FTX™ IDENTITY

Addressing the Trust Dilemma in the Digital Identity Landscape

The digital world is expanding at a rapid pace, and so are the issues associated with it. One of the fundamental issues of our time is how to properly and securely perform online identity verification so that we can give them access to safe and secure means of performing digital activities. There are several conceptions of what constitutes a digital identity, which presents the first obstacle to be solved. Many competing technologies are being employed in a complicated and fragmented market to address some of the problems in our digital lives.

Since there is no easy or universal solution to this issue, there is a big chance for technology companies to create focused solutions to onboarding, compliance with anti-money laundering (AML) and know your customer (KYC) regulations, or something even more major—a digital version of a passport or a national identity system. The issue of how to validate a person's identity for access to online shopping is resolved by services for verifying an identity. They address the problem of trust between service providers and their customers in the absence of universal digital identities that can be used across websites and cross-border digital identity.

David Britton, Experian's Vice President of Industry Solutions, observed in 2019 that, "we are in a state of transition where we will have a combination of old and new identity—physical ID documents and digital identity. This is where eIDV (electronic identity verification) is solving an immediate problem." Many businesses that want to lessen their physical footprint and support digital transformation initiatives while lowering the risk of fraud have a compelling need for the capacity to onboard new customers to services through remote digital channels, including web and mobile.

Digital Onboarding

The most recent AML, KYC, and customer due diligence (CDD) regulations are met through digital identification and document verification services, which also assist digital onboarding. These provide an immediate solution to the identity-proofing issue. Digital identity and document verification specifically respond to the following questions:

- **Are they a genuine user?**
- **Is the user permitted to utilize the data that they presented?**
- **Can the user do business with the service provider?**
- **What are the risks associated with interacting with the user?**

Service providers are adopting digital identity and document verification services in ever-increasing numbers thanks to a combination of ever-more accurate facial recognition, document verification, and a wider variety of verifiable identity sources (data and signals) powered by machine learning (ML) and artificial intelligence (AI).

The four questions identified have been shown to be connected to four main parts for digital identity and document verification:

- **Validity of Presence:** That the thing presented is a real person, not a fake. The typical method for handling this is to use a camera—a smartphone or webcam—to capture the individual's face and then use a variety of technologies to confirm that it is a live face.

- **Capturing a Document:** Authentication of the trusted document being submitted to a service provider by secure capture and confirmation that it is genuine and unaltered.

- **Risk Reduction and Corroboration:** Validation of the acquired photos, the document, and the face. Various alternative methods, such as gathering signals (device and network) and data, will be utilized according to the risk appetite to validate the entity's identity and validity to accomplish a certain task, such as opening an account.

- **Orchestration:** The workflow that oversees the operations and connects all of the many technologies and data sources.

Digital Onboarding Cont'd

DRIVER LICENSE

Based on these four key elements, the following information represents an entire process and lists the most popular technological approaches:

Digital Identity Verification Process from Start to Finish

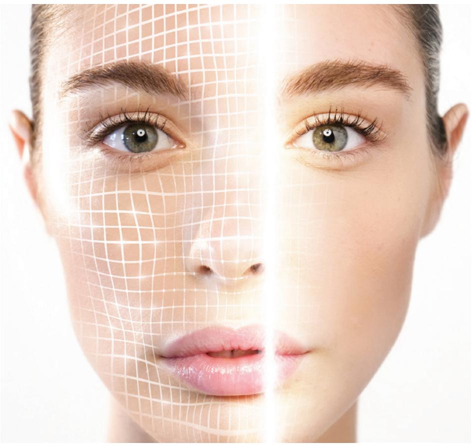
- **Snap a Selfie:** Utilizing facial recognition software, the user snaps a selfie.
- **Capture a Document:** A government-issued ID is scanned by the user.
- **Data is Verified:** Verifiable information is gathered to support already-collected ID and biometric data.
- **Data is Analyzed:** The system validates the data.

Using Biometrics to Ensure Authentic Presence

A key piece of technology for digital identity verification services is biometrics. When a person's identity is being verified remotely or without assistance, it takes the position of a human. Instead of a bank employee or a telecom employee comparing a customer's face to the image on a government-issued document in-branch or in the store, facial recognition software captures a picture of the customer's face and compares it to the image taken from the government-issued document. Real-time spoof and liveness detection, also known as presentation attack detection (PAD), is a crucial component of authentic presence assurance. A strong facial recognition system must be able to resist typical spoof attempts and be able to tell whether a person is legitimate and present during the identity verification procedure.

Improved Facial Recognition Methods

Numerous advantages of contemporary facial recognition algorithms include:



- **Assuring the live image** is suitable for facial recognition before it is collected and after it is scanned.
- **Liveness techniques** including eye blink, head movement, texture, light reflection, sharp lines, perspective shifts, and behavior.
- **Searching the facial watchlist** for previously fraudulent applications.
- **A facial search of past applicants** from a certain time period, a high-risk group of applicants, or all applicants is done to look for applications that purport to be from different people but have the same face.

Due to the availability of machine learning (ML) and deep neural network (DNN) capabilities, considerably larger and more diversified data sources, and the capability to continually train algorithms on real data, the level of accuracy increase in facial algorithms has been tremendous.

What Are MRTD and MRZ?

A machine-readable zone is referred to as MRZ, while a machine-readable travel document is referred to as MRTD. Most passports and other forms of identification around the world use the MRZ format. It includes the document holder's information in a visually readable and optical character recognition-encoded format.

Document Capture and Verification Accuracy Rates

In order to achieve AML/KYC compliance and controllable fraud rates, a solution must be able to capture fraudulent identification documents, making document capture and verification accuracy an essential evaluation criteria. There are many degrees of document verification accuracy, and research indicated that accuracy rates where auto verification was successful were in the 80% range. 15% were typically regarded as suspicious and call for more investigation, usually by human analysts, whereas 5% were unsuccessful and were seen as fake. With biometric passports, accuracy rates may be greater since information, including biometric data, is read from a chip using NFC and then confirmed. The quality of the pictures utilized when extracting data directly from a chip as opposed to utilizing a scanned image is important when using NFC for biometric chip reading.

Capturing and Verifying Documents

It is important to ensure that the documents submitted to the service provider are genuine and unaltered.

Document types that are utilized include:

- **Passport (biometric and non-biometric)**
- **Driver's license**
- **National identity card**

This is often either the first or second procedure that will be followed as part of the end-to-end digital verification service, depending on the workflow. Verifying an identity using a government-issued document with an image complies with AML/KYC standards and is typically done in a physical office or retail setting under the guidance of a trained individual (for instance, in a bank branch when opening up an account). Document collection and verification are shifting online due to the expansion of digital services and a decline in the use of physical bank offices and retail establishments. When an identity chip is present, such as in biometric passports, identity information is read from the document using a camera, a smartphone, a personal computer (webcam), or via NFC (near field communication).

The application of artificial intelligence (AI) and machine learning (ML) to this field is improving dependability and accuracy rates. The powers of AI should not, however, be overstated, particularly when used for document authentication and verification. Even with AI assistance, accuracy rates for document verification typically fall in the 80% bracket, and to increase accuracy, an analysis performed by a human is usually required.

Risk Management, Orchestration, and Corroboration

Corroboration, risk management, and orchestration make up the last three parts of digital identification and document verification. In order to increase the accuracy rates for verifying an identity, corroboration uses signal and data collecting. For service providers looking to offer comprehensive end-to-end identity and document verification services, orchestration, or workflow, services are essential. As they ultimately decide, based on the information provided to them, whether a person's identity can be trusted, is legal, and is linked to a person who is permitted to perform a certain action, such as opening a bank account, the decision-making or risk-management aspects of identity and document verification are becoming more and more significant.

False Positive and Negative: When a legitimate document is marked as a fake or suspicious one, it is known as a false positive. A false negative is flagged as genuine and accepted by the system.

Using identification signals and data in addition to document verification and facial recognition can significantly increase the accuracy of identity verification. These data sources include social network data as well as more conventional ones like name, social security number, and mobile number.

- **Mobile Network Operator (MNO):** Current information from the mobile device and an MNO
- **Citizen:** Data obtained from a utility or government database
- **Customer:** Information obtained via direct promotional campaigns

Risk Management, Orchestration, and Corroboration Cont'd

Identity Signals and Data

- **Credit:** Information obtained by a credit agency, or bureau, that is authorized to collect and maintain consumer credit information on people
- **Electoral Roll:** A list of registered voters that the government has compiled and released
- **Government-Issued:** Governmental databases include those for passports, driver's licenses, and national insurance
- **Property Penalties:** Information provided by the government about property ownership
- **Utility:** Information was released for a national provider of telephone, gas, electricity, and water services
- **Watchlists:** List of countries with screening programs – for instance, the Office of Foreign Assets Control (OFAC)

Market Drivers and Adoption

The support for digital onboarding, age verification, compliance with AML and KYC regulations, and building confidence in the sharing economy are a few of the major market drivers for digital identity and document verification services. Due to the emergence of challenger banks and Fintech providers, it is crucial to have a solid digital onboarding solution that complies with AML and KYC regulations. As a result, challenger banks are setting the standard for the support of digital identification and document verification services. This market is quite booming, and several sectors are driving adoption efforts, including:

- **Financial services including insurance**
  (BFSI—short for banking, financial services, and insurance)
- **eCommerce including the sharing economy and age-restricted industries**
- **Both mobile and fixed telecommunications**
- **Gaming activities, such as gambling and video gaming**
- **Physical retail**

A combination of AML/KYC compliance, fraud reduction, and digital transformation programs within the financial service providers have substantially influenced the use of electronic identity and document verification services for the financial services. Financial service providers can gain a lot from the capacity to rapidly and securely enroll new customers using smartphones, and it fits with the strategy of challenger banks and Fintech companies that only have an online presence. There is significant activity from the challenger bank community which prides itself on being digital-based and mobile first and foremost. It is crucial for these banks to be able to onboard new customers and allow them to open accounts by proving their identification on a smartphone or during a web session because the capacity to operate financial services without a physical presence (branch) is a key aspect.

In the telecoms industry, which is also experiencing rapid adoption development, there are primarily two situations in which the telecom operator is a:

- **Provider of eIDV services**
- **Purchaser of eIDV services for use by its own customers**

As an MNO owns vital information on mobile customers, such as name, mobile number, and geolocation information, there is a tremendous possibility for telecom providers to play a key part in the identity verification marker.

FTx Identity is the Solution to This Concern

A user-friendly, AI-based, multi-stage platform for centralized login authentication and authorization, age verification, and identity management are all offered by FTx Identity. Our identity and age verification technology (AVT) seamlessly integrates with desktop, mobile, and online apps to prevent fraud and the sale of products with age limits to minors. Our straightforward solution helps retailers adhere to regulatory standards while saving time, enhancing dependability, and automating the ID verification process.

The advantages provided by FTx Identity are as follows:

- **Continuous assessment and efficient integration**
- **Cost-effective**
- **Examining various forms of identification issued by the government**
- **Global coverage**
  (various ID documents from over 180 countries are fully supported by FTx Identity)
- **Thorough assessment that goes beyond age verification**

AI-Based Multi-Stage Verification

Our AI-based multi-stage verification process, which assures quick response times and accurate document verification, is one of FTx Identity's most prevalent features.

Checks Against a Database of Fake IDs

We cross-reference the customer's ID with a global database of fake and invalid identification documents that we have collected from both public and private sources.

Photo Forensic Analytics Utilizing Vision AI

Our innovative verification platform uses photo forensics to stop users from tricking ID verification systems by submitting fake documents, capturing documents from the screen, or editing or fabricating documents in Photoshop. Through the use of deep learning and image forgery forensics, our vision AI can combat fraudulent attempts.

Examining Active Security Features

The majority of documents issued by the government have active and passive security elements like watermarks, ultraviolet inks, fluorescent overlays, holograms, microtext, and laser engravings. To ensure that no fake documents get past our verification system, our AI engine evaluates and compares each security feature to the original copy of sample documents in our database using the template.

Compare the Data on the ID's Front and Back

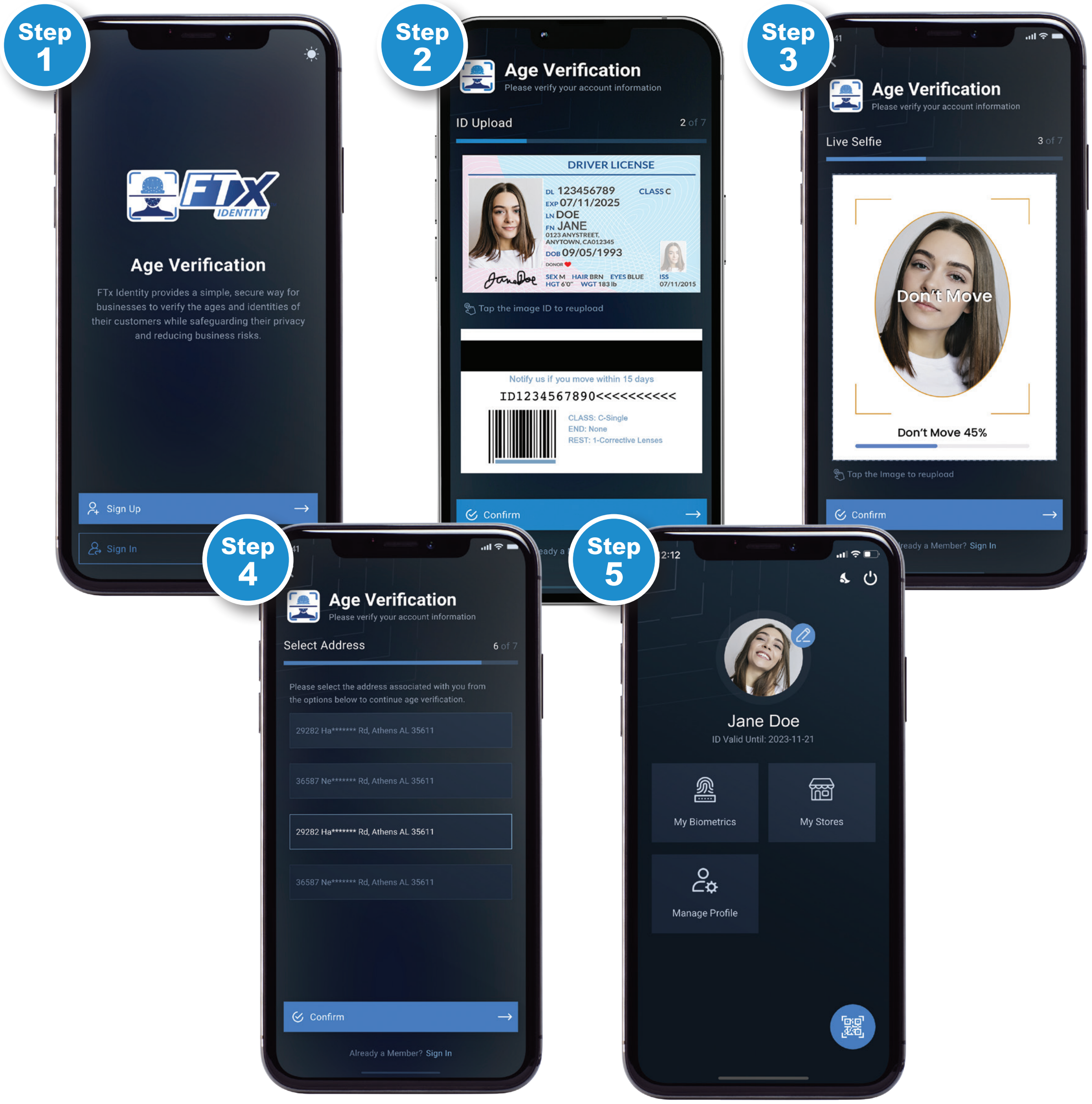
Our verification engine reads and compares data from the front and back of the ID paper via OCR visual data scanning, MRZ scanning, or barcode scanning.

Examine and Comparing Selfie Photo

Masks, avatars, and other complex spoofing attempts like deep fakes are all blocked by our selfie photo liveness detection technology. Additionally, our AI engine checks to see if the selfie the user supplied matches the image on the ID document.

Online ID Scanning for Self-Registration

One of FTx Identity's greatest advantages is that, thanks to its efficiency and convenience, it is user-friendly for customers. Customers can register directly on the site by uploading a photo of their government-issued ID and a selfie that they took on their phone or computer. When the technology successfully compares the customer's selfie with the ID's image, it automatically extracts personal data to build a secure profile for the customer on the FTx Identity platform. Then, customers may view and share their profile with the businesses they choose.



Step 1

Age Verification

FTx Identity provides a simple, secure way for businesses to verify the ages and identities of their customers while safeguarding their privacy and reducing business risks.

Step 2

Age Verification

Please verify your account information

ID Upload 2 of 7

DRIVER LICENSE

DL 123456789 CLASS C
EXP 07/11/2025
LN DOE
FN JANE
0123 ANYSTREET,
ANYTOWN, CA012345
DOB 09/05/1993
DONOR ❤
SEX M HAIR BRN EYES BLUE ISS
HGT 6'0" WGT 183 lb 07/11/2015

Tap the image ID to reupload

Notify us if you move within 15 days

ID1234567890<<<<<<<<<<

CLASS: C-Single
END: None
REST: 1-Corrective Lenses

Step 3

Age Verification

Please verify your account information

Live Selfie 3 of 7

Don't Move

Don't Move 45%

Tap the Image to reupload

Step 4

Age Verification

Please verify your account information

Select Address 6 of 7

Please select the address associated with you from the options below to continue age verification.

29282 Ha******* Rd, Athens AL 35611

36587 Ne******* Rd, Athens AL 35611

29282 Ha******* Rd, Athens AL 35611

36587 Ne******* Rd, Athens AL 35611

Step 5

Jane Doe

ID Valid Until: 2023-11-21

Interested in finding out more about our identity verification solutions?
Contact one of our specialists, and they can help you with any questions you might have.