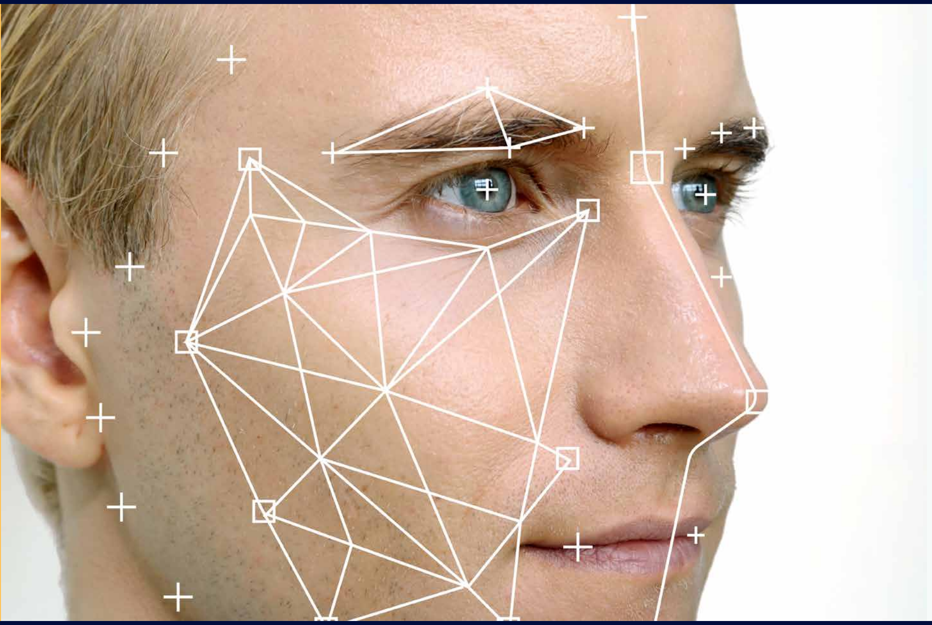
A Comprehensive Guide To Age & Identity Verification For Your Business



FTX IDENTITY™

A Comprehensive Guide To Age & Identity Verification For Your Business

Contents

Introduction

In this era of digitization, the demand for online security is at an all-time high. Businesses are under increasing pressure to confirm that their users are who they claim to be as the demand for online goods and services grows. Many of them must adhere to strict regulations that differ from country to country, especially in digital banking and money management apps. Others, like ride-sharing apps and gaming platforms, view verifying an identity as a chance to foster customer trust while combating the growing problem of on-line fraud in all sectors of the economy.

Online identity verification is essential for creating safer, more engaging digital experiences, but it hasn't been widely used yet. Identifying one's identity online is frequently difficult from a user-experience (UX) perspective and is known to have a negative impact on account activation rates. Another issue is privacy, as the majority of the market's leading companies are cloud-based providers who handle sensitive data on their own servers. Finally, the market's current solutions frequently fail to confirm the validity of the user's ID document, creating a huge opportunity for fraud.

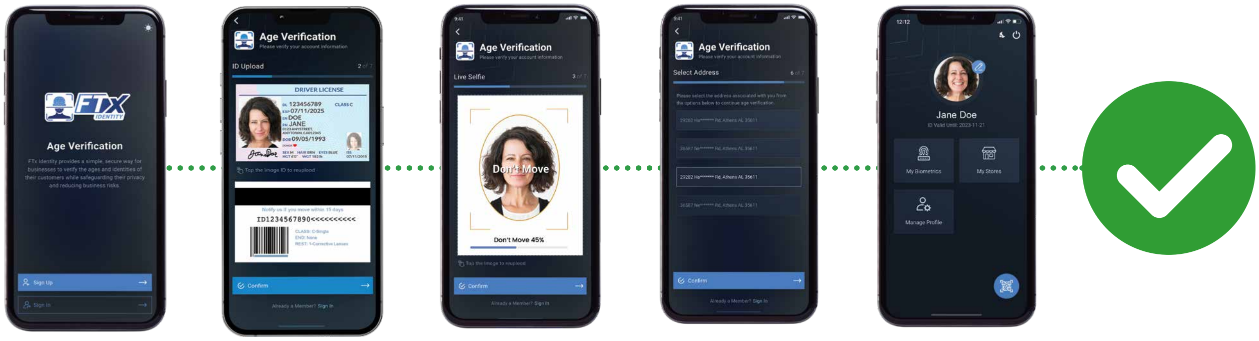
The Need for Identity Verification

The already rapidly growing number of remote workers and shoppers is increasing as a result of the global coronavirus outbreak. Because millions more people were working from home, shopping online, and transacting in other ways in response to the COVID-19 pandemic, almost every business began dealing with an increase in the number of identities they needed to verify online. Almost every remote use case can benefit from an identity proofing solution's combination of robust security and enjoyable user interfaces. Enterprises, consumer marketers, financial institutions, and governmental organizations should investigate contemporary identity proofing. As we go through this ongoing health crisis, the number of identities you need to monitor and verify will rise. After the pandemic completely passes, the population of distant users will also continue to grow as individuals grow accustomed to having constant connectivity.

Identity Proofing: Combining Protection and Usability

You'll hear a variety of responses when asking what identity proofing is. The methodology has, in general, been around for many years. Most of us can recall being asked to confirm our identity by stating the name of our very first dog or other such details. Given the prevalence of hackers, malware, and social engineering, this approach, often known as static PII (personally identifiable information), is far from secure.

These online identity verification methods are problematic because they combine poor security with a bad user experience (friction). Customers frequently lose patience throughout the onboarding process and skip crucial steps like creating new accounts or signing up for new goods and services. Technology suppliers often unintentionally create alluring new opportunities for hackers when they propose solutions to reduce some of that friction. Although some of these early procedures have changed, many of the ID proofing solutions available today are still just marginally improved versions of earlier high-friction/low-security approaches. Therefore, one should inquire


Age Verification
Sign Up
Sign In
Age Verification
Please verify your account information
ID Upload
2 of 7
DRIVER LICENSE
Top the image ID to reupload
Confirm
Already a Member? Sign In
Age Verification
Please verify your account information
Live Selfie
3 of 7
Don't Move
Don't Move 45%
Top the image to reupload
Confirm
Already a Member? Sign In
Age Verification
Please verify your account information
Select Address
6 of 7
Confirm
Already a Member? Sign In
Jane Doe
ID Valid Until: 2023-11-21
My Biometrics
My Stores
Manage Profile

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.

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

Onboarding in a Flash

A contemporary identity verification process is necessary for banks, corporations, government organizations, and other organizations that must promptly and securely onboard a significant number of individuals. And for a smooth user experience, these companies should make sure that an ID proofing solution can be easily connected with their own apps, websites, or other digital properties.

How It Operates:

1. Download an App

Customers, staff, residents, or other users often download your app onto a mobile device with a high-resolution camera. This app includes identity proofing in it.

2. Reputation Check for Devices

Artificial intelligence (AI) capabilities built into mobile apps check that the device being used is not stolen and doesn't have a history of participating in shady business dealings. By doing this, legitimate credentials cannot be stolen.

3. An Official ID Photo

An official identity document, such as a passport, driver's license, or national ID card, must be captured by users. A significant portion of the user's personal data, including name and address, is pre-populated in the customer application form.

4. Verification of Documents

The app evaluates the legitimacy of the document in real-time, and FTx Identity accepts a variety of ID documents from over 180 countries.

5. Take a Selfie

A live image rather than a photo of a photo is ensured using AI technologies.

6. Verifying the Identity

The crucial last step is this one. In order to authenticate the user's identity, effective solutions use AI to compare the selfie and the image on the identity document.

Suitable Areas for Identity Verification

Your users are counting on you to keep their identities safe and are holding you accountable. Users increasingly assume you are responsible for safeguarding their identity and accountable for the consequences of a breach, whether they are accessing financial services, government programs, business VPNs (virtual private networks), or eCommerce websites. Adding layers of the highest assurance security measures makes sense from that perspective.

Unfortunately, if the identity proofing procedure is too difficult, customers will give up on account opening procedures, and employees will find ways to get around security safeguards. Finding a modern solution that provides users with minimal friction and high assurance security is critical.

Examples of use cases are provided below, along with important factors for each:

Opening an Account

Customers are becoming more open to using banks and other service providers without close physical locations. This enables them to compare a greater variety of products with ease. Banks and other customer marketers have an opportunity to make the process of opening an account quick, simple, and secure. For businesses that don't make that transformation, it poses a threat to their ability to compete.

Onboarding New Customers

Strong digital business portfolios are held by banks, retailers, and other customer marketers. The number of competing products and services will increase in tandem with customer connectivity. An effective cross-selling and upselling strategy requires a streamlined onboarding procedure.

Onboarding Employees

By automating the registration of current employees for access to apps, networks, and websites or the onboarding of new employees, the correct identity proofing system will quickly pay for itself.

Streamlining Compliance in Several Aspects

Any organization that employs identity proofing must continually adapt to the changing regulatory environment. The regulators who are committed to safeguarding customers' interests as well as those of financial institutions, businesses, healthcare providers, governmental entities, and other organizations must change along with hackers. The European Union's General Data Protection Regulation (GDPR) created a standard in several ways for safeguarding customers' privacy.

The regulation states in one of the sections that pertains to identities the following: "Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures." Although the rule only applies to customers in Europe, it serves as a standard for other regulatory bodies.

The financial consequences of breaking GDPR can be extremely severe, as the majority of security professionals are aware. Therefore, while looking at identity proofing technology, it's crucial to pick a solution that makes GDPR compliance simple—and is probably going to be compatible with future laws that follow the EU statute.

GDPR Compliance Guidance

Data Retention Procedures

According to GDPR, you can only gather the personal information you require for a given business purpose, and you can only keep the absolute minimal amount of that information for the long term. Look for a solution that erases selfies, PII, and other identity information.

Compliant Algorithms

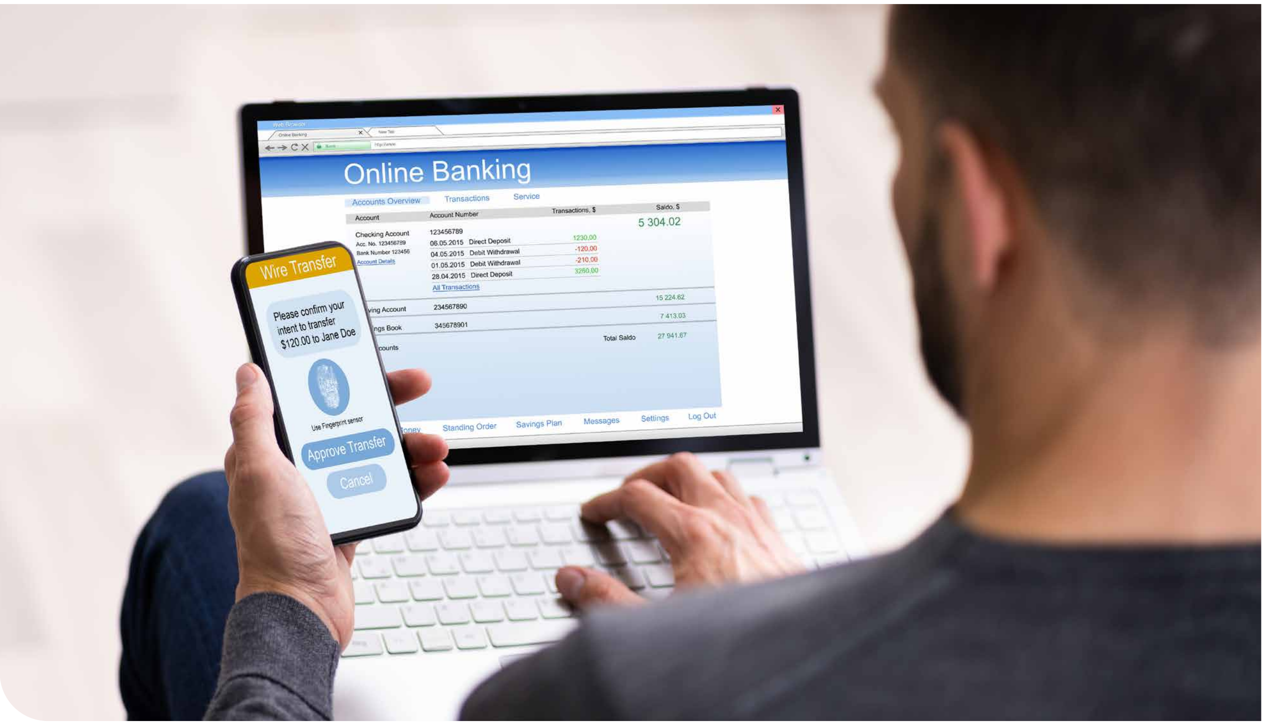
The platform cannot be designed to generate machine learning algorithms by combining data from several customers and prospects. Machine learning tools must only focus on people when used in applications for financial services; they cannot create aggregate models.

KYC and AML for Financial Institutions

Banks and other institutions are required by Know Your Customer (KYC) regulations to confirm the identification of customers before granting them access to financial products and services. The law also addresses methods for determining and monitoring associated risks, frequently in relation to criminal actions like money laundering. Respecting KYC regulations is a high-assurance need. Relying on antiquated techniques and PII won't cut it. Look for a solution that makes use of live facial recognition, biometrics, and device reputation analysis powered by AI. These cutting-edge, high-assurance security technologies are signs of a platform that complies with KYC regulations.

Anti-money laundering

(AML) regulations are made to make it easier for institutions to stop, catch, and report money laundering operations. The rule aims to protect institutions from being unintentionally used for money laundering while also preventing institutions from profiting from unlawful activity. Since AML and KYC are closely related, you should look for many of the same qualities in an identity proofing technology. This incorporates biometrics, live facial recognition, and device reputation analysis, much like with KYC. These characteristics will assist you in reducing the application and onboarding burden for legitimate customers while offering a solid line of defense against fraudulent practices.



Bringing Transaction Security and Continuous Monitoring Together

Your digital business initiatives can be greatly modernized by utilizing identity proofing technology to develop engaging user experiences and implement high-assurance security measures. However, the top identity proofing platforms will keep developing, just like your digital business. They will advance by learning new skills, becoming more intuitive, and expanding their capacities.

Therefore, it's crucial to pick an identity proofing solution that integrates easily with a bigger authentication platform. This method allows you the freedom and flexibility to grow, include use cases, and add security measures as your world changes. For the best security of your customers and your business across the customer journey, combine identity proofing with a more comprehensive authentication platform.

Here are some things you can anticipate from an ideal identification platform that will grow and scale to incorporate these new capabilities:

Identity Verification

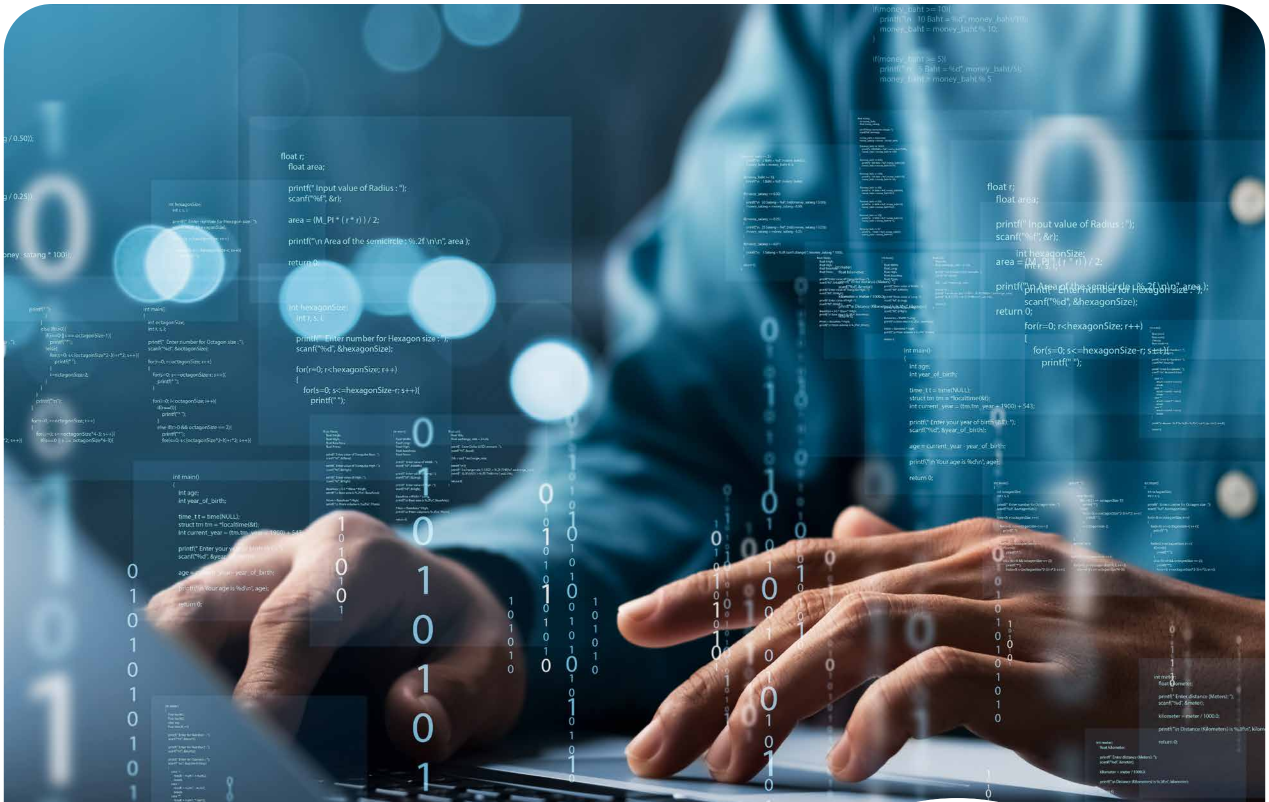
The application and onboarding processes feature a cutting-edge UX and robust security.

Transaction Protection

Protect against man-in-the-middle attacks and other dangers.

Constant Watching

Maintain the confidentiality of authorized identities.



Selecting the Best Technology for Your Business

Everyone agrees that connectivity and mobility have altered how identity is defined and valued. Nothing in the contemporary setting functions without a trusted identity. Employees working from anywhere, customers using mobile devices to access services, and other vital ecosystems all depend on trustworthy identities.

The fact that customer expectations for ease and the sophistication of cyber-attacks are both advancing at the same astonishing rate is a major concern in these ecosystems. Due to all of this change, previous identity definitions and methods of identity authentication are no longer valid.

It will be crucial to keep in mind a few best practices when looking for the perfect identity proofing solution.

Construct a Search Team That is Truly Cross-Functional

The requirement for outstanding customer engagement and robust enterprise security both have an impact on this choice. Members that represent both interests should be included.

Begin by Adjusting Your Idea of Identity

The previous definition and procedures are no longer sufficient. Examine how ideas like decentralized and distributed are changing what constitutes “identity.”

Carry Out Fundamental Research on Customer Preferences

Customers, workers, residents, and other users all have preferences that are influenced by their interactions with other businesses. Keep up with changes in what they desire because they come and go quickly.

Determine the Most Urgent Cybersecurity Threats

In the same way that customer preferences change over time, hacker tactics do as well. To comprehend present and new dangers, collaborate with your security staff.

Discover the Modern Identity and Authentication Elements

The newest elements of trusted identity are biometrics, encryption, device reputation, artificial intelligence (AI), and machine learning. In order to gain a better grasp of these technologies, get in touch with reliable partners.

Analyze the Effects of Important Regulatory Requirements

Regulatory bodies are working to stay on top of important topics including privacy concerns and cyberthreats. Regulations are constantly evolving and posing brand-new problems.

Age Estimation and Age Verification Technologies Around the World

Children who use the internet are susceptible to a variety of online dangers, including cyberbullying, addiction, access to age-restricted content, and the processing of personal data. These might impede their general growth and wellness. In this setting, there has been a push for implementing two key measures to make the internet a safer place for children: providing age-appropriate content and limiting how data fiduciaries can use children's personal information.

It is crucial to employ technological tools to confirm the age of online users before implementing these restrictions. The proposed Personal Data Protection Bill (PDPB), 2019 in India requires data fiduciaries to do age verification and get parental consent before processing children's data in order to provide a legal compliance requirement for this. Additionally, it gives the proposed Data Protection Authority (DPA) the authority to appoint codes of practice for the same. Worldwide, the technology used to confirm an online user's age is developing quickly. An analysis of these developments is essential in light of the PDPB's proposal to require age verification.

Why Age Verification is Important

Through a variety of channels, the internet reaches people from all socioeconomic backgrounds. In the modern world, we are surrounded by internet-enabled gadgets and platforms that we use for a variety of purposes, including education, entertainment, and social contact, just to name a few. Children were using the internet much more frequently when lockdowns brought on by the COVID-19 pandemic were in place. They are using it to access online learning resources, social media, and game apps.

The use of the internet by children can help them be more mentally and socially healthy in general. The internet serves as a formidable instrument for communication and allows children the chance to build solid social networks that can improve their wellbeing. Additionally, it gives children access to many materials that support their mental development. However, children who use the internet are also more susceptible to many forms of online harm, which requires attention. It is vital to categorize the various online risks that children can encounter when using the internet.

Cyberbullying

The act of bullying someone online is known as cyberbullying. This may involve, but is not limited to, intimidating and harassing someone via text messages or other channels, threatening to subject someone to sexual exploitation and abuse, inflicting emotional harm by trolling and making disparaging comments, and coercing someone into posting images or videos online, among other things. Children may occasionally be persuaded to meet the stalker online, which puts them in danger of sexual assault, child trafficking, and so on.

Financial Losses

Financial fraud could be involved. Such frauds can take place while carrying out money transactions on websites for gaming, eCommerce, and other forms of entertainment. This could also apply to situations in which children who get dependent on particular services, like gaming apps, wind up transacting enormous sums of money.

Addiction

Children who have easy access to the digital world are also more likely to become addicted to social media and online gaming. Their overall health is harmed by such addictions, which can also cause sleep problems, mental health issues, and body anxieties.

Age-Restricted Goods, Services, and Content Access

- **Products:** Alcohol, tobacco, etc.

- **Services:** Online gaming and adult services are available on websites and apps, putting children at risk of sex grooming.

- **Content:** Gaming, adult movies, sexual material, etc.

Processing of Personal Information and Ad Targeting

The processing and use of children's personal data acquired by data fiduciaries, such as social media intermediaries, for marketing and product targeting is possible. The information gathered can also be sold or shared with other parties. As a result, there is a very real chance that children's privacy will be violated. In addition, many children may not completely comprehend the notion of data privacy, so even if they give their consent for the use of their data, that consent may not be informed. Therefore, it is important to highlight the principles of data minimization and purpose limitation.

Creating a Safer Environment for Children

In light of the aforementioned online dangers, it is crucial to establish and provide a safer online environment for children and to safeguard their safety and wellbeing. Recent international developments in this area include the introduction of the Kids Internet Design and Safety Act and the Children and Teens' Online Privacy Protection Act in the United States Congress, the release of Age Appropriate Design by the United Kingdom's (UK) Information Commissioner as a code of practice for online services, and consideration of the Online Harms Bill by the UK parliament. Furthermore, a resolution on children's digital rights was also adopted by the Global Privacy Assembly. Children's online gaming apps are now subject to restrictions imposed by the Chinese government.

Due to these developments, a number of data fiduciaries have come under fire, and new information has also revealed how hazardous social media can be for underage users. Since these developments, several of them have begun to take actions like banning marketing directed at minors and providing young users with greater agency. However, age verification has been recognized as a key tool that will force data fiduciaries to implement policies that will give children a safer internet in order to create a strong protective framework against the mentioned online harms.

Furthermore, age verification will enable data fiduciaries to personalize information and content for specific age groups in addition to assisting them in preserving children's personal information and ensuring their safety from online damage. For instance, social media sites could use child safety features to limit the content that children can access, search engines may limit the display of alcohol or cigarette advertisements, or an online gaming company could limit access to its services to a specific time period. While age verification can't guarantee that all children will be protected from all online risks, it does offer a component of the solution that can be used to give them a safer online experience.

Understanding the various age verification options is crucial so that data fiduciaries can choose the best method or set of procedures to apply depending on the situation, such as the socio-economic condition of users, their level of awareness, etc.

The following approaches should be used:

- Have privacy awareness and be mindful of data minimization.
- Easy to use and don’t overwhelm data fiduciaries.
- Don’t restrict the options that the internet offers children.

The aim is to develop an age assurance system that is effective at shielding children from online danger, respects people’s privacy, is simple enough for children to use, is accurate, and is feasible for widespread use.

While some techniques are used to confirm age, others can be used to determine an individual’s age or age range. Age assurance refers to both age estimation and verification. Such technologies are covered in detail in the following section.

Evaluation of Crucial Age Assurance Techniques

Age assurance procedures come in a variety of forms. One approach is to make it a necessity to have an online identifier connected to a government identity proof. Other approaches involve employing technology, such as machine learning and artificial intelligence techniques, to estimate a user's age. A comparison should be done to show off the distinctive qualities of each one while also examining the potential effects on users, particularly their privacy. A flexible solution that can handle privacy issues is attributes-based age verification, which uses the assigned attributes of an individual, such as name, nationality, and so forth, or associated attributes, such as work data, etc.

Three distinct types of attributes exist:

1. **Unchanging Attributes:** These characteristics, such as biological parents, birthdate, birthplace, and distinguishable biometrics (fingerprint, iris), etc., cannot be changed.

2. **Given Attributes:** These are biographical details that have been recorded, such as a person's name, signature, gender, nationality, etc.

3. **Associated Attributes:** These come from interacting with the outside world; for example, employment information, home address, talents, government and financial interactions, internet usage, etc.

Understanding the goals of the technique provides a useful foundation for evaluating the use of these variables for age assurance. Three categories can be used to classify it:

1. **Identification Methods (ID):** Determine the user's actual identity.
2. **Age Verification Methods (AV):** User identification is not required to verify age.
3. **Age Estimation Methods (AE):** Calculating the user's age.

As a result, although using some attributes may result in identification, using others may result in age estimation or age verification. The user's privacy can be protected by conducting transactions using non-identifiable attributes. Additionally, the next section's discussion of new age estimates and verification technologies can help you reduce data collection and protect user privacy.

All of these techniques, however, have their uses, benefits, and drawbacks. The comparison was based on the following parameters:

- **Privacy-Friendliness:** The user should not be identifiable, and the principles of data reduction and purpose limitation must be upheld.

- **Simple for the Child to Use:** A simpler way wouldn't stress children too much.

- **Accessibility and Inclusivity:** Children should be able to use the procedures while taking into account their developmental potential, socioeconomic position, and availability to their parents, among other factors.

- **Degree of Preciseness:** It is crucial that the technique used to verify the user's age can actually determine their age.

- **Possibility of Widespread Implementation:** Considering the level of knowledge in India regarding secure internet access, digital infrastructure, and connection, among other factors, many solutions might not be practical to apply and might result in exclusion. The viability of widespread adoption must therefore be considered.

While privacy-friendliness, child-friendliness, accessibility, and inclusivity are taken into consideration as parameters to capture the interest of younger customers, interest, accuracy, and the feasibility of adoption are taken into consideration as parameters to capture the challenges and viewpoints of date fiduciaries that adhere to the age verification standards.

Based on the aforementioned criteria, we will contrast the various age assurance techniques that are currently available. The comparison will make it clearer how data fiduciaries can employ these techniques to confirm online users' ages and adhere to PDPB 2019 requirements.

Methods of Age Assurance

Method 1

Self-Confirmation/Age Declaration (Age Verification Method)

Users who choose to use this approach must declare that they are older than a specific age range. It is one of the strategies that social networking sites employ the most. The minimum age to use the service is typically 13 years old. In response to the EU GDPR (General Data Protection Regulation), WhatsApp reduced the minimum age to 16 in the European Union region. Users cannot register on these websites or apps by providing an age that is lower than the established age restriction. However, it is dependent on users being truthful and makes the assumption that they are. This approach is not error-free because anyone can check the confirmation box and submit a fictitious age, misrepresenting information. Because a user can defeat the age verification procedures by entering a false age, even if the age verification approach best protects privacy and is economical, it is not strong.

Method 2

Hardline Identification Utilizing Government Identification (Identification Method)

Hardline identification requires the user to present a government-issued form of identification, such as a passport, PAN card, or other document that may be used to verify the user's identity. The aim behind this is to use an existing, massive, centralized database to use government-issued identification to confirm someone's identity. This method provides a high level of accuracy because it uses a person's identification. The data fiduciary/processor gathers all information that can be used to identify a person. It is affordable and simple to scale.

Governments from all across the world have created eID cards. It is a government-approved ID card that provides a citizen with an electronic identity. Use of public services, signature of electronic documents, and identification are all possible with the eID card. An example of an eID card is the Aadhaar card in India.

Different instances of excellent practice, in which the regulator permits gaming companies access to the electronic identification database to cross-check alleged identity details, can be found in countries like Denmark and Spain. Therefore, the data fiduciaries can either conduct a check using the eID card or request that users submit hard copies of their identity documents.

Submitting a Copy of a Government-Issued ID

Identification is needed in order to use some services, such as cryptocurrency trading or making financial transactions on the stock market. Platforms for trading stocks must follow the Reserve Bank of India's (RBI) guidelines. Data fiduciaries frequently ask users to upload selfies of themselves with official identification. Platforms for trading stocks and cryptocurrencies need customers to upload a selfie while carrying their government-issued ID as part of the KYC requirements. The German Federal Supreme Court has ruled that an attempt to employ an age verification system based on an identity card or passport number and the postal code of the city of issue is an effective barrier to preventing minors from accessing age-restricted content online in Germany. A technique like that, meanwhile, does not respect user privacy.

Using an eID Card Issued by the Government

The e-KYC (e-Know Your Customer) process, which identifies a user based upon the centralized stored database Aadhaar, is one of the examples of this technique currently being implemented in India. Telecom operators and fintech data fiduciaries that run payment banks and offer payment wallets (like Paytm, Airtel Money, etc.) are already using the Aadhaar biometric-based e-KYC procedure in India. Users must scan their fingerprints as part of this process at specific stores that provide e-KYC services.

Due to the use of the National Registry identification number, which is incorporated into the eID card and discloses the child's date of birth and gender, it has been claimed that Belgium's eID card is ineffective because it is too invasive and disproportionate. It is crucial to remember that the internet offers a variety of services that do not call for financial transactions, and as a result, identification may not even be necessary. Only age verification is necessary to comply with the PDPB so that data fiduciaries can prevent children from accessing unsuitable content and give them a secure online experience.

Moreover, data fiduciaries do not necessarily need to be aware of a user's identity in order to sell all products, even if financial transactions are to be undertaken in sectors like e-commerce. Once the user has been identified, data fiduciaries and processors are free to use the data however they see fit. While it might save children from harm online, it really invades users' privacy rather than protecting it.

Also, the approach is not ideal because there have been instances where adult online services like OnlyFans have failed to prevent children from using their services, according to reports. Government IDs used as proof of adult status by children as young as 13 have been used to access these services. Additionally, e-KYC cannot be required in order to use every online service (website or app). As a result, this method of identification might not be the most popular and should only be used, as was already indicated, in businesses where it is absolutely necessary.

Method 3

Using Non-Government and Current Online Database for Age Verification/ Identification (Age Verification/Identification Method)

This method makes use of already-in-use internet services that provide a variety of publicly available data. The UK is one country where this is true. In the UK, data aggregators and credit reference agencies cover 85–90% of the adult population, providing a method for identity and age verification that is independent of a single central identity database. This is according to a study done by Victoria Nash, Rachel O'Connell, Bendert Zevenbergen, and Allison Mishkin of the University of Oxford in 2013. Credit card holders here are regarded as adults and are permitted to participate in online gambling.

Combining more authentication techniques can increase success rates, but it can be time-consuming. This method uses a decentralized system and offers a higher level of privacy than the official ID proof identification method. In this case, the procedure may be used for age verification or identity verification, depending on the system being set up. Additionally, it might be economical for data fiduciaries and processors.

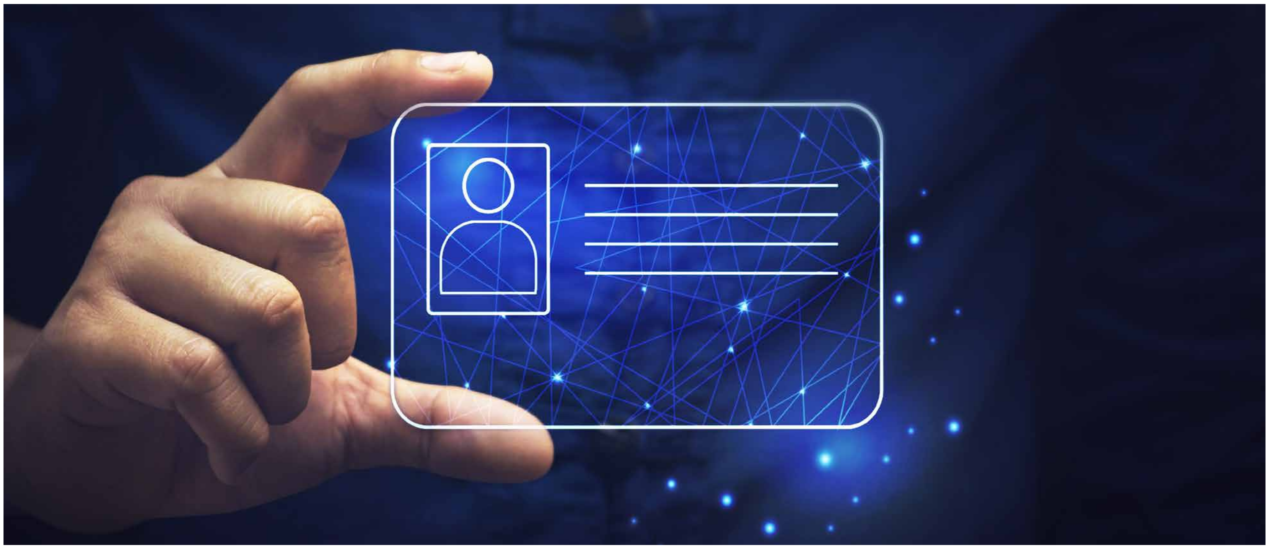
However, as mentioned in the preceding method, this method only works for industries where financial transactions take place. The data fiduciary does not need to be aware of the user's identity in order for them to utilize services like social media and online entertainment. The data fiduciary will have access to the credit/debit card information even if the method is just used for age verification, which is undesirable because it is private and sensitive information. Data minimization is still lacking, so data fiduciaries can use the collected data to target minors with advertisements and other content. The principle of goal limitation is also gravely violated in this situation.

One of the core privacy principles is violated when data that was initially acquired for purposes other than age verification is used. The PDBP has acknowledged the same as a key component. As a result, this practice can be regarded as unfair and may result in the processing of personal data without authorization. The procedure is also not accurate at all.

Even though in the UK credit cards are only issued to those over the age of 18, there are apparent instances in which people under the age of 18 can receive and/or use such credit cards. If someone over the age of 18 pays the bill, an adult can legally give a child under the age of 18 a credit card that is in someone else's name. There have been instances where people under the age of 18 used credit cards to access services, according to reports. Although the retailer lacks a detection system, using a credit card in this situation cannot be reliably used as a proxy for age.

Continued on next page

Additionally, there are issues with this method's practicability. The use of banking information for age verification is not a smart idea, according to banks, which claim that information is requested when creating an account but is not stored in a manner that can be easily accessed. And last, India suffers from a substantial digital divide. A significant portion of people do not own or frequently use credit or debit cards. As a result, the technique cannot be applied to age verification in all situations.



Method 4

Utilizing an eID Card from a Non-Government Third Party for Age Verification/ Identification (Age Verification/Identification Method)

Not all data fiduciaries can access personally identifiable information like names, dates of birth, etc. through this method. The true identity is concealed; in some countries, third-party, non-government eID card issuers exist who confirm a user's identity by validating it against a government-issued ID card. As a result, for the purpose of age verification, the issuer of the eID card acts as a middleman between the user and the data fiduciary.

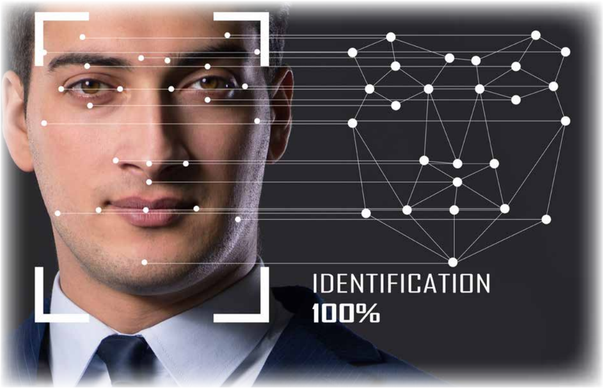
The eID card can be used by users to prove their identity. These services typically continue to be free for users and only charge minimal fees to companies that use them. Businesses are willing to use the services provided by such eID card issuers since they must abide by the regulations governing age verification.

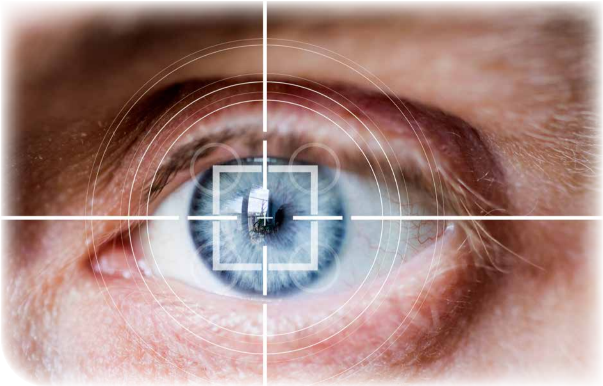
Due to its simplicity, accessibility, and potential for broad adoption, this method has experienced considerable adoption. The process still necessitates the use of official ID proof for identity verification by the third-party eID card issuer company. As a result, someone's privacy is jeopardized.

Method 5

Using Biometrics (Identification/Age Verification Method)

Age verification can also be done via biometrics. According to the criteria for comparison already defined, various types of biometrics could be utilized. They are given below in the table, along with their benefits and drawbacks.





Biometric: Speech

Pros:

- Moderate accuracy
- No extra hardware is needed

Cons:

- Simple to get around
- Low dependability for children 11 to 13 years old

Biometric: Fingerprint

Pros:

- High accuracy

Cons:

- A fingerprint reader is needed
- Minimal anonymity

Biometric: Facial Features

Pros:

- High accuracy
- No extra hardware is needed

Cons:

- Simple to get around

Biometric: Iris

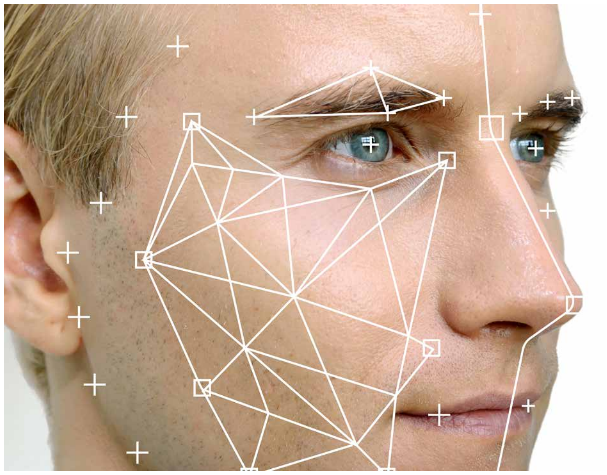
Pros:

- Low accuracy

Cons:

- An iris reader is needed
- Minimal anonymity

Using Unique Biometrics for Hardline Identification/Age Verification (Identification/Age Verification Method)



Biometrics, such as a fingerprint or an iris, are unique and cannot be the same for any two people. So, as was previously described in self-verification method 1, biometric verification can result in a hardline identification. A central database that stores people's biometric data is required for this strategy.

In India, Aadhaar is utilized for this function. However, this procedure violates the idea of protecting a user's privacy and should only be utilized in specific industries that demand such identification. Furthermore, it is extremely unlikely that this could be implemented on a large scale because it requires users to have iris and fingerprint scanners.

A third-party corporation could hold user biometric information and serve as a middleman between the user and the data fiduciary for age verification, much like method 4 in which a third party served as an eID card issuer. In this instance, a decentralized approach is used as opposed to a centralized database kept by the government. Similar to method 4, however, the method only offers a little amount of anonymity and privacy, making it unsuitable. Additionally, because they are simple to hack, biometrics that don't need additional hardware, like speech recognition features, cannot be employed for this purpose.

Features of the Face (Identification/Age Verification/Age Estimation Method)

Identification, age verification, and age estimation can all be done using facial features.

Identification: In this case, it will be necessary to maintain a centralized database. Additionally, this violates the user's right to privacy and goes against data minimization. It doesn't need any additional hardware, which is the only benefit.

Verifying an Age: Similar to method 4, age verification may be carried out by a third party.

Estimating an Age: Algorithms based on machine learning and AI could be utilized to determine the age of users. The following are details:

Creating a digital ID could be one approach for age assessment using facial features. The user is given access if the prediction indicates that their age is above 25.

Continued on next page

If the predicted age falls between 18 and 24, the user is prompted to confirm with official identification. Users are prohibited from accessing improper content if the predicted age is less than 18 years. However, the cloud is used in this instance to analyze the data for age estimation (online). In order to process and determine the user's age, a photo of the user's face is taken and sent to third-party servers.

Even though the third-party company might assert that it doesn't save the user's facial photos, the information nevertheless makes its way to its systems, jeopardizing privacy. Additionally, there are a number of other issues with age assessment using facial traits.

The age of the face depends on one's lifestyle. People with similar ages but different lifestyles will have different-looking faces.

Drug use and psychological stress have an impact on skin texture and color, causing spots and blemishes. Diet, genetic makeup, ethnicity, skin diseases, and cosmetics are among the variables that determine how people perceive their facial aging. Face aging is influenced by exposure to wind and dry air, in general. Wind and a dry atmosphere dehydrate the skin, which causes wrinkles. Additionally, some facial expressions, such as smiling, frowning, showing surprise, and laughing, can leave wrinkle-like lines on certain parts of the face. These lines that resemble wrinkles could be recognized as wrinkles during age assessment, which could affect the accuracy of age estimation.

Degree of Fingerprint Development (Age Estimation Method)

Age can be estimated by using artificial intelligence to analyze the level of development of the user's fingerprint. High degrees of accuracy can be achieved in identifying the user's age group using the method. But once again, data privacy is at risk because the analysis takes place on the servers of the data fiduciaries.

Method 6

Local Device Based Execution of AI and Data Processing for Estimating an Age (Age Estimation)

Most of the approaches that were discussed before this one demand that users either reveal their identities to one party or another or provide their personally identifiable information, including biometrics. Processing of the user's data still takes place on the data processors' cloud servers even if the user is not providing those details, and age estimation is done using facial feature or fingerprint development analysis. Therefore, techniques for storing and processing user data that prevent their personal identity from being revealed to any entity should be devised in order to truly protect privacy.

Edge computing, which stores and processes data on users' devices while protecting their privacy, can be used to achieve this. Data fiduciaries can use a software development kit to include a machine learning-based age estimation algorithm. An API might be developed that can be integrated with any app to make integration easy.

With various types of data, edge computing techniques and artificial intelligence can be applied. The following are some of these:

- Artificial intelligence-based device-level verification utilizing facial recognition and fingerprint development.

- Information obtained from a user's physical actions or interactions with a device (touch data and motion analysis on a device). Information collected from the user's static long-term physical and biometric features.

Method 7

Semantic Analysis and Knowledge-Based Authentication (Age Estimation Method)

Semantic analysis is another technique for age estimation. The process of examining user-written language and determining its age is known as semantic analysis. Users may be asked to respond to various questions by the age estimation software. The user's privacy can also be protected in this way.

It is possible to utilize technology to examine a social media profile or user's behavior to estimate their age range using information provided by their use of an app, service, or platform. The method may not be particularly reliable, though, as it takes a lot of training to get the desired accuracy results.

Method 8

Parental Authority (Age Verification Method)

This approach allows parents to implement parental control while giving their child access to a smartphone or other internet-capable device. They will be able to manage how their children use the device as a result. It gives parents the ability to keep an eye on and manage how their children use their Android or iOS cellphones. Parents can view their children's screen time, among other features. Children could still be exposed to hazardous content since the product might not be able to prevent unsuitable content.

The fact that parents from various socioeconomic situations could have varying perspectives on technology and the internet is a serious matter of concern. Some people might comprehend the dangers of online harm better than others, though. As a result, the layer of parental oversight and consent is similarly thin. The main issue is that children can use technology like VPNs but aren't mature enough to use it responsibly. Although they are responsible, parents lack digital skills.

Parents can also be obliged to disclose more personal information about their children in order to protect their privacy. Some technological advancements could mislead parents into believing that their children are secure online. In addition, technology could be abused for immoral objectives, like keeping tabs on one's spouse.

Conclusion

When it comes to age and identity verification, we at FTx Identity have you covered. Our platform packs a real punch with our integrated login authentication and authorization system, identity management, and effortless age verification. Our age verification technology (AVT) solution interfaces easily with desktop, mobile, and online apps to prevent fraud and the sale of age-restricted products to children. Additionally, your customers will feel satisfied knowing that their information is protected. FTx Identity preserves the security and confidentiality of a customer's data by maintaining it in a cloud-based, guarded digital vault. The information is saved in encrypted form so that only the end user can access their individual profile. Customers have the option to share or unshare their personal information with the businesses they choose, and this information is never disclosed to third parties without their permission.

Looking to experience the best identity verification and age verification platform?

Get in touch with us to set up a consultation and schedule a demo with one of our specialists.