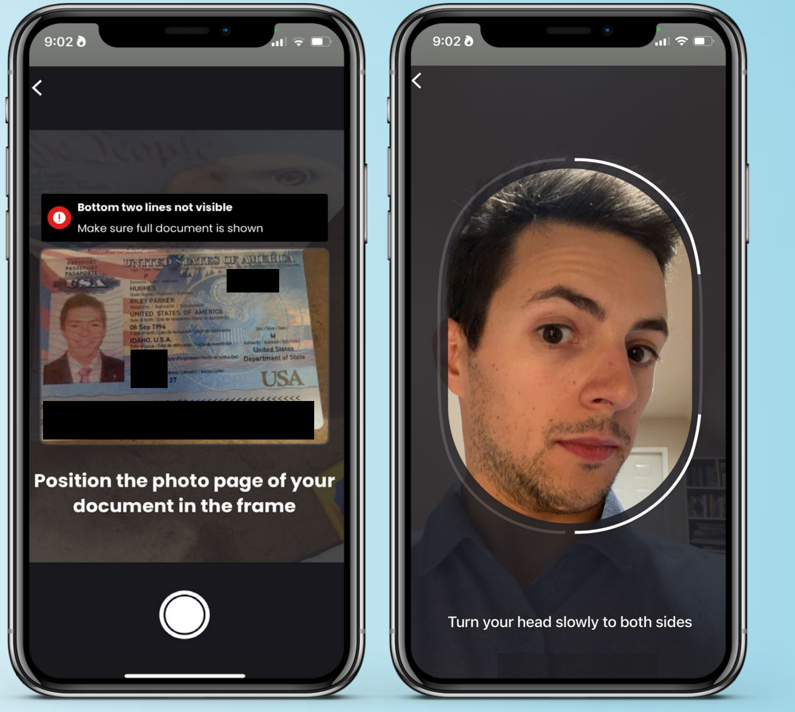
9:02

Turn your head slowly to both sides

DocV Market Size

Digital ID Market Size

⏱ ~50 seconds



9:02

Bottom two lines not visible

Make sure full document is shown

[redacted]

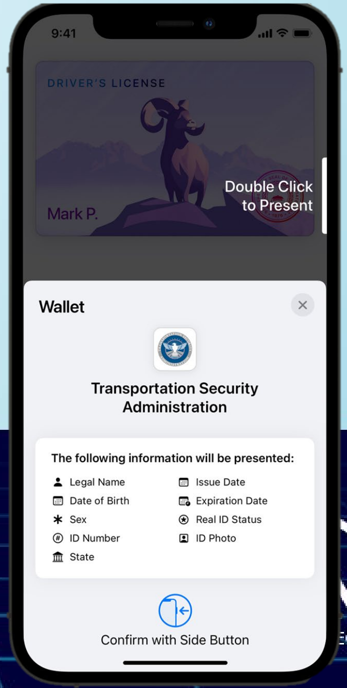
[redacted]

[redacted]

Position the photo page of your document in the frame

Turn your head slowly to both sides

⏱ ~5 seconds



9:41

DRIVER'S LICENSE

Mark P.

Double Click to Present

Wallet

Transportation Security Administration

The following information will be presented:

- Legal Name
- Issue Date
- Date of Birth
- Expiration Date
- Sex
- Real ID Status
- ID Number
- ID Photo
- State

Confirm with Side Button

What's New in the World of Digital Credentials

Lee Campbell
Google

IDENTITY & PAYMENTS SUMMIT
SECURE TECHNOLOGY ALLIANCE | Feb 24-26, 2025