IDVerse™

An OCR Labs® Company

International AML Digital Identity Verification Regulations 2022

16TH FEBRUARY 2023

IDVerse™ An OCR Labs® Company

FINTRAIL

We work with many global companies, so we know the last thing you want to do is get bogged down in the digital identity verification regulations in each country you operate in. What you want is one digital identity verification (IDV) solution that works in every region you cover, no matter the local Anti Money Laundering (AML) and Know Your Customer (KYC) regulations. Being able to manage one global IDV system centrally, minimises time and expense, and enables you to get on with running your business securely and profitably.

IDVerse provides the most certified and compliant IDV platform in the world. It handles over 16,000 ID documents in 230+ countries: ID Cards, Passports, Drivers Licences, Residence Permits, ID Books, Passport Cards, Firearms licences, Defence IDs, National Health Cards etc. These documents are properly read, not just simple MRZ reading, and we have a 99.7% success rate against fraud.

By checking the countries relevant to you in this document you will see that we are up-to-date with all the regional regulations and state clearly how IDVerse' solution is compliant with them. With IDVerse you have peace of mind that your IDV solution is compliant everywhere it needs to be, leaving you free to focus on your business.

Research was carried out by FINTRAIL in 2021

FINTRAIL considered the following for each geographic market:

- Impact of regulation, including primary AML regulation, views of regulators and any recent news that may impact IDV and use of liveness
- Any recent or anticipated changes in the regulatory approach
- The local landscape, including leading providers and uptake of IDV & liveness (or selfie tech, where liveness is less dominant) in the public and private sector

This is based on open source information and anecdotal evidence, as gained from FINTRAIL's work with 60+ financial institutions.

Contact IDVerse

USING OUR TECH

HSBC

BMW

Australian Government

vodafone

bp

ING

Westpac

zip

American Express

trunarrative
Part of LexisNexis® Risk Solutions

Reed Screening

OYAK

Cognito

Table of Contents

Digital identity verification regulations in Canada

KEY POINTS:

1. FINTRAC regulates AML in Canada
2. Only a government-issued photographic ID can be used for IDV
3. Any selfie or video must be examined using facial recognition tech and not manual review.

IDVerse is compliant in Canada as our facial recognition does not use manual review and we recognise government-issued photographic ID

Regulatory detail

- Canadian financial crime regulation is delivered by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and is amalgamated from various pieces of national legislation.
- FINTRAC's 2021 guidance allows IDV in situations where a person is not physically present. Unless relying on credit reports, an authenticated government-issued photographic ID is required for IDV and FINTRAC is explicit in that matching an unauthenticated document to an image or video will not suffice.
- FINTRAC outlines (Section 2.A) that, where a person is not physically present, document verification should be complemented with either a "live video chat session" or a selfie photo/ video.
- They further specify that any selfie or video must be examined using facial recognition tech and not manual review.
- The Pan-Canadian Trust Framework (PCTF) is a key underpinning to ensure that the Canadian digital identity ecosystem is trustworthy and encourages a fair, innovative, and competitive environment.
- There are some provincial restrictions on the use of IDV in certain circumstances (for example, the Government of British Columbia only allows IDV for criminal record checks where an applicant has resided in Canada for 2+ years with 6+ months in-country credit history).

Recent changes

- It has been less than three years since FINTRAC updated its guidance (Nov. 2019) and underlying regulation (Proceeds of Crime (Money Laundering) and Terrorist Financing Act) to permit non-face-to-face identification, including the use of liveness checks alongside document scans.
- The June 2021 changes mostly just move around some of the previous language, but it's made these methods top of mind again.
- As of July 1, 2020, virtual currency dealers are in scope of the AML legislation. Canada also considers foreign money service businesses (FMSBs) that service Canadian users to be subject to the Canadian requirements, including KYC.

Contact IDVerse

Digital identity verification regulations in France

KEY POINTS:

1. AMF ultimately regulates IDV in France
2. KYC must be in line with eIDAS regulation
3. Document requirements are not prescriptive

IDVerse is compliant in France as our IDV complies with eIDAS and AMF

Regulatory detail

- The Autorité des Marchés Financiers (AMF) is responsible for AML/CFT regulation. Different licensing bodies, including ACPR, are also responsible for oversight. The Criminal Code and Monetary and Financial Code set out requirements for regulated institutions.
- IDV is permitted, while requirements are not prescriptive.

Recent changes

- 5MLD was transposed into French law in early 2020. Tax advisors and commercial court clerks are now in scope of requirements. France also restricted requirements on art and real estate brokers to those handling transactions of more than EUR 10,000.
- Remote identification is no longer automatically high risk, but KYC must be in line with eIDAS regulation (Regulation 910/014) or by pairing two methods outlined in the decree.
- Two documents were required to be collected as part of KYC previously; now one document is considered acceptable, when paired with other appropriate IDV checks.
- In March 2021, data authority National Information Systems Security Agency (ANSSI) published an update to its standards for remote verification, including video verification. The AMF expects these standards to be met.
- The PACTE law enacted in 2019 already pulled crypto asset companies into scope of AML/CFT regulation, with requirements for companies to also register with the AMF. This only covered crypto to fiat transactions, though, while a June 2021 update also pulled crypto to crypto transactions and trading platforms that operate in France.

Digital identity verification regulations in Germany

KEY POINTS:

1. BaFin regulates IDV in Germany
2. IDV standards must mirror EU eIDAS regulations
3. A person's nationality must be collected, a requirement not seen in many other EU countries.

IDVerse is compliant in Germany as our IDV complies with eIDAS and BaFin

Regulatory detail

- BaFin is Germany's primary AML/CFT regulator and outlines requirements in the Geldwäschegesetz (GwG), also known as the Money Laundering Act.
- The regulation itself does not get specific on the use of selfie or video technology—like the Netherlands, it only stipulates that standards must mirror eIDAS or similar local requirements, or a photographic identity document should be used, e.g. German National ID Card or a Passport.
- It further states that only technology "equivalent to" examining documents in person can be used.
- A person's nationality also must be collected, a requirement not seen in many other EU countries.
- Pursuant to BaFin Circular 3/2017, video identification is recognized in accordance with the AML Act in Germany.
- The model is meant to mimic face to face interactions between trained staff in a secure premise and a customer instead of simply matching a liveness check or selfie against a document. This introduces a manual element not seen in countries that employ matching methods.
- Any documents used as part of video identification must have a secure machine readable zone (MRZ) feature, as well as additional tamper-proof security features.

Recent changes

- In 2020, Germany's implementation of 5MLD brought art markets and estate agents into scope of AML requirements.
- Cryptoasset companies were also broadly impacted, with any broker/dealer, advisor, portfolio manager, underwriter, wallet provider, key custodian or placement agent required to register and become licensed. They also consider crypto to crypto transactions in scope.
- This is a broader interpretation of 5MLD than other EU countries chose to make, and also prevents passporting into Germany without a licence or partnership with a licensed cryptoasset company.
- In 2020, Germany announced that by September 2021 all Germans would have access to an electronic identity that could replace the physical national identity cards.

Digital identity verification regulations in Hong Kong

KEY POINTS:

1. HKMA regulates IDV in Hong Kong
2. Document requirements are not prescriptive
3. Hong Kong is moving towards digital identity for all citizens called iAM Smart

IDVerse is compliant in Hong Kong as our IDV complies with HKMA

Regulatory detail

- The Hong Kong Monetary Authority (HKMA) is responsible for AML/CFT regulation, via the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO), and oversight.
- The regulations are technology neutral and read that "documents, data or information provided by a reliable and independent source" can be used for verification.
- KYC must include a document with a "photograph of the customer", with HKMA mandating that firms set a time limit on the verification process (for ex., the firm may choose to close any accounts that have not completed KYC in 90 days).
- HKMA guidelines were last updated in 2020 for stored value issuers, and 2018 for all other regulated firms.

Recent changes

- In January 2019, HMKA released a circular that clarified its position on IDV, including facial recognition and liveness checks. The model is similar to that in Europe, relying on a combination of document authentication and matching documents to selfie or liveness checks.
- A report last year by HKMA read that manual checks were still needed to spot "unusual background of selfie or unusual facial expression by the applicant". The same thematic review applauded manual oversight of selfie and liveness checks while companies were first integrating new verification software.
- Hong Kong is moving towards digital identity for all citizens under a program called iAM Smart, launched in late 2020. The program will pair biometrics with HKID cards and other information. HKMA and the Securities and Futures Commission (SFC) have both released statements encouraging financial institutions to consider using iAMSmart for remote onboarding.
- In May 2021, the government shared the results of a consultation on a licensing regime under the SFC for cryptoasset providers similar to those in place elsewhere. The regime intends to restrict access by casual investors, with checks required to ensure customers are high net worth or institutional investors. This is expected to be enacted in 2022.
- In August 2021, HKMA circulated a letter stating that it would launch the AML and Financial Crime Regtech Labs later in the year. This is among other initiatives they are leading to "ensure that the mandate for innovation in AML/CFT is supported".

Digital identity verification regulations in India

KEY POINTS:

1. Reserve Bank of India (RBI), India's central bank. regulates IDV in India
2. India's regulations refer to KYC as CIP or Customer Identification Program
3. In May 2021 India enabled video-based KYC (known as V-CIP)
4. 99% of Indians have the Aadhaar digital identity document

IDVerse is compliant in India as our IDV complies with RBI regulations and recognises Aadhaar.

Regulatory detail

- India's AML/CFT regulations are administered by the Reserve Bank of India (RBI), India's central bank. The primary regulation is the Prevention of Money Laundering Act (PMLA) and associated rules.
- India's regulations refer to KYC as CIP or Customer Identification Program.
- This program is prescriptive, and mandates that KYC uses a photographic identity card issued by the government or a letter from a gazetted (authorised) officer with a "duly attested photograph" attached. Additional documents, such as bank statements, are allowed to complement this check.
- IDV is allowed for non-face-to-face account opening if additional measures are also applied. This includes collecting additional documentation or requiring that documentation is certified.
- The Indian government administers a digital identity program available to all Indian residents known as UIDAI (Unique Identification Authority of India), or better known as Aadhaar. Facial recognition was added to Aadhaar in 2018. The AML/CFT regulations stipulate that UIDAI should be accepted by financial institutions in India as valid identity.
- The Securities and Exchange Board of India (SEBI) still mandates in-person verification checks, particularly for high value accounts, although it accepts that IDV is appropriate in addition to in-person checks.

Recent changes

- In May 2021 India relaxed KYC requirements in the 'Master Direction to KYC', the official RBI guidance, by allowing video-based KYC known as V-CIP. There are several requirements, such as that video recordings should be geotagged and date stamped.
- In June 2021, industry body Internet and Mobile Association of India (IAMAI) kicked off an initiative to encourage self-regulation with AML/CFT requirements, particularly KYC, by cryptoasset firms.
- Official crypto regulation is expected to follow, particularly as an enforcement action was recently issued against Binance subsidiary WazirX in India.
- Online gaming is under pressure from the Indian Financial Intelligence Unit after a fine was levied on one platform that processed payments. Although the platform argued that they are not in scope of the AML/CFT regulations, it signals that the industry may soon be.
- This follows a fine by the Indian FIU on PayPal in late 2020. While focused on failures to properly identify and report suspicious activity, and not KYC, the fine highlights increased regulatory pressure on the online payments industry.

Digital identity verification regulations in the Netherlands

KEY POINTS:

1. The Netherlands Central Bank (DNB) regulates IDV
2. IDV standards must mirror EU eIDAS regulations
3. A copy, scan or sight of photographic ID is best practice, but not mandated

IDVerse is compliant in the Netherlands as our IDV complies with EU eIDAS regulations

Regulatory detail

- The Netherlands Central Bank (DNB) sets the AML/CFT regulations, known as the Wwft.
- A copy, scan or sight of photographic ID is still considered to be best practice in the Netherlands. The regulation now reads that other documents, information or data can be used provided they come from a “reliable, independent source” but this has been slow to be adopted.
- The AML/CFT guidance does allow for electronic verification.
- Like other European markets, the Netherlands allows for verification to take place after account opening only where the firm has determined the account is low-risk. Firms will often look to perform a single, simple KYC check at account opening and carry out further checks if the customer’s risk is found to be standard or high.

Recent changes

- As with other countries subject to the EU MLDs, the Netherlands pulled a number of new sectors into scope of its AML/CFT regulation in 2018. This most notably included dealers in high value goods (EUR 10,000 or greater, a reduction from the previous definition’s threshold of EUR 15,000), of which many are based in the Netherlands, and gambling providers.
- Cryptoasset exchangers and wallet providers were also pulled into scope in 2020.
- Non-face-to-face account opening, on its own, is no longer a reason for enhanced KYC measures, as per the 2018 update.

Digital identity verification regulations in Poland

KEY POINTS:

1. The Polish Financial Supervision Authority (PFSA) regulates IDV
2. PFSA recommend limiting video verification to Polish citizens
3. Every Polish adult residing permanently in Poland has to have a national identity card
4. In 2018 Poland's eIDAS implementation passed the European Commission's conformance tests

IDVerse is compliant in the Poland as our IDV complies with PFSA regulations

Regulatory detail

- The Polish Financial Supervision Authority (PFSA) is responsible for the Act on Counteracting Money Laundering and Terrorist Financing (AML Act).
- Unlike many other countries, Poland requires citizenship to be collected as part of identification. Verification methods are not prescriptive, and allow for the use of a "document confirming the identity of a natural person, a document containing valid data from the extract of the relevant register or other documents, data or information originating from a reliable and independent source."
- The AML Act also specifies that customers must be notified of any data processed as part of KYC.
- In June 2019, the PFSA issued a notice on video verification best practices. It specified banks and credit institutions but did not appear to prohibit other sectors from using the technology. Of note, it encouraged companies to look for signs of persons under the "influence of intoxicants", third parties manipulating persons or signs that the person was not aware of the steps they were taking (i.e. account opening).
- They also recommend limiting video verification to Polish citizens or residents, or taking other steps to limit the process to lower risk groups.
- Poland has ramped up Trusted Profile, a nascent digital identity and electronic signature system, in reaction to COVID-19. The system is currently used with government and not private services.

Recent changes

- The following sectors are pulled into scope of the AML Act, based on an April 2021 amendment: real estate agents and art or antique market participants with transactions of EUR 10,000 or more. Tax advisors and other professional service providers are also in scope.
- Virtual asset exchanges were added in scope in 2018, but Poland failed to introduce a register of exchanges as per 5MLD. This register was introduced with the recent change and will increase regulatory scrutiny on Polish exchangers. The register goes live in November 2021, with existing companies allowed a grace period until May 2022.
- The amendment also states that documented rationale must be on file for any instances where verification is unsuccessful, including verification on certain data points (i.e. not simply if an account cannot be verified, but any information on that account).
- This amendment was seen as long overdue and represents a significant no. of changes for regulated entities.

Digital identity verification regulations in Singapore

KEY POINTS:

1. The Monetary Authority of Singapore (MAS) regulates IDV
2. Their AML/CFT guidelines stipulate that IDV can be used but additional checks must supplement the IDV process.
3. Over 60% of citizens use Singpass, a digital identity system that gives citizens access to government and private services.
4. SingPass Face Verification allows re authentication via facial Recognition.

IDVerse is compliant in Singapore as our IDV complies with MAS regulations

Regulatory detail

- The Monetary Authority of Singapore (MAS) is the supervising AML/CFT authority in Singapore.
- Their AML/CFT guidelines stipulate that IDV can be used with non face-to-face products but that, because of the heightened risk of non face-to-face activity, additional checks must supplement the IDV process.
- The guidelines also read that “Where the customer is a natural person, a payment service provider should obtain identification documents that contain a clear photograph of that customer.”
- This is repeated in more recent, industry-specific guidelines. Requirements to collect photo-based documents are relatively rare, with most regulators allowing firms to choose the verification method(s) that make sense given their risk.
- The Payment Service Act (PS Act) entered into force in January 2020, with amendments following. Payment services providers, including cryptoasset companies and virtual asset service providers, must now be licensed and comply with KYC requirements.
- Singapore has invested heavily in Singpass, a digital identity system that gives citizens access to government and private services. SingPass Face Verification allows re authentication via facial Recognition.

Recent changes

- Under PSN01, guidelines for licence holders under the PS Act, “the payment service provider shall, at his or its own expense, appoint an external auditor or an independent qualified consultant to assess the effectiveness of the policies and procedures referred to in paragraph 7.34, including the effectiveness of any technology solutions used to manage impersonation risks.” This covers IDV and KYC solutions.
- These audits are a new requirement, with each new firm and firms who have made changes to their programs having to undergo them.

Digital identity verification regulations in Spain

KEY POINTS:

1. Sepblac regulates IDV in Spain
2. Sepblac accepts IDV solutions that comply with eIDAS.
3. But Spain's approach to AML is one of the most complex in Europe

IDVerse consults with clients on specific uses that are compliant with Sepblac

Regulatory detail

- Sepblac is Spain's AML/CFT supervisory authority.
- The country's approach to AML is viewed as one of the most complex, and toughest, in Europe—but not necessarily in a positive way. This includes some requirements imposed on EU regulated firms passporting into Spain in addition to their home state requirements, such as the need to register a designated representative with Sepblac.
- The Regulation of Law 10/2010 on the prevention of money laundering and terrorist financing has been amended since and outlines the country's AML/CFT requirements.
- Any non-face-to-face methods have to be "authorised" by Sepblac, which now accepts IDV solutions that comply with eIDAS.
- In 2018, Sepblac issued updated guidance on video verification stipulating that only "reliable" documentation can be used, and only from a single device.
- The guidance also permits pre-recorded videos used in verification, but considers these as higher risk and expects firms to treat them as such.
- Firms must undergo stringent technical risk assessments before using any such solution.
- Spanish citizens must use a Spanish National Identity Card to open a bank account, while others can use a passport or other official documentation such as a residence permit. Beyond that, Sepblac states that "Under no circumstances does Sepblac establish the obligation to request specific documents from specific clients."

Recent changes

- The Spanish data protection authority, AEPD, has ruled that biometric facial authentication should not be used to meet regulatory compliance obligations for remote client registration.
- The decision states that the country's 'Prevention of Money Laundering and Terrorist Financing' or 'AML/CFT Law' specifies identification methods allowed (see the "authorization" above), and does not include biometrics.
- While implementing 5MLD in early 2021, Spain pulled real estate brokers conducting large rental transactions (EUR120,000/annum), crypto asset exchangers and wallet providers, and professional service providers (i.e. tax advisors) into scope of AML/CFT requirements.
- It was also clarified that documents do not need to be stored where eIDAS regulations on digital identity are met.
- This overrode an earlier 2020 draft meant to implement 5MLD that failed. This had included crowdfunding, which has faced heavy scrutiny in Spain, as in scope.
- In September 2021, several cryptoasset exchangers were targeted by the government, who issued a list of those not yet registered under new requirements.

Digital identity verification regulations in Turkey

KEY POINTS:

1. Ministry of Finance and Central Bank regulates IDV in Turkey
2. Within the Ministry of Finance, BRSA is the general regulatory authority and MASAK is the financial intelligence/investigatory regulator.
3. Biometric verification technologies such as facial recognition between the applicant and the document photo are permissible in IDV.

IDVerse IDV complies with BRSA & MASAK regulations in Turkey

Regulatory detail

- In Turkey, the Ministry of Finance and Central Bank set regulatory standards that are taken from multiple AML and CFT laws within Turkey.
- Within the Ministry of Finance, BRSA is the general regulatory authority and MASAK is the financial intelligence/investigatory regulator.
- Turkish regulations allow for the use of electronic submissions of documentation for verification, as well as in-person traditional methods. Of note, a signature sample, place of birth and parent details are required as part of identification and the latter two signals are expected to be verified. Signature is used as a reauthentication method, as expected under the regulation.

Recent changes

- In April 2021, Turkish authorities issued new guidance on the use of IDV services allowing for the use of electronic submission and video verification of applications to open bank accounts, specifically referencing the use case of remote-onboarding.
- The guidance stipulates that technologies such as near-field communication (NFC) can be employed for chip-enabled documentation, and that video-calling should be deployed to support the verification process.
- Biometric verification technologies such as facial recognition between the applicant and the document photo are also referenced as being permissible in the remote IDV process.
- Also in April 2021, regulation was published stating that cryptocurrencies cannot be used as a form of payment. This has been seen by many as a political move to curb depreciation of the Lira. Two platforms, Thodex and Vebitcoin, essentially collapsed following the news and subsequent government intervention.
- In May 2021, cryptoasset companies were added into scope of the AML/CFT law under presidential decree.
- Changes were published in June 2021 for the telco sector around identity verification, Four distinct methods, including video verification are now approved under relevant regulation.

Digital identity verification regulations in United Arab Emirates

KEY POINTS:

1. The Central Bank (CBUAE) regulates IDV in United Arab Emirates
2. But free zones like Dubai International Financial Centre have their own authority
3. In February 2021, the UAE Cabinet approved a 'trial run' of facial recognition technology in several sectors, including the financial sector.

IDVerse consults with clients on specific uses that are compliant with UAE

Regulatory detail

- The Central Bank (CBUAE) sets the AML/CFT regulation within the UAE. The regulation does not specifically reference use of IDV services, however it does stipulate that financial institutions must take adequate measures to verify identity.
- Free zones are under their own authority, as well as the federal law. As an example, the Dubai Financial Services Authority (DFSA) regulates the DIFC. Historically, the DFSA has been seen as more progressive.
- The Central Bank oversees the KYC Blockchain Consortium, which launched in 2020 and includes HSBC and the DIFC as members. The idea is to allow banks to query verified identity information.
- The UAE is implementing a national digital ID for its citizens known as UAE Pass App, which will become a mandatory form of ID for some government services and can also be used by the private sector. The system uses facial recognition software. This state-issued ID system is what the World Bank describes as a 'government-driven centralised system'.
- There is a high foreign national or expat population in the UAE. Visas and employment permits are often still required in addition to foreign government-issued documents.

Recent changes

- In-person document-based verification was mandatory until 2019. It's still required to collect a digital copy of a document (typically a passport or UAE ID card).
- In February 2021, the UAE Cabinet announced that it was approving a 'trial run' of facial recognition technology in several sectors, including the financial sector.
- The CBUAE launched new AML/CFT guidelines in June 2021. Following with other leading nations, the guidelines now say that identity must be verified against "documents, data or information " (6.3.1). They follow by stating that "The verification of a customer's identity, including their address, should be based on original, official (i.e. government-issued) documents whenever possible ".
- The UAE Securities and Commodities Authority (SCA) have been working on regulation of cryptoassets, but this has not directly looped in with the country's AML/CFT legislation yet. Numerous cryptoasset firms operate in or from the UAE currently.

Digital identity verification regulations in United Kingdom

KEY POINTS:

1. The EU's Money Laundering Directives are still the UK's primary IDV regulation
2. How closely the UK will continue to mirror the EU directives is still unknown
3. The UK doesn't dictate how IDV is conducted but the Joint Money Laundering Steering Group (JMLSG) set out best practice and the Financial Conduct Authority (FCA) expects firms to follow this standard.

IDVerse IDV complies JMLSG best practice standards in United Kingdom

Regulatory detail

- The UK's Money Laundering, Terrorist Financing, and Transfer of Funds Regulations 2017/10 (the MLRs) helped to introduce the EU's Money Laundering Directives and build on the earlier Proceeds of Crime Act 2002, which is still the UK's primary AML regulation.
- The Joint Money Laundering Steering Group (JMLSG) guidance is prepared by an industry body and is seen as industry best practice. The Financial Conduct Authority (FCA) expects firms to follow this standard.
- Within the JMLSG and the MLRs, electronic verification (IDV) is deemed acceptable as long as the users are confident that the information electronically obtained is: "secure from fraud and misuse and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact that person. Firms should therefore document steps taken in this regard." (JMLSG Part I, 5.3.33)
- The regulation is technology neutral, meaning that the UK doesn't dictate how IDV is conducted.
- This means users of IDV can design their controls based on their risk exposure and desired customer experience.
- However, regulators are increasingly expecting firms to illustrate that they know how their IDV technology works and that they have appropriate checks in place to identify when it fails. As an example, firms should use providers with: "transparent processes that enable the firm to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject." (JMLSG Part I, 5.3.52)
- The Department for Digital, Culture, Media & Sport (DCMS) regularly issues new updates to its digital identity trust framework part of the government's wider plan to make it quicker and easier for people to verify themselves using modern technology

Recent changes

- The MLRs are under amendment, with an open consultation under way.
- How closely the UK will continue to mirror the EU directives is still unknown.
- The FCA explicitly mentioned "'selfies' or videos" as legitimate means to identify individuals in a Dear CEO letter from March 2020, spurred on by COVID-19 and issues with in-person identification processes. Later clarification explained that those liveness tests must be combined with other checks or documents.
- When published in 2017, the MLRs were expanded to cover sectors such as art market participants, auction houses, real estate, and tax advisors. Cryptoasset exchanges were added in a 2019 amendment. These sectors are likely still iterating on compliant solutions to onboarding and KYC.

Digital identity verification regulations in United States of America

KEY POINTS:

1. The financial crimes enforcement division (FinCEN) of the US Treasury regulate IDV
2. FinCEN has not recognised selfies or liveness checks officially, but did refer to such checks as standard protocol in 2020
3. The Anti-Money Laundering Act of 2020 also emphasises the use of "innovative approaches" without clarity on what might be acceptable.

IDVerse consults with clients on specific uses that are compliant with USA on a state by state basis

Regulatory detail

- The 1970's Bank Secrecy Act (BSA) is seen as pioneering AML regulation, and has since been amended by various statutory instruments and rules released by the US Treasury and its financial crimes enforcement division FinCEN.
- This includes the CDD Rule in 2016, which led to widespread remediation efforts to identify and verify beneficial owners.
- The US mandates a Customer Identification Program (CIP) based on documentary and/or non-documentary verification methods, as was reformed by Section 326 the USA PATRIOT Act.
- Under it, a risk-based approach is required but regulated firms must collect ("identify") a customer's name, date of birth, address and identification number (social security or tax identification number).
- The US still maintains that non-face-to-face products are higher risk from an AML/CFT perspective.
- US NIST Standards, under the US Department of Commerce, outline that remote onboarding by video should include a second party, i.e. an "operator", to be present so as to increase reliability. The Standards include several levels of proofing, authentication and federation assurance that firms can choose based on their risk levels or tolerance.
- Under the standards, pictures/selfies and video recording are considered to offer standard assurance (IAL2) if also combined with other "strong evidence" of the person's identity, including scanned identity documents. The highest level involves a person (i.e. an "operator", as above) to mimic in-person identification, similar to Germany's program.

Recent changes

- While FinCEN has not recognised selfies or liveness checks officially, FinCEN did refer to such checks as standard protocol in its July 2020 Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic.
- In early 2021, the Anti-Money Laundering Act of 2020, part of the National Defense Authorization Act, introduced the most AML/CFT changes seen since the USA PATRIOT Act in 2001. Its aim is to make progress on beneficial ownership and identify any individuals that own or control a company authorised to do business in the US.
- The Act also emphasises the use of "innovative approaches" without clarity on what might be acceptable.

IDVerse™
An OCR Labs® Company

Secure and seamless user verification for a remote world.

From anywhere, anytime.

IDVerse helps businesses verify their users identity at the blink of an eye.
Onboard them and scale your business without the compliance & operational overheads.

Contact IDVerse

About IDVerse

IDVerse is the leading automated identity verification platform to onboard and re-authenticate trusted users at scale.

What sets IDVerse apart? Our commitment to Zero Bias™ machine learning means that we are pioneering the use of generative AI to protect against discrimination on the basis of ethnicity, age, and gender. We build technology capable of authenticating tens of thousands of ID document types and verifying the liveness of billions of real people without manual human intervention—all underpinned by technology that achieves maximum inclusion and fairness.

IDVerse can recognize over 16,000 ID types in 142 languages from more than 220 countries and territories. The world's leading companies like Amex, HSBC, and Hertz trust us to help their users prove their identity in as few as 30 seconds.

IDVerse Certifications

IDVerse meets the most stringent privacy, data protection, security, resilience standards and global digital identity trust frameworks - including Australian TDIF accreditation as an Identity Service Provider, SOC Type 1 & 2 and ISO 27001, 27017, 27018, 27701, 29100, 22301, 30107-3 (covering both PAD level 1 and 2), 19795 and 9001. IDVerse is ranked #1 globally for detection of real and fraudulent individuals.

IDVerse™

An OCR Labs® Company