ISF 2023

Information Security Forum for Texas Government

Driving Trust and Improved Customer Experiences with Digital Programs

incode

REIMAGINE TRUST

March 29, 2023

CHALLENGE

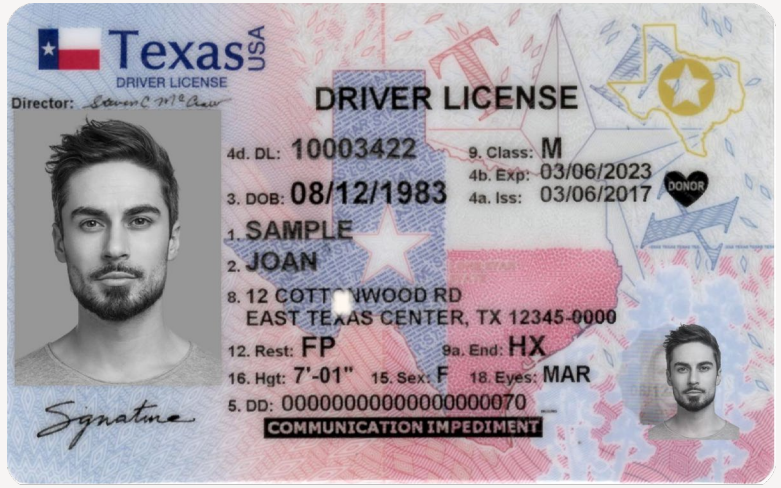
- System relies on 3,000-year-old tech (IDs)
- IDs are often tampered with, borrowed, found, stolen, etc.
- Deepfakes/synthetic identities are increasingly sophisticated
- Common processes are cumbersome, time-consuming, and present security risks

$56 billion
Cost of US identity theft in 2020 (2021 Identity Fraud Study, Javelin Strategy & Research)

42 million
Americans experienced identity fraud in 2021 (AARP)

2,920%
Annual increase in cases where a victim's information was frauduently used (AARP)

40%
Of people abandon digital onboarding processes due to difficulty, confusion, or length (Biometric Update)



Identity Fraud Continues to Skyrocket

Why Identity Thefts Are Increasing Each Passing Day

Rob Turner

Tweet Post Share

Identity Theft Report: Social Media Account Takeovers up 1,000% As 40% Of Personal Data Theft Victims Saw Their Information Misused

SCOTT IKEDA · OCTOBER 6, 2022

U.S. watchdog estimates $45.6 billion in pandemic unemployment fraud

Applicants got aid using dead people's Social Security numbers and the names of people serving federal prison terms

By Tony Romm

Updated September 23, 2022 at 9:31 a.m. EDT | Published September 22, 2022 at 2:00 p.m. EDT

SPECIAL REPORT

Largest Cases of COVID-19 Relief Fraud

Liz Blossom

April 27, 2022 1:00 pm

Pandemic response watchdogs urge agencies to focus on ID theft

Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios

JON BATEMAN JULY 08, 2020 PAPER

Identity fraud skyrockets as hackers stick to pre-pandemic techniques

Karen Hoffman April 6, 2022

Advisor › Personal Finance Advertiser Disclosure

1 in 4 ID Theft Victims Had Thousands Of Dollars Stolen During The Pandemic. Here's How To Keep Your Financial Info Safe

By Kelly Anne Smith, Forbes Advisor Staff

Reviewed By Korrena Bailie, Editor

Updated: Jul 6, 2022, 10:21am

A New Frontier of Fraud: Synthetic Identity Fraud

by Ari Jacoby — May 6, 2022

New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021

Reported fraud losses increase more than 70 percent over 2020 to more than $5.8 billion

February 22, 2022

Three sentenced in $87 million Medicaid fraud scheme

TRIB LIVE PAULA REED WARD | Wednesday, Sept. 28, 2022 6:00 p.m.

Losses From Stolen Identities Skyrocketed 79% to $24 Billion in 2021, a Javelin Study Finds

John Stewart March 30, 2022

Competitive Strategies, Credit Cards, Debit Cards, E-Commerce, Featured, Fraud & Security, Mobile Commerce, Point-of-sale

Better Business Bureau: $52 billion lost to identity thieves in 2021

Randy Hutchinson

Published 9:00 p.m. CT June 25, 2022

FOX NEWS INVESTIGATES · Published October 10, 2022 5:46pm EDT

FBI raises flag on elder fraud after thousands of retirees are scammed out of $1.7 billion

Edge Articles | 2 MIN READ | THE EDGE

Fraud Is On the Rise, and It's Going to Get Worse


THIS IS NOT MORGAN FREEMAN.

The Evolution of Identity Verification

1st GENERATION
Slow & Manual

- Human bias & errors
- Slow & unable to scale
- Low conversion rates

2nd GENERATION
Evolutionary change

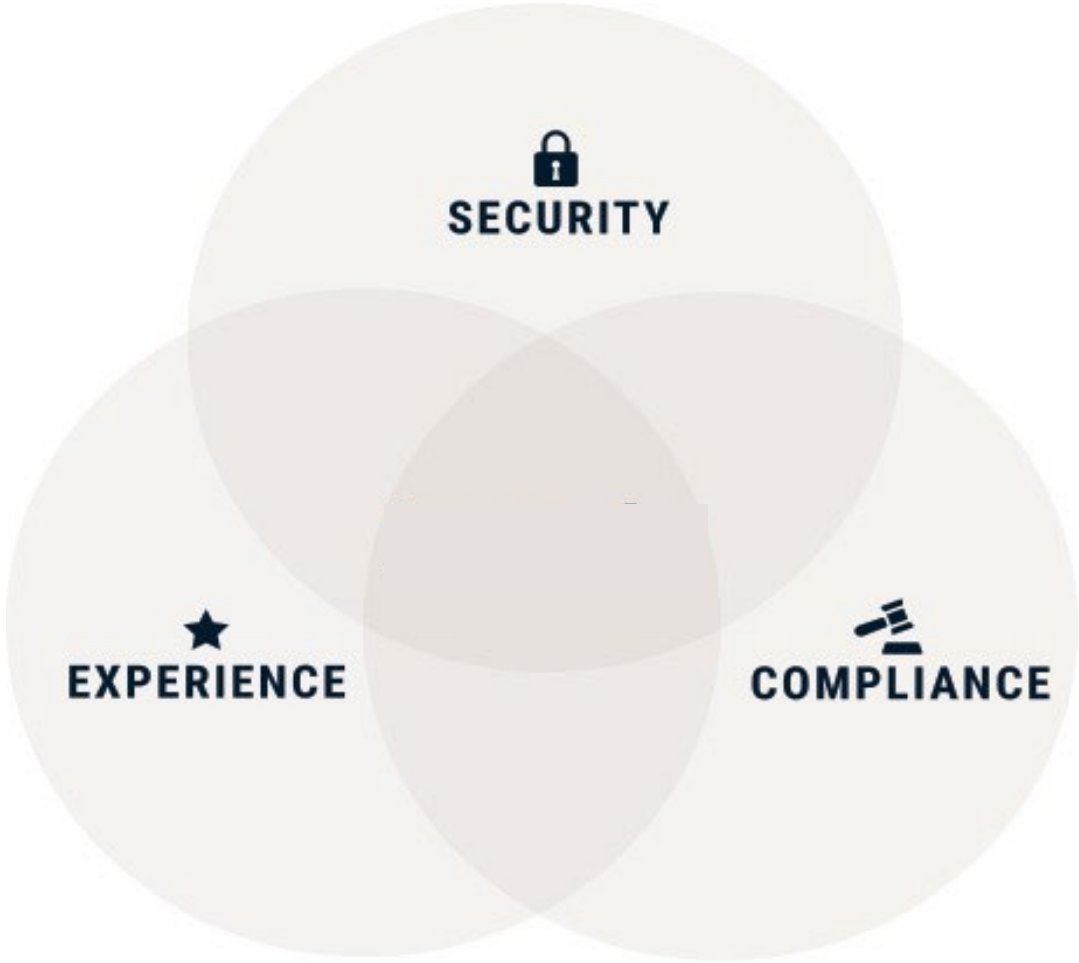
- Non-learning process
- Limited automation
- Privacy concerns

NEXT GEN
Paradigm Shift

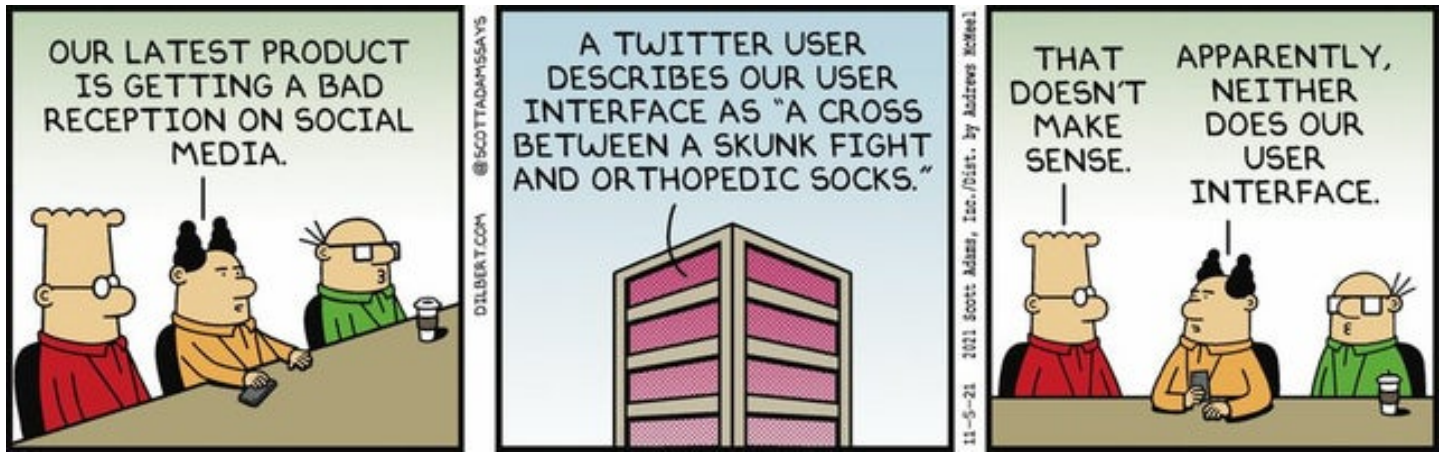
- Passive Liveness
- AI (No human interaction)
- Machine Learning
- Unified database

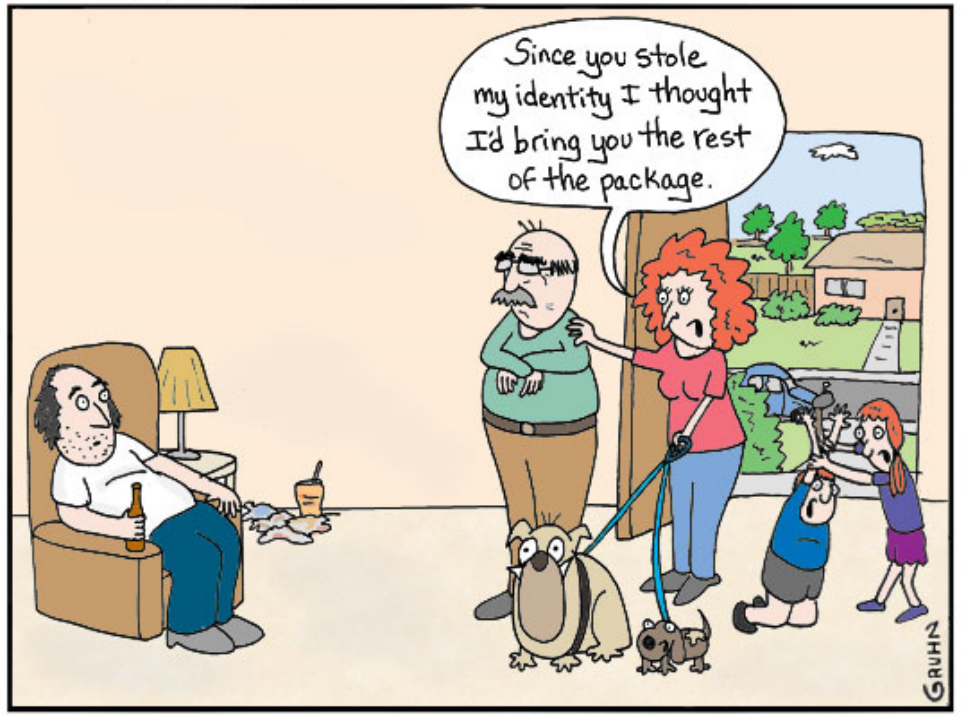
Top Considerations for Government

Eliminate fraud while optimizing security and compliance with superior customer experience



Customer Experience

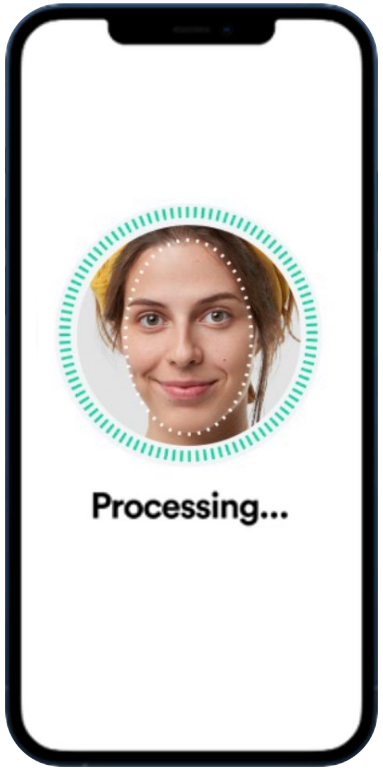




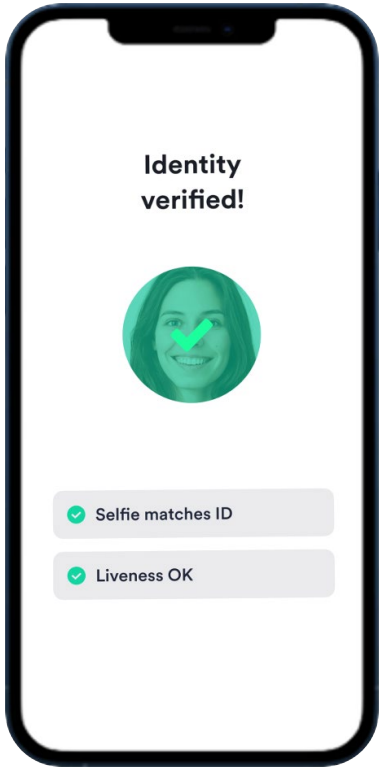
Next Gen Solutions

The use of facial biometrics is the most secure, accurate method of identity verification

SOURCE OF TRUTH



LIVENESS



FACIAL RECOGNITION

Document Authentication Technology

- ☑ Consider providers who offer a complete and continuously updated template library of credentials.
  - Libraries are typically created with machine learning models, which are trained on all US driver license and state ID credentials, tribal credentials, military IDs, passports, and other relevant document types

Subset of Texas Document Types

- Commercial Driver License
- Commercial Driver License - STAR
- Commercial Driver License Under 21
- Commercial Driver License Under 21 - Non- STAR
- Commercial Driver's License - Temporary Visitor
- Non-STAR Commercial Learner Permit
- Commercial Learner Permit - STAR
- Commercial Learner Permit Under 21 - Non- STAR
- Commercial Learner Permit Under 21 - STAR Concealed Handgun License
- Driver License
- Driver License - STAR
- Driver License Under 21
- Driver License Under 21 - Non-STAR
- Driver License Under 21 - STAR Driver's License
- Driver's License - Temporary Visitor - Non-STAR
- Driver's License - Temporary Visitor - STAR
- Driver's License Under 21 - Temporary Visitor - Non-STAR
- Driver's License Under 21 - Temporary Visitor - STAR
- Identification Card
- Identification Card - STAR
- Identification Card Under 21
- Identification Card Under 21 - Non-STAR
- Identification Card Under 21 - STAR

JAPANESE SHOP SELLS MASKS OF REAL PEOPLE'S FACES

Liveness Technology

NIST Conformance

- ☑ Consider providers with liveness technology evaluated by a NIST-accredited test lab.
  - Evaluated by Presentation Detection Attack (PAD) testing against the ISO 30107-3 standard
    - **PAD 1** tests against screens and paper/paper masks that are readily available
    - **PAD 2** tests against 3D printing and resin or latex masks that are more difficult to produce

These images are AI generated. None of these "people" exist.





Facial Recognition Technology

NIST Face Recognition Vendor Test (FRVT)

NIST

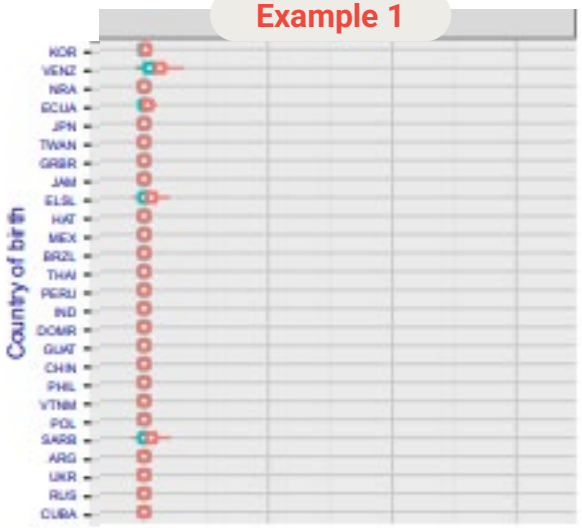
☑ Consider providers that are top ranked by NIST.

- Face Recognition Vendor Test (FRVT) is an ongoing program to evaluate facial biometric algorithms for speed, accuracy, and bias.
- Participation is voluntary and open to anyone. Participants can submit up to two algorithms.

NIST FRVT
Overview of Bias Analysis

- NIST uses 600K images tested with different populations (countries) as a measure of bias
- The graphs show the FNMR (False Non-Match Rate) or False negatives/incorrect rejections per country for two different FMR (false match rates)
- High and varying degrees of FNMR or rejections are seen in these plots when significant bias is present

Example 1



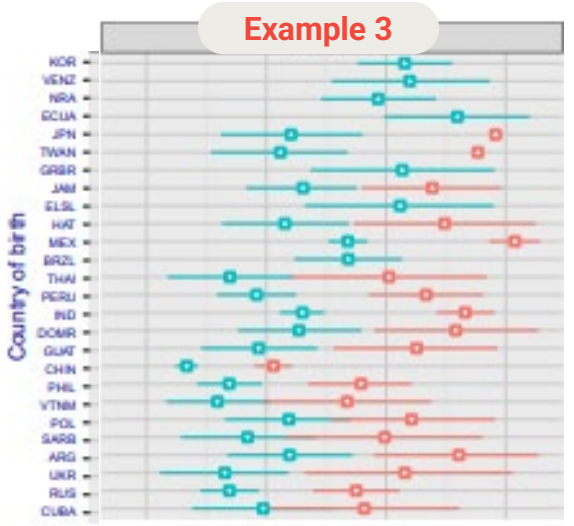
Low/insignificant bias

Example 2

Bias

High Bias

Example 3



NIST FRVT
Example Rankings

FALSE NON-MATCH RATE (FNMR)

Company Name	Constrained, cooperative		Less constrained, non-coop.			Time (ms)2	
FMR	VISA MC 0.0001		VISA 1E-06		VISA 0.0001	MUGSHOT 1E-05	WILD 0.0001	Template Creation	
Company A	**0.0077**	2	**0.0132**	2	**0.0034** 2	**0.0096** 2	**0.0313** 5	**479**	3
Company B	0.0267	7	0.0385	7	0.0081 6	0.0258 6	0.0470 8	355	2
Company C	0.0064	1	0.0116	1	0.0024 1	0.0096 3	0.0379 6	941	8
Company D	0.0160	5	0.0244	5	0.0065 5	0.0199 5	0.0309 4	306	1
Company E	0.0230	6	0.0353	6	0.0085 7	0.0398 7	0.0301 2	577	5
Company F	0.0098	3	0.0136	3	0.0040 3	0.0105 4	0.0303 3	678	7
Company G	0.0125	4	0.0214	4	0.0047 4	0.0085 1	0.0282 1	540	4
Company H	0.1733	8	0.2257	8	0.052 8	0.2610 8	0.0450 7	669	6

Note: In NIST 1:1 Face Recognition Vendor Test, every company can submit up to two algorithms, and the report is based on algorithms.

Facial Recognition Technology
Diversity, Equity, & Inclusion (DEI)

The US General Services Administration (GSA) is conducting an **Equity Study on Remote Identity Proofing** to test how methods like facial recognition perform across various demographics. Learn more here.

- 2,000 incentivized volunteer participants will go through a remote identity verification process to measure equity and bias. Study results will be released in a peer-reviewed publication.

The U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T), in partnership with other federal agencies, will host a series of test events through its **Remote Identity Validation Technology Demonstration (RIVTD)**. Learn more here.

- RIVTD will test system ability to authenticate identity documents, assess the "liveness" of selfie photos, and evaluate identity verification using images taken with smartphones and similar devices.
- The study will objectively measure performance against realistic and sophisticated attacks; answer questions about the overall performance, risks, and fairness of these technologies.

Sample of Critical Standards

Document Authentication & Facial Recognition

NIST 800-63-3A NIST 800-63-4	Requirements for enrollment and identity proofing of applicants that wish to gain access to resources at each Identity Assurance Level (IAL).

Liveness

ISO 30107-3	Establishes principles and methods for performance assessment of PAD mechanisms; reporting of testing results; and a classification of known attack types.

Accessibility

WCAG & Section 508	Federal standards for web and app accessibility to ensure access for those with visual, hearing, mobile, and other impairments.

Security & Compliance

NIST 800-53 & 800-171 (FedRAMP)	FedRAMP sets the security and compliance requirements mandatory for all cloud services used by Federal agencies.

Additional Considerations

Facial Recognition

Is your agency interested in doing 1:1 or 1:N facial recognition? What is the provider's solution?

Data Usage

What controls does the provider have in place for data collection, storage, deletion, marketing, and monetization?

Deployment

Which deployment method is the agency interested in (e.g., on-prem, cloud, hybrid) and which methods does the provider offer?

Adoption

Does the provider require users to create an account or download an app?

Potential Use Cases

Securing credential issuance

Eliminate fraud using facial recognition at issuance

Securing testing

Eliminate fraud and improve the customer experience

Securing call-center services

Eliminate fraud and improve the customer experience

Securing in-person check-in

Improve the customer experience and in-person service times

3rd Party Verification

Eliminate fraud and protect privacy through data matching services

Securing online services

Eliminate fraud and improve service times

THANK YOU!

Rob Mikell
VP, Public Sector
404-732-4504
rob.mikell@incode.com