

HELP GUIDE

Secure Identity Verifications in Account Enrollment

Secure and streamlined account openings — without the fraud risk



As fraud continues to grow, identity verification helps you stay safer

According to the 2022 Data Breach Report from the Identity Theft Resource Center, healthcare and financial services were the most targeted industries in cyberattacks. The personally identifiable information most frequently stolen were names, Social Security numbers, dates of birth, current home addresses, and government ID credentials.¹

With that personal identifiable information, fraudsters can create new accounts with a synthetic identity and counterfeit ID to execute acts of sabotage and theft that take years to recover from. They can decimate remaining security defenses, wreak havoc on operations and even destroy a company's reputation.

Cutting-edge identity verification (IDV) technology offers businesses a fighting chance against fraud's growing pervasiveness. By systematically verifying each user's identity during the account enrollment process — even before onboarding — you can encourage user conversion and avoid transaction abandonment, while remaining compliant with any regulations.

The Impactful Role of Identity Verification Technology in Account Enrollment

Prevents Fraud: Stops fraudsters and the monetary loss associated with identity theft and account takeover.

Promotes Conversion: Promotes conversion and reduces abandonment. Companies realize up to a 6.6x return from new users and successful transactions.²

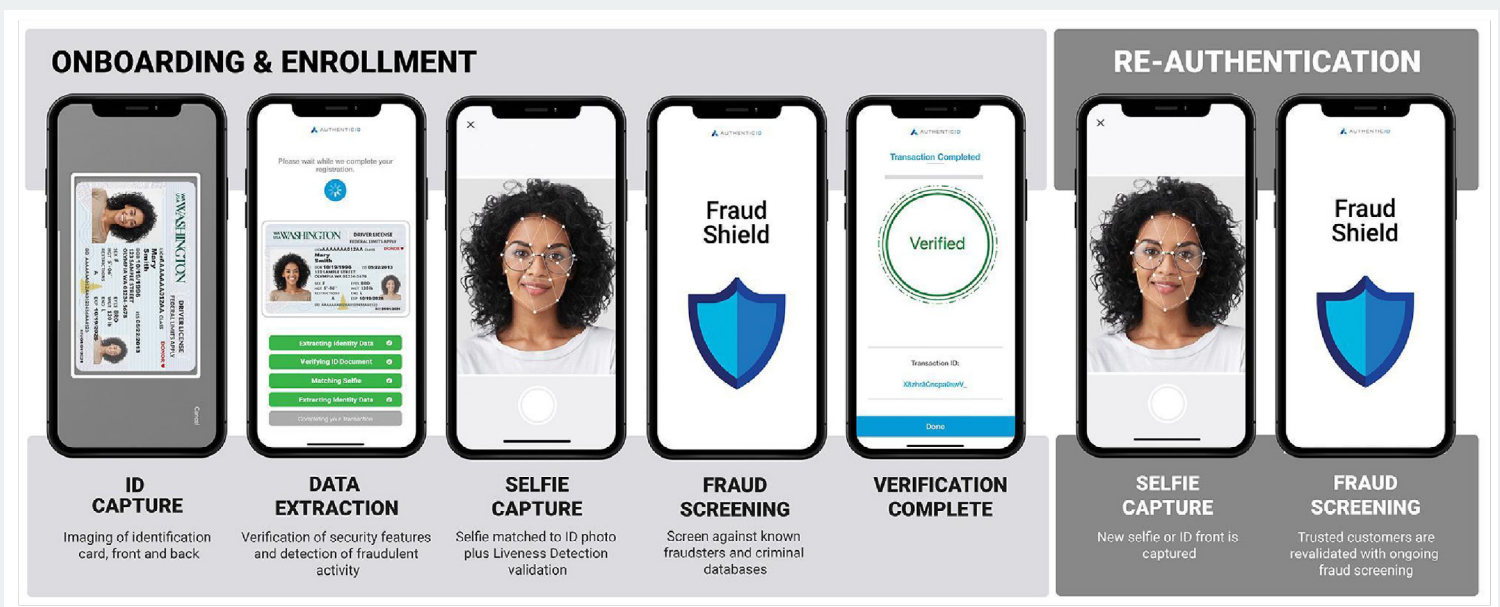
Ensures Compliance: Mitigates global compliance risk and regulatory fines associated with Know-Your-Customer (KYC) guidelines.

Boosts Operational Efficiency: Leveraging automated identity verification reduces the need for teams to verify users at account opening manually.

How Identity Verification Works in Onboarding and Enrollment: Easy, streamlined and protected

In the application and account enrollment phase, keeping bad actors out while allowing good customers in is crucial to growing your business. But balancing security and user experience is often difficult. Using a friction-smart identity verification solution can provide customers and your company the security and experience they're looking for.

Below is a sample workflow of the AuthenticID ID Verification Solution for Enrollment:



- First the user captures an image of a government issued ID. The ID is analyzed by proprietary AI and machine learning technology that uses over 2000 computer vision models to verify its authenticity in seconds.
- Once the ID is analyzed the user captures a selfie. The biometric data is matched to the government-issued ID to ensure the person taking the picture is in possession of the ID. Liveness detection is used to ensure the person taking the picture is doing so in realtime to prevent spoofing.
- When fraudsters or counterfeit IDs are detected, faces and identification data can be added to Fraud Shield watchlists to protect future attacks.

Industry Use Cases for Identity Verification in Account Enrollment

Next-gen identity verification holds significant advantages across diverse industries, offering a multitude of benefits to both businesses and consumers. Ranging from enhancing security to driving financial savings, its impact is far-reaching and transformative.



Government

Preventing unauthorized access to key resources and verifying individual benefit eligibility.



Financial Services

Verifying account enrollees for KYC and AML compliance.



Retail

Mitigating chargeback fraud on high-cost purchases and safely selling age-restricted products.



Healthcare

Keeping patient data private and upholding HIPAA compliance.



Telecom

Preventing SIM Swap, account takeover fraud and other common scams.



Gaming

Ensuring geographic jurisdiction and age verification rules requirements are met for players.



Sharing & Gig Economy

Build trust and ensure safe interactions in online marketplaces and shared service programs.

Customer-centric verification enrollment checklist

Ready to implement identity verification into your enrollment process? Here's a checklist to ensure it's friction-free and robust enough to do the job:

Is the transaction time quick enough to avoid abandonment?

How many attempts does it take for users to verify their identity, and is there an information extraction tool to cut down manual entry?

Is your technology/process removing bias from decisions?

With automated, **AI-driven technology**, biases can be eliminated and true identity verification can shine through.

Is your technology tracking for comprehensive signs of fraud?

Do you have a black list for failed verifications to help avoid:

Spoofing

Material Analysis

False PII Data

Security feature analysis

Computer generated signatures

Behavioral data analysis

Is the data secure and complying with retention policies?

Consider how vetted and verified your employees are on the other side of your identity verification software; what **types of credentials** would you qualify for?

Fraud protection at every touchpoint

Fraud prevention doesn't end after someone signs up within your system. After account enrollment and onboarding, it's critical to implement additional measures to supplement any Identity Verification solution. Options for this further layer of protection include processes such as Step Up Authentication, non-legacy multi-factor authentication, continuous authentication and reauthentication. Whichever method you choose, continued vigilance is necessary for effective security and breach mitigation.

Not all authentication methods are created equal, which is why we curate your solution to your business, industry and expectations. We can help ensure that the sophistication you need for your onboarding process is up to the standards set by both the government and your customers.

Sources:

1. https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf
2. <https://www.authenticid.com/liminal-report-2023/>
3. <https://www.csoonline.com/article/574877/legacy-password-based-authentication-systems-are-failing-enterprise-security-says-study.html>
4. <https://www.dowjones.com/professional/risk/glossary/know-your-customer/>

To learn more about Secure Identity Verifications in Account Enrollment, visit our website or [schedule a demo](#) today.