NEXT-GENERATION DIGITAL ID FOR KYC A GUIDE FOR MLROS

How OneID®'s electronic identity verification complies with the UK's Money Laundering Regulations (MLRs) and the Joint Money Laundering Steering Group (JMLSG) guidelines

ANTI-MONEY LAUNDERING – TODAY'S CHALLENGE

More and more business is now done online, increasing the risk of fraud, money laundering, identity theft, and deep fakes.

At the same time, the customer's experience of digital onboarding can be poor, usually requiring presentation of ID documents and selfies, which in themselves can be compromised by a growing epidemic of deep fakes.

The UK Government has certified a number of digital ID providers under the Digital Attributes and Trust Framework (DIATF) to provide a modern alternative for the growth of the digital economy.

OneID®, as one of those certified providers, has recognised the twin challenge of improving the customer experience without compromising duties under the MLRs by using the verifiable credentials held by the banking network in a cutting-edge solution.

WHAT IS ONEID®?

OneID® is a provider of a bank-based digital ID service that enables anyone with UK mobile or online banking to simply and safely prove who they are online in just seconds.

Individuals use our service when they sign up for or use a service provided online by one of our corporate customers ('relying parties').
We provide ID services across the financial services sector (KYC), employment screening (DBS, Right to Work) and esigning, through our integration with both Adobe and Docusign, where we are currently providing verified identity to signatories on their platforms.

The individual clicks a OneID® button, authenticates with their bank app or login using their existing bank credentials and confirms what bank-verified ID data is being shared.
This gives them greater visibility and control over how they verify their identity, where their data is being used, and a consent history for past data-sharing transactions. OneID® sources ID evidence data from multiple verified and authoritative data sources, including UK banks, credit reference agencies and fraud databases, to meet JMLSG requirements for multiple data sources.

OneID® is regulated by the FCA and certified as an Identity Service Provider (IDSP) under the Department of Science, Innovation and Technology's ID framework.

Our ID service is independently certified for AML use cases against the requirements for an electronic identity provider that are contained in the current MLRs and industry guidance for:

- **Financial Services (JMLSG)**
- **Legal Services (LSAG)**
- **Accountancy Services (CCAB)**

COMPLIANCE WITH MLRS AND JMLSG

OneID®'s digital identity verification service is fully compliant with the MLRs and JMLSG.

Indeed, the MLRs were amended in 2020 to expressly allow for electronic IDV, per MLR 28(19) stipulates:

"For the purposes of this regulation, information may be regarded as obtained from a reliable source which is independent of the person whose identity is being verified where—

(a) it is obtained by means of an electronic identification process, including by using electronic identification means or by using a trust service ... and

(b) that process is secure from fraud and misuse and capable of providing assurance that the person claiming a particular identity is, in fact, the person with that identity, to a degree that is necessary for effectively managing and mitigating any risks of money laundering and terrorist financing."

In Part I 5.3.52, JMLSG further expands on the required characteristics of the organisation providing such electronic verification. OneID® fully meets these required characteristics, which we set out below:

"Before using an organisation for digital identities, electronic or digital identity verification, or trust services, firms should be satisfied that information supplied by the provider is considered to be sufficiently extensive, reliable, accurate, independent of the customer, and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact that person. This judgment may be assisted by considering whether the provider meets the following criteria:

- ***It is recognised, through registration with the Information Commissioner's Office (or national equivalent for EEA/EU registered organisations), to store personal data;***
  - OneID® is registered with the Information Controller's Office (ICO) as a data controller
- ***It is accredited or certified to offer the identity verification service through a governmental or industry process that involves meeting minimum published standards;***
  - OneID® is certified under the DIATF
- ***It uses a range of multiple, positive information sources, including other activity history where appropriate, that can be called upon to link an applicant to both current and previous circumstances;***
  - OneID® has access to the real time data of 29 banks and the UK mobile network operators, the latest information from the credit reference agencies and access to government identity data sources.
- ***It accesses negative information sources, such as databases relating to identity fraud and deceased persons;***
  - OneID® accesses the National SIRA Fraud, DDRI and Amberhill Match
- ***It accesses a wide range of alert data sources;***
  - Synectics and CRAs
- ***Its published standards, or those of the scheme under which it is accredited or certified, require its verified data or information to be kept up to date, or maintained within defined periods of re-verification;***
  - OneID® is certified under the DIATF

- ***Arrangements exist whereby the identity provider's continuing compliance with the minimum published standards is assessed***
  - Through the DIATF
- ***It has 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.***
  - We provide the Relying Party with the evidence used to confirm the identity in every transaction using open standards for ID data sharing. We are one of only a few providers who can provide ID assurance up to a Very High level under GPG45, and also offer document scan and selfie methods of onboarding.
- ***It keeps sufficient records of information used to provide its services.***
  - Encrypted evidence stored, which is only decrypted by the relying party and never by OneID®.

RISKS WITH PHYSICAL DOCUMENTATION

Reliance on physical documentation carries the risk of fraudulent documents being presented, which can also be 'fraudulently issued genuine documents' that will get through the process.

Criminals can exploit weaknesses in processes to obtain genuine ID documents using fake or other people's ID data. Templates to create fraudulent documents are readily available online, e.g. to print bank or utility statements at home or present them online. Paper-based ID evidence is inherently insecure and unverifiable. AI-generated document images are increasingly hard to differentiate from real images, with deep fakes now widespread, which makes the captured data higher risk and the 'trusted source' data more important and reliable as ID evidence.
Remote checking of a physical document is also now at risk from the rapid advances in generative AI's ability to create 'synthetic IDs' that can combine real ID attributes with generated ones and is leading to increased attacks on ID service providers. Images and videos that look real can easily be created and cannot be differentiated from actual people. Countermeasures include 'liveness' checks to verify it is a real human and security measures to prevent 'data injection' into the ID data capture process.

This type of attack vector is negated by the OneID® because there is no document for a fraudster to forge or biometric (such as a facial scan) to attack.

WHAT ARE THE BENEFITS OF USING DIGITAL IDENTITY VERIFICATION WITH ONEID®?

The next generation of digital identity is where the evidence itself is digital and can be accessed via secure mechanisms such as strong authentication of the person and secure APIs.
This is a true 'digital ID'; both the evidence and channel are digital. As it is fully digital, the process also causes less friction and is faster than document scanning..

Unlike documentary evidence, which are point-in-time checks, banks conduct through-life checks on their customers and monitor for unusual usage behaviour or access locations. They build a customer profile over time, instead of an identity evidence that was created or delivered yesterday. This provides strong evidence of the identity's existence over a period of time.

To use OneID®, an individual has to pass the bank's authentication which means to log in using the trust over time behavioural biometric algorithm of the bank. If using their mobile banking app, they have to use the phone that is registered with

the bank and their facial or fingerprint recognition method or their passcode to unlock the app and verify themselves. If using online banking on a laptop, they have to enter the username and password for the account and provide a second factor of authentication such as using their debit card with a card reader. Both these measures present highly reliable proof that the individual is who they say they are.

Digital ID evidence is much harder to compromise; e.g., a fraudster needs to successfully open a bank account and develop a pattern of normal behaviour, including carrying out transactions with real money over a period of time to appear as a real person.

The benefits of using a digital ID include:

- **Secure process to obtain the digital ID (e.g., pass both a bank AML/KYC process and ID proofing process under the UK government's identity framework DIATF rules)**
- **Consent to use the data for specific purposes**
- **Use of secure authenticators, such as bank-provided Strong Customer Authentication (SCA), to protect the ID evidence from improper use**
- **Better customer experience and faster process increases usability and conversion**
- **More frequent usage creates more data that can be used to spot unusual activity**
- **Enhanced data enables networks to share fraud 'signals' data for fraud prevention**
- **Multiple sources of ID evidence can be cross-checked in real time**
- **Better data protection by using secure distributed data stores**
- **Alignment of the UK to international approaches for ID services**
- **These higher barriers to obtaining payment accounts through digital IDs mean they are more effective at preventing money laundering.**

HMT'S CONSULTATION ON IMPROVING THE EFFECTIVENESS OF THE MLRS (2024)

HMT recognises that the current MLRs could benefit from clarification on compliant methods of identity verification, so that secure digital IDs come into mainstream use.

Accordingly, its consultation document sets out its views:

"Digital identity verification

1.28 Identity verification is an important step in ensuring that regulated firms know their customers and can identify those who may pose a high risk of money laundering or terrorist financing. Thorough and effective processes to verify the identity of customers can prevent the use of false or stolen identities, which is a common feature of certain types of economic crime.

1.29 For these reasons, verification of customer identity is a fundamental part of the customer due diligence measures required under the MLRs. However, the government recognises that identity verification can be complex and resource-intensive for regulated firms, as well as time-consuming for legitimate customers.
The government is committed to considering ways to minimise the burden of identity verification for firms and customers while ensuring it remains effective at reducing the risk of ML/TF.
This section considers issues related to digital identity verification through this lens.

1.30 A digital identity is a digital representation of you and facts about you. It lets you prove who you are during interactions and transactions. You can use it online or in person.

1.31 The government is committed to actively encouraging and realising the benefits of digital identity technologies in the UK without creating or mandating identity cards. As part of the Data Protection and Digital Information (DPDI) Bill [now Digital Information and Smart Data Bill – King's Speech, July2024], we are now putting in place the necessary framework and tools for people to use digital identities confidently in an increasingly digital economy, if they choose to do so.

1.32 In collaboration with key organisations across the public and private sectors, the government recently updated its Good Practice Guide 45 (GPG45), which helps individuals and businesses decide how to check someone's identity. Measures in the DPDI Bill build on our commitment to strengthen domestic and international confidence in the UK's digital identity marketplace.
They underpin the UK's digital identity and attributes trust framework (currently in its beta version), which sets out rules, including roles, principles, policies, procedures and standards against which organisations can have their digital identity products and services certified.

Digital Identity and the MLRs

1.33 [etc]

1.34 The MLRs are currently intended to be technology neutral with no preference between the use of Digital identities or physical identity sources are used to verify customer identity.
As set out in regulation 28(18), in this context, verifying a customer's identity means verifying that identity on the basis of documents or information 'obtained from a reliable source which is independent of the person whose identity is being verified'. Regulation 28(19) clarifies that an electric identification process may be used where such a process is "secure from fraud and misuse" as well as being "capable of providing assurance that the person claiming a particular identity is, in fact, the person with that identity, to a degree that is necessary for effectively mitigating any risks of ML/TF."

The current Government are signalling their intent to strengthen the legislative framework still further, including the MLRs, to ensure that approved digital ID solutions, including OneID®, will become mainstream and secure the acceleration of the digital economy.