

GUIDE FOR FINANCIAL SERVICE PROVIDERS

veriff 

Staying Internationally
IDV Compliant

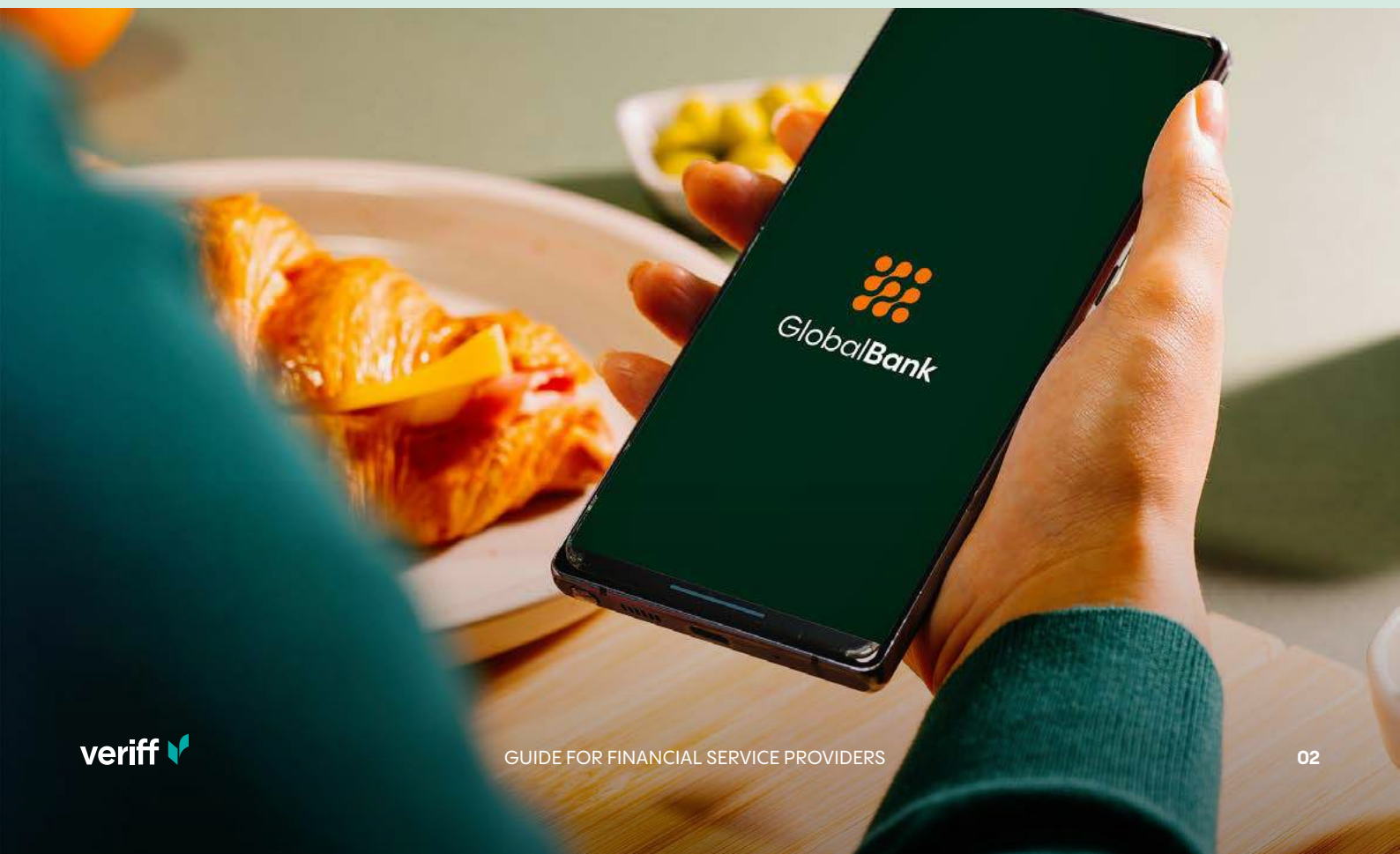


Introduction

Why IDV Matters for Financial Service Providers: For financial service providers (finserv), identity verification (IDV) is not a standalone regulation but a cornerstone capability that enables compliance with international Anti-Money Laundering (AML), Know Your Customer (KYC), and Counter-Terrorism Financing (CTF) requirements. These obligations are critical for preventing money laundering and terrorism financing, and IDV provides the foundation for meeting them effectively.

For startups and small and medium businesses (SMBs), navigating these regulations can feel overwhelming. Yet compliance is more than avoiding fines—it's about protecting your business, building customer trust, and ensuring you're not inadvertently enabling financial crime. Beyond AML and CTF obligations, robust IDV also helps reduce fraud risk, further strengthening operational integrity and safeguarding long-term growth.

Disclaimer: This guide is for informational purposes only and is tailored to financial service providers (finserv). It does not constitute legal advice. Always consult qualified legal counsel in each jurisdiction where you operate to ensure full compliance with applicable laws and regulations.



Contents

1

The Basics of IDV for Financial Service Providers

page 04

2

The Global Standard for IDV Compliance: FATF

page 05

3

A Simple 5-Step Framework for Compliance in Financial Services

page 06

4

Regional Regulations for Financial Service Providers

page 14

5

Conclusion: Simplifying Compliance, Strengthening Trust

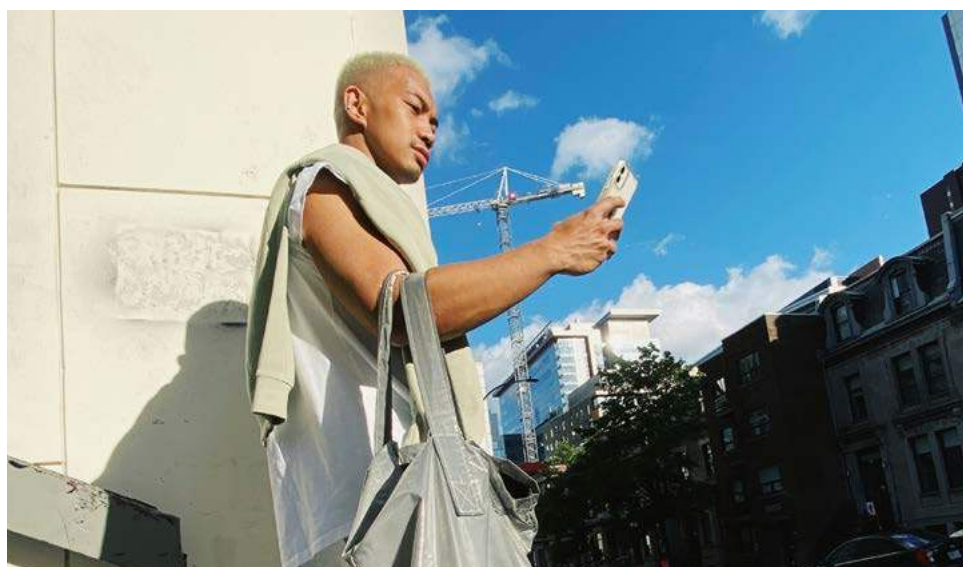
page 15

1 THE BASICS OF IDV FOR FINANCIAL SERVICE PROVIDERS

Identity Verification (IDV) is a cornerstone for financial service providers in meeting their regulatory obligations. It underpins compliance with three key pillars:

- **Anti-Money Laundering (AML):** Refers to a broad set of laws, regulations, and obligations designed to prevent criminals from disguising illegally obtained funds as legitimate income. Financial service providers rely on IDV to implement AML measures such as customer identification, transaction monitoring, and reporting suspicious activities.
 - **Know Your Customer (KYC):** Requires financial service providers to verify the identities of their customers, assess risk profiles, and monitor ongoing activities. IDV is fundamental to KYC, ensuring accurate identity checks that support AML and CTF compliance.
 - **Counter-Terrorism Financing (CTF):** To prevent the flow of funds to terrorist organizations, financial service providers must screen customers against sanctions and politically exposed persons (PEP) lists. IDV enables these checks by validating identities and supporting effective monitoring.
- Why It's Important for Financial Service Providers:

Non-compliance can result in severe penalties, including fines, reputational damage, and loss of operating licenses. A strong IDV program not only protects your business but also builds trust with customers and regulators.



2 THE GLOBAL STANDARD FOR IDV COMPLIANCE: FATF

The Financial Action Task Force (FATF) is an intergovernmental body that sets the international standard for AML and CTF compliance, specifically for financial service providers. FATF's 40 Recommendations provide a framework for countries to develop their own AML/CTF laws and regulations. Understanding and aligning with these recommendations is critical for global compliance.

Key FATF Principles for Financial Service Providers:

- **Risk-Based Approach (RBA):** Financial institutions must focus compliance efforts on high-risk customers, products, and geographies. For example, customers in high-risk industries like cryptocurrency or from FATF "grey" or "black" list countries require enhanced due diligence (EDD).
- **Customer Due Diligence (CDD):** Financial service providers must collect and verify customer information, including beneficial ownership details for businesses. Monitoring customer activity to ensure it aligns with their stated purpose is also critical.
- **Record-Keeping:** Financial institutions are required to maintain verification records for at least five years after the business relationship ends. These records must be accessible for audits or investigations.

Note: Customer Due Diligence

Digital ID systems (such as government-issued digital identity documents or national identity databases) can streamline compliance by providing trusted identity credentials. Biometric verification and liveness detection are complementary technologies that help confirm that the person presenting the credential is real and matches the identity. Together, these tools enhance the efficiency and security of CDD processes.



3 A SIMPLE 5-STEP FRAMEWORK FOR COMPLIANCE IN FINANCIAL SERVICES

STEP 1 ASSESS YOUR RISKS

Start by identifying the specific risks your business faces. Consider these four areas (Risk-based Approach):

Customer Risk

- **High Risk:** Politically Exposed Persons (PEPs), high-net-worth individuals, or customers in cash-heavy industries.
- **Low Risk:** Local government agencies or publicly traded companies.

Geographic Risk

- **High Risk:** Customers from countries on FATF's "grey" or "black" lists.
- **Low Risk:** Customers from well-regulated jurisdictions (e.g., FATF member countries)

Product/Service Risk

- **High Risk:** Products that allow anonymity or high-value transactions (e.g., crypto wallets).
- **Low Risk:** Basic savings accounts with low transaction limits.

Channel Risk

- **High Risk:** Non-face-to-face onboarding or use of third-party agents.

In-person onboarding isn't foolproof

- A fake physical ID can be presented just as easily as a fake digital one. The "security" of in-person is often overstated.

What to Do: Create a risk-scoring system to categorize customers as low, medium, or high risk. Apply the appropriate level of diligence:

- Simplified Due Diligence (SDD): For low-risk customers.
- Standard Due Diligence (CDD): For most customers.
- Enhanced Due Diligence (EDD): For high-risk customers, including additional checks like verifying the source of funds.



STEP 2 COLLECT AND VERIFY CUSTOMER INFORMATION

The specific requirements for collecting and verifying customer information are heavily influenced by local AML laws and regulations. While there are common global practices, such as those outlined by FATF, each jurisdiction may impose additional or unique requirements. Financial service providers must ensure their processes align with the specific laws in the countries where they operate. Always consult legal counsel to confirm compliance with local regulations.

Collect the Basics

At a minimum, financial service providers are generally required to collect the following customer information

- Full Legal Name
- Date of Birth
- Address
- Government-Issued ID Number

Verify Their Identity

- Use document verification tools to check the authenticity of IDs.
- Use biometric verification (e.g., selfies with liveness detection) to confirm the person matches the ID.
- Cross-check customer data with trusted databases (e.g., government registries, credit bureaus).

Identify Beneficial Owners (UBOs)

- Verify their identities using the same steps as individual customers.
- Be aware that some jurisdictions may have stricter thresholds for identifying UBOs or additional requirements for documenting ownership structures.



Note: Collect the Basics

The exact information required may vary depending on local AML laws. For example, some jurisdictions may require additional details, such as tax identification numbers or proof of income, while others may have simplified requirements for low-risk customers.

STEP 3 SCREEN AND MONITOR CUSTOMER

Sanctions and PEP Screening

- Check customers and UBOs against global sanctions lists (e.g., OFAC, UN, EU) and PEP databases using specialized AML screening tools. Identity verification (IDV) software can be integrated into this process to ensure that the person being screened is genuinely who they claim to be.

Ongoing Monitoring

- Continuously monitor customer activity for red flags, such as unusual transaction patterns or high-value transfers. Set up alerts for suspicious behavior.

Sanctions and PEP Screening

- Check customers and UBOs against global sanctions lists (e.g., OFAC, UN, EU) and PEP databases using specialized AML screening tools. Identity verification (IDV) software can be integrated into this process to ensure that the person being screened is genuinely who they claim to be.

Ongoing Monitoring

- Continuously monitor customer activity for red flags, such as unusual transaction patterns or high-value transfers. Set up alerts for suspicious behavior.

STEP 4 STAY COMPLIANT WITH DATA PRIVACY LAWS

- Collect only what's necessary (data minimization).
- Securely store data with encryption and access controls.
- Be transparent with customers about how their data is used.

STEP 5 USE IDV SOFTWARE TO SIMPLIFY COMPLIANCE

IDV software automates compliance processes, including CDD, EDD, and ongoing monitoring. Platforms like Veriff streamline identity verification, fraud detection, and reporting.

How IDV Software Works: IDV software automates and enhances the identity verification process by leveraging advanced technologies and workflows. Here's a step-by-step overview of how it typically operates:

1. Customer Onboarding

The software integrates with a company's onboarding process (e.g., website, app, or API) to collect customer information and documents during account creation or service registration.

Customers are prompted to upload government-issued IDs, take selfies, or provide other required documentation.

2. Document Verification

The software uses optical character recognition (OCR) and AI-driven algorithms to extract and analyze data from uploaded documents (e.g., passports, driver's licenses, national IDs).

It checks for authenticity markers like holograms, watermarks, MRZ codes, and font consistency to detect forgeries or tampering. For documents with embedded chips (e.g., ePassports), NFC technology is used to read and validate chip data, ensuring that printed and digital information align securely.

3. Biometric Verification

Customers are asked to take a selfie or record a short video. The software uses facial recognition and liveness detection to ensure the person is real and present (not a photo, mask, or deepfake).

The selfie is matched against the photo on the ID document to confirm identity.

4. Database Cross-Referencing

The software cross-references customer data with trusted databases, such as:

1. Government registries, **2.** Credit bureaus, **3.** Global sanctions lists (e.g., OFAC, UN, EU), **4.** Politically Exposed Persons (PEP) lists.

This step ensures the customer is not flagged for high-risk activities like money laundering or terrorism financing.

5. Reporting

The software generates detailed audit trails and reports, documenting every step of the verification process.

These reports are stored securely and can be retrieved for regulatory audits or investigations.

6. Ongoing Monitoring

Many IDV platforms offer real-time transaction monitoring and periodic re-verification to ensure ongoing compliance.

Alerts are triggered for suspicious activities, such as unusual IP addresses, high-value transactions, or changes in customer behavior.

What IDV Software Does to Help Companies Stay Compliant

IDV software addresses compliance challenges by automating complex processes, reducing human error, and ensuring adherence to global and regional regulations. Here's how it helps:

1. Automates Compliance with AML/KYC/CTF Regulations

Customer Due Diligence (CDD):

IDV solutions help financial service providers collect and verify required customer information (e.g., name, date of birth, address, ID number) in line with regulations such as FATF Recommendation 10, the USA PATRIOT Act, and the EU's AMLD6.

Example: Veriff's platform verifies government-issued IDs, matches them with customer-provided data, and also supports non-document verification through government databases where available.

Enhanced Due Diligence (EDD):

For high-risk customers, IDV platforms enable additional checks such as screening against politically exposed persons (PEP) and sanctions lists, and conducting adverse media searches. These capabilities strengthen AML and CTF compliance, though financial service providers remain responsible for implementing broader due diligence measures beyond identity verification.

Ongoing Monitoring:

Ongoing monitoring, as envisioned under FATF Recommendation 1 (Risk-Based Approach), involves the continuous review of customer transactions and financial behavior to identify suspicious activity or changes in risk profiles. While not all IDV platforms directly monitor transactional activity, they play a critical role in enabling ongoing monitoring by ensuring that customer identity records remain accurate and up to date. By allowing organizations to refresh and update IDV data in a timely manner, these platforms support compliance efforts and strengthen the broader monitoring framework.

- Ongoing monitoring requires scrutiny of transactions and customer financial behavior.
- IDV platforms do not typically monitor transactions themselves.
- Instead, they facilitate ongoing monitoring by enabling timely updates to identity records.
- This capability helps organizations maintain accurate risk profiles and meet compliance obligations.

2. Ensures Adherence to Data Privacy Laws**Data Minimization:**

IDV software collects only the data required for compliance (e.g., the “minimum four” PII: name, DOB, address, ID number). Collected data should align with applicable data privacy laws like GDPR, LGPD, and CCPA.

Secure Data Storage:

Platforms like Veriff use end-to-end encryption and access controls to protect sensitive customer data. They also comply with data retention requirements (e.g., 5 years under FATF) and securely delete data after the mandated period.

Purpose Limitation:

IDV software ensures that customer data is used solely for compliance purposes, preventing unauthorized use for marketing or analytics.

3. Ensures Adherence to Data Privacy Laws**Multi-Jurisdictional Support:**

IDV platforms are designed to assist financial service providers in meeting compliance obligations across multiple jurisdictions. They provide the tools needed to support requirements such as:

1. FATF Recommendations (global standard),
2. FinCEN CDD Rule (U.S.),
3. AUSTRAC Rules (Australia),
4. MAS Notices (Singapore)

Language and Localization:

Many platforms support multiple languages and adapt to local document types, making it easier to onboard customers globally.

For example, Veriff supports document verification across more than 230 countries and territories, offering broad coverage of local ID types. While this capability enhances onboarding reach, financial service providers remain responsible for ensuring compliance with all applicable local regulatory frameworks beyond IDV.

4. Enhances Fraud Detection and Prevention**AI and Machine Learning:**

IDV software uses advanced algorithms to detect fraudulent documents, synthetic identities, and abnormal behavior patterns.

Example: Veriff's AI can identify subtle inconsistencies in document fonts, holograms, or MRZ codes that may indicate forgery.

Biometric Verification:

Liveness detection ensures that the person being verified is real and present, reducing the risk of impersonation or deepfake attacks.

Technical data analysis:

Some platforms analyze user behavior to identify potential fraud.

5. Provides Audit Trails and Reporting**Regulatory Reporting:**

IDV software generates detailed reports that document every step of the verification process, including timestamps, risk scores, and verification results. These reports are critical for regulatory audits and investigations.

Audit Trails:

Platforms maintain secure logs of all customer interactions, ensuring transparency and accountability.

6. Scales with Business Needs**Flexible Integration:**

IDV software integrates seamlessly with existing systems via APIs, making it easy to scale as customer volumes grow.

Example: Veriff's API allows businesses to embed IDV workflows directly into their apps or websites.

Customizable Workflows:

Companies can tailor verification workflows to align with industry-specific requirements. For financial service providers, this flexibility enables organizations to define the checks, risk flows, and verification steps needed to meet regulatory obligations and internal risk policies. By customizing workflows, Financial service providers can ensure that identity verification supports AML, KYC, and CTF requirements while adapting to their unique compliance and customer onboarding needs.

Real-Time Verification:

Automated processes enable instant verification, reducing onboarding times and improving customer experience.

Key Features of Veriff's IDV Platform

Global Coverage:

Support for over 230 countries and territories and multiple document types.

AI-Powered Verification:

Advanced fraud detection and document analysis.

Biometric Liveness Detection:

Ensures the person being verified is real and present.

AML Screening Support:

Provides identity verification and screening capabilities that help financial service providers meet obligations under FATF, AMLD6, FinCEN, and other regulations. Compliance responsibility remains with the provider.

Secure Data Handling:

End-to-end encryption, access controls, and transparent data retention schedules.

Customizable Risk Scoring:

Tailored risk assessments based on customer profiles.



4 REGIONAL REGULATIONS FOR FINANCIAL SERVICE PROVIDERS

1. European Union

6th AML Directive (AMLD6):

Requires UBO identification and centralized UBO registers.

GDPR:

A specific law emphasizing secure storage, data minimization, and transparency.

GDPR:

A cornerstone regulation emphasizing secure storage, data minimization, and transparency in handling personal data. For practical guidance, see Veriff's ["Understanding the seven key data protection principles of GDPR"](#).

2. United States

USA PATRIOT Act:

Mandates a written Customer Identification Program (CIP).

FinCEN CDD Rule:

Requires UBO identification and verification.

U.S. Data Privacy Laws:

Cover consumer data protection, including state-level frameworks such as CCPA and federal sectoral laws (see Veriff's ["Ultimate guide to US Data Privacy Protection Laws 2025: Stay secure with Veriff"](#))

3. Australia

AML/CTF Act:

IDV must be completed before providing services.

AUSTRAC Rules:

Encourage the use of digital IDV systems.

Privacy Act 1988 (AU): Governs handling of personal information, including principles for collection, use, and disclosure (see [Privacy Act 1988 \[Cth\]](#)).

4. Singapore

MAS Notices:

Allows post-onboarding verification with risk controls.

PDPA:

Focuses on data privacy compliance.



5 CONCLUSION: SIMPLIFYING COMPLIANCE, STRENGTHENING TRUST

Identity verification (IDV) is a vital part for financial service providers to meet their compliance obligations—but it doesn't have to be daunting. By adopting a risk-based approach, leveraging purpose-built IDV software, and staying aligned with evolving global and regional regulations, organizations of all sizes can build a resilient compliance framework that safeguards both their business and their customers.

Whether you're an enterprise navigating complex regulatory landscapes or a startup scaling fast, platforms like Veriff offer a powerful advantage. By automating identity checks, enhancing fraud prevention, and ensuring regulatory alignment, IDV solutions help streamline operations, reduce risk, and foster customer trust from day one.

Note:

This guide is intended for informational purposes only and does not constitute legal advice. Please consult qualified legal counsel to ensure compliance with applicable laws and regulations.





Veriff is a global identity platform helping businesses build trust online. Our AI-native technology combines automation and human expertise to quickly and accurately verify users worldwide with minimal friction.

Our trust infrastructure helps businesses stay compliant, prevent fraud, protect users, and scale globally, enabling a safer, more transparent internet for everyone.

Speak to one of our fraud experts today to discover how we can create customizable fraud protection for your business:

veriff.com