AUTHENTICID

A GUIDE TO IMPLEMENTING

Identity Verification in Financial Institutions

Table of Contents

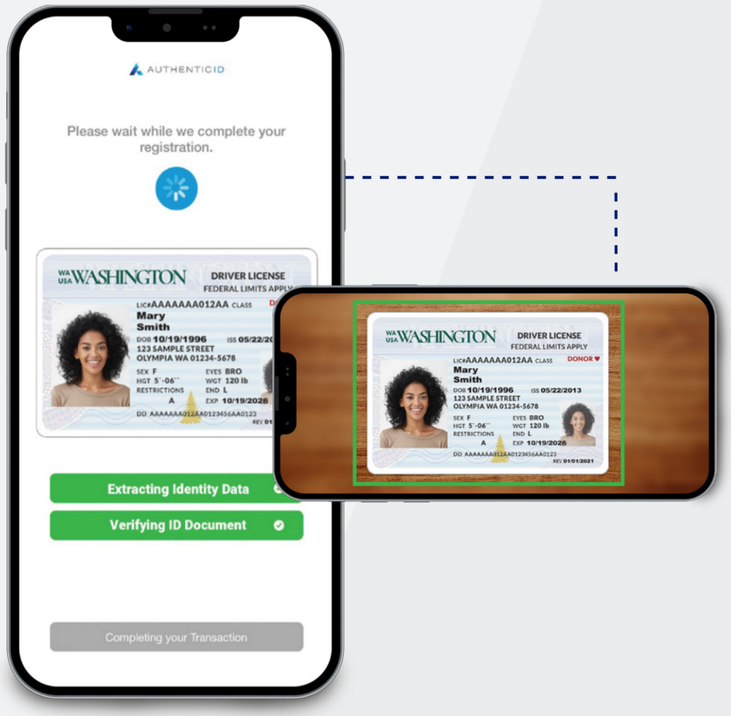
AUTHENTICID

Gaining the Most ROI Out of Your Identity Investment

Ensuring that any investment in your business delivers tangible results is vitally important. Implementing your identity verification platform is no different: it's a crucial aspect of doing business.

Why? The continued risks of doing business online mean that your identity verification system is more important than ever. More and more customers prefer doing business online, and fraudsters have caught on.

As a result, regulations continue to change, and new business challenges will emerge. Setting your business up for success is critical.



AuthenticID software offers protection against fraud through ID verification and biometric authentication. Our solution is driven by proprietary AI and machine learning technology that ensures accurate, quick results.

Our extensive industry experience will help you implement your identity verification software to maximize your ROI. That means you'll stay compliant, prevent fraud, improve your customer experience, and build trust with your customers.

This guide aims to help you implement a robust identity management and security solution to ensure business continuity and customer loyalty.

AUTHENTICID

Assembling the Right Team

Fraud and risk personnel who are critical to the entire process: from identifying fraud vectors and threats, to tuning systems for specific business needs, to defining success metrics.

Your strategy and risk team will consist of several important pieces to this puzzle:

- **Fraud & risk personnel** who are critical to the entire process: from identifying fraud vectors and threats, to tuning systems for specific business needs, to defining success metrics.
- **Information technology & security personnel** to build cloud infrastructure and protect online banking system data.
- **Compliance & regulation staff** to maintain regulatory compliance.

Your customer-focused team will bridge the gap to user experience:

- **UX Designers** to develop a user-friendly digital experience.
- **Customer Service Associates** to assist users with any potential issues.

AUTHENTICID

Gather Data Intelligence

Financial institutions face many challenges and shifts within the industry that force institutions to constantly reevaluate their priorities and how to protect sensitive information. Data intelligence includes understanding current tech and optimization needs, security certifications, and any relevant data retention policies.

Take inventory of the fraud threats and breaches the institution has experienced in the past year or even in the last quarter. Which fraud types are most prevalent and how can you shift your policies to reduce these issues in the future? This could include education and further safeguarding your most vulnerable data intel.

Businesses should have cybersecurity education measures in place for employees, vendors, and potential customers as part of their fraud prevention solution and identity verification. Offering online intelligence courses, blogs, and other content to everyone involved with your institution can help prepare them for greater protection.

Additionally, consider the type of security and verification solution you need to meet the demand of your customers. To answer this, think about where and how your customers interact with your institution - online, in branch, or through an app.

Tip: Build an omnichannel strategy that will break down identity data silos between channels and departments. With data orchestration, you'll create a more holistic, real-time profile of each good customer and bad actor for actionable insights.

AUTHENTICID

Financial Compliance and Regulations

Without proper protection, your financial institution could experience what Danske Bank did in 2022: They forfeited $2 billion and lost the trust of their customers after they were found to have defrauded U.S. banks through violations of AML regulations.

The institution failed to take stock of where its online banking system was vulnerable to attack and implement viable changes to protect that data.

Government regulatory requirements that can impact the configuration of your identity verification solution:

- Know Your Customer/Anti-Money Laundering (KYC/AML)
- California Consumer Privacy Act (CCPA), originally published in 2018 to improve privacy rights and protect consumers
- General Data Protection Regulation (GDPR), a data privacy and security protection law in E.U.
- Payment Services Directive Two (PSD2), an E.U. regulation for electronic payment services for online transactions
- Payment Card Industry Data Security Standard (PCI DSS compliance)

AUTHENTICID

Moving Through Customer Journeys

Identity verification (IDV) is used in a variety of touchpoints in customer, employee, or vendor onboarding. It can also be implemented as part of reauthentication processes after customer sign-up. Here are the most common points during the user journey that may be vulnerable to fraud or cyber breaches and identity verification should be implemented:

- In-branch retail withdrawals or check cashing
- Digital, or call center sign-up
- Enrollment and onboarding
- ID and selfie validation for KYC
- High-value purchases
- Account Changes
- PII Data consent releases
- Loan Applications
- Ongoing facial biometric re-authentication

A Layered Approach to Identity Verification

As you consider how to protect your customers, you may come to realize that there are multiple ways of verifying someone is who they say they are. The more layers of protection you add to your verification process the stronger your shield becomes against fraud attacks.

LAYER ONE: DOCUMENT VERIFICATION

Using only their ID as verification; users take a photo of their government-issued ID or another document. The goal is to capture, extract, and analyze ID data in order to authenticate these identity documents.

LAYER TWO: BIOMETRICS

Adding in biometric authentication + photo document verification; users submit a real-time selfie or series of selfies, which are then analyzed for liveness and are often compared against a government-issued photo ID.

LAYER THREE: DATA ENRICHMENT

Include third-party APIs + biometric authentication + ID verification; utilize databases like credit bureaus, phone carriers, etc. to verify identity datapoints.

AUTHENTICID

Determine Your Risk Tolerance

"Risk tolerance" focuses on the acceptable level of variation around risk objectives. This is a measurement of exactly how much of a loss you are willing to experience given your existing assets.

"Risk appetite" represents the level of risk that the organization is prepared to accept. Setting fraud risk appetite requires understanding your institution's threshold for different types of fraud.

Both risk tolerance and risk appetite set boundaries of how much risk an entity is prepared to accept.

HOW TO CUSTOMIZE YOUR IDENTITY VERIFICATION SOLUTION

Ask yourself these questions:

- How do we balance customer experience and satisfaction levels while providing security that doesn't inconvenience the end user?
- How do we ensure our fraud prevention and identity verification measures can stay agile and accommodate any new growth, products, or channels?
- How can identity verification help organizations facilitate "smart" growth?
- What level of support should our identity verification vendor deliver to our organization?
- What legacy systems do we have in place that might need replacement? What does the replacement look like in terms of time and cost?

The answer to these questions will depend on your customer needs and compliance requirements.

AUTHENTICID

Set Your KPIs or Success Factors

Understanding what makes your identity verification solution successful will help evaluate your system and support more seamless user experiences. Here is a look at what you should consider measuring:

FALSE REJECTION RATE (FRR)

The percentage of customers that are wrongly rejected. The goal for this metric is to keep it as low as possible to ensure high customer satisfaction.

FALSE ACCEPTANCE RATE (FAR)

On the opposite side of approval rates, FAR measures how many fraudulent accounts were accepted. Keeping this metric low can help improve the safety of your website.

FIRST-TIME PASS RATE

This metric measures the number of users that get through the verification process on the first try, without the need to recapture an image. A high first-time pass rate improves the user experience and reduces abandonment. AuthenticID has an industry-leading, 94.07% first-time pass rate.

APPROVAL RATE

This measures how many transactions were authentic and accepted accurately. This will depend on incoming traffic and should be monitored for optimization opportunities.

FRAUD REJECTION ACCURACY

Also known as Precision, this is the measure of how many accounts were rejected that were actually fraudulent.

BIAS

Ensure the risk of bias in your system is managed by tracking the size, completeness, relevance, and diversity of your ML training data sets on a regular basis. Measure whether certain algorithms exhibit bias in acceptance and rejection rates.

When evaluating solutions, consider an identity verification vendor that offers a platform with real-time reporting and dashboards.

AuthenticID is Your Trusted Identity Verification Partner

AuthenticID's platform offers the secure, trusted technology you need to keep your business and customers safe. Security is in everything we do: we exceed InfoSec and legal process compliance standards to secure data, including meeting SOC 2 Type 2 and ISO27K security and performance certifications. Through our channel network, our technology has passed Level 2 Presentation Attack Detection (PAD) liveness tests.

Each year AuthenticID is rigorously audited by independent third-party companies as well as government bodies to prove that we comply with global and regional standards. That's why we're trusted by the United States government and many of the world's largest banks.

Fraud will continue to get more sophisticated as customers continue to demand a more streamlined and secure system. By implementing AuthenticID's identity verification solution, your business can keep customers happy while stopping fraud in its tracks.

Sources

https://www.dnb.nl/en/publications/research-publications/working-paper-2020/693-trust-in-financial-institutions-a-survey/

AUTHENTICID

For more information on our platform, request a demo today.