innovate identity

experts in id

FATF consults on digital identity draft guidance

Ewan Willars

The Financial Action Task Force (FATF) have recently released draft digital identity guidance for consultation. Here we look at the main themes emerging from the guidance, and how this might impact on the UK digital identity ecosystem.

FATF produces a range of guidance intended to supplement the 40 FATF recommendations that provide the backbone of the international anti-money laundering and terrorist financing regime. Recommendation 10 provides the blueprint for how Customer Due Diligence (CDD) is undertaken: the types of checks that regulated organisations have to carry out, and the types of circumstances in which CDD is required.

The new draft guidance released by FATF looks at how digital identity solutions can meet CDD requirements, and the issues that governments and regulators, regulated entities themselves and digital identity providers must consider when utilising digital identity to identify a customer.

As ever with FATF guidance it straddles existing best practice and emerging practice. It therefore directly reflects a lot of recent changes that we have already seen captured in the 5th Money Laundering Directive (5MLD) and other initiatives, but it also goes beyond existing rules in a number of areas, and by so doing points towards the likely direction of travel for the anti-money laundering (AML) regime in the years ahead.

So, what are the main themes that emerge from the guidance, and what are their potential implications?

1. Digital Identity is now a mainstream way to undertake CDD

The lack of regulatory clarity that has plagued the use of digital identity by regulated firms has been addressed by 5MLD, which should hit the UK statute book in the coming months. This clarity is further addressed in the FATF guidance, which is very clear in setting out that digital identification and authentication can be at least, if not more secure, than face-to-face methods. This should finally lay to rest any lack of regulatory confidence in utilising digital identity solutions much more widely in financial services and other regulated industries.

2. The need to demonstrate reliability and independence remains

Ensuring that information obtained for CDD is both reliable and independent has been a core tenet of AML practice for a long period, and this is retained in the guidance for digital identity. Identity service providers must think carefully about how they demonstrate not only the reliability and independence of the identity data they share, but also of their own architecture, processes and governance.

3. Risk-based approach extends to assessing identity solution providers themselves

The risk-based approach has been enshrined in CDD for a long time, and the guidance makes it clear that the architecture, processes and governance of an identity solution are very much part of the risk assessment. Are there central architectures that are inherently more risky? Is an identity provider's governance up to scratch? And how can this be evidenced to relying parties? These are some of the questions relying parties and identity service providers alike will need to address.

4. Non-face-to-face will no longer be an automatic high-risk factor

FATF guidance acknowledges that digital identity information from reliable and independent sources can be equivalent or lower risk than face to face customer identification and transactions.

5. The importance of aligning to Standards

FATF's risk-based approach relies on "a set of open-source, consensus-driven assurance frameworks and technical standards". It specifically mentions the NIST Digital ID Guidelines and the EU's eIDAS regulation, as well as the ongoing work by the International Organisation for Standardisation (ISO) and International Electrotechnical Commission (IEC) toward developing a 'comprehensive global standard' for digital identity systems. It is clear that FATF points towards solutions that conform to recognised standards frameworks. It looks likely that solutions wishing to play into the regulated identity market will need to align themselves with recognised standards.

6. Government authorisation, or government-backed certification may be critical

One significant element of the FATF draft guidance is the emphasis on digital identity solutions that have some form of government certification or authorisation. Relying parties are encouraged to consider the following questions:

- Does it have authorisation from government to be used for CDD?
- *If not*… then then do you know the robustness and assurance level of the solution (including its design and governance)?
- And, is the assurance level sufficient to address the level of risk?

Clearly having some form of official confirmation or certification concerning the assurance level of the digital identity is an important factor for providers. At present there is no government-backed certification for private sector digital identity providers available in the UK – will this need to be addressed going forwards? Will there need to be a licensing or certification authority put in place?

7. The importance of inclusion

Another noticeable element of FATF guidance is the emphasis on inclusion: both how digital identity ensures it does not become a barrier to inclusion, and how digital identity can itself help towards inclusion. The guidance suggests that some flexibility in how standards accommodate low risk use cases should be considered, and digital identity should be accommodated as an inclusion tool.

The potential impact of this could be that additional lower levels of assurance are needed to be developed in addition to the four low/medium/high/very high Identity Levels set out in Good Practice Guide 45 and reflected in eIDAS regulation. Ensuring that the level of assurance is proportionate to the level of risk, and does not unnecessarily exceed the level of risk, will be a conversation that is needed to be had by relying parties and regulators, to avoid unnecessarily high bars being set which would result in digital identity exclusion.

Conclusions

The Guidance remains a draft for now, and FATF are open to comments until late November. However, the direction of travel is clear, and unlikely to change – digital identity has been adopted into the mainstream of the AML regime.

There are clearly areas that have not yet been addressed in the UK ecosystem – the need for further development of digital identity standards, the need for some form of approved certification regime, and a closer focus on inclusion and proportionality probably key amongst them.

But the guidance is positive news - now that the regulatory position of digital identity is much clearer, another barrier has been removed to the more widespread application of digital identity solutions in the UK, even for highly regulated use cases.

You can view the consultation and the key questions posed by FATF **here**.

About Innovate Identity

Innovate Identity was founded in August 2012 as an independent consultancy providing advisory services focussed on digital trust, data and technology innovation within the global online community.

In this hyper-connected world, knowing whom you are dealing with, understanding the risks, ensuring compliance and respecting privacy, whilst dealing with the opportunities and challenges this creates has never been more important.

Our areas of expertise include Identity Assurance, Federated Identity Management, Digital Identity, Money Laundering Regulations and Customer Due Diligence, and Data Privacy.

We have deep functional and unrivalled vertical industry expertise in regulated industries, banking, payments, e-commerce and government, as well as breadth of geographical knowledge across multiple jurisdictions.

Innovate Identity Ltd
71-75 Shelton Street
LONDON
WC2H 9JQ

CONTACT US

Email: ewillars@innovateidentity.com
Telephone: +44 (0) 7825 077740