GDF GLOBAL DIGITAL FINANCE

**29 November 2019**

Financial Action Task Force
2, rue André Pascal
75775 Paris Cedex 16
France

**VIA EMAIL:**
FATF.Publicconsultation@fatf-gafi.org

## Re: Public consultation on FATF draft guidance on digital identity

Dear Financial Action Task Force,

Global Digital Finance support efforts by global standard setters, national authorities and regulators to consult and work with the nascent global digital / virtual asset industry.

To that end, we are hereby providing input to the Consultation regarding the proposed draft guidance on digital identity.

The input has been drafted and led by the GDF Anti-Money Laundering Working Group. Contributors who wish to be named are listed at the end of this document.

## About GDF

Global Digital Finance ("GDF") is a not-for-profit industry body that promotes the adoption of best practices for crypto and digital assets, and digital finance technologies through the development of conduct standards, in a shared engagement forum with market participants, policymakers and regulators.

Established in 2018, GDF has convened a broad range of industry participants, with 300+ global community members—including some of the most influential digital asset and token companies, academics and professional services firms supporting the industry. GDF is proud to include Circle, ConsenSys, DLA Piper, Diginex, Hogan Lovells, Huobi and R3 as patron members.

The GDF Code of Conduct is an industry-led initiative driving the creation of global best practices and sound governance policies, informed by close conversations with regulators and developed through open, inclusive working groups of industry participants, legal, regulatory and compliance experts, financial services incumbents and academia. Code principles undergo multiple stages of community peer review and open public consultation prior to ratification.

## Areas of focus

### 1. Are there any specific money laundering / terrorist financing risks that arise from the use of digital identity systems for CDD, other than those already mentioned in Section IV of the guidance?

Section IV of the guidance has provided good depth on the areas of specific money laundering ("ML") and terrorist financing ("TF") risks that arise from the use of digital identity systems for CDD. However, GDF contributors to this response have noted:

- Paragraph 115 on risks within the enrollment process: In addition to the two general categories, GDF believes a third category exists that is not adequately covered by the first two; willful use of genuine identity by organised crime groups (OCGs). It is briefly covered in paragraph 121 which alludes to willful collusion. However, there appears to be no mention of coercion or unintentional collusion.
    - Coercion may be considered where the real owner of a general or limited purpose identity is forced to create a digital identity against their will, with the subsequent binding, credentialing and authentication controlled by the OCG.
    - Unintentional collusion may be considered where the real owner of a general or limited purpose identity creates a digital identity in return for a cash sum. This may be more prevalent in low-GDP countries with lower penetration of digital services where a cash-sum equivalent to a monthly salary could be low enough to make it profitable for the OCG, and where the identity owner is unaware of what their identity will be used for.

- Although the guidance mentions the collection of additional data such as IP and physical addresses, it makes no mention of the risk that such data can be used to obfuscate the activities of an OCG. We recommend that the guidance draw attention to such risks, as there may be a lack of awareness regarding how misuse can occur, and the subsequent impact on verification. For example:
    - An IP address can be masked behind a virtual private network (VPN). There are legitimate reasons where it is prudent to utilise a VPN but it can also be used to mask activity, particularly anonymous VPNs. Thus, a financial institution may wish to track a customer's use of VPN as part of its ongoing monitoring activities.
    - A mobile phone number used for one-time passwords (OTP) can be set up for temporary use to facilitate the OTP. This removes the ability to be able to track ongoing transactions against, say, a cellular network.
    - Similarly, an email address can be set up for one-time use, that masks the intent of the creator but is sufficient to validate an account.
    - Finally, a postal address could be a temporary virtual address, such as virtual office address.

## 2. What is the role of digital ID systems in ongoing due diligence or transaction monitoring?

The role of digital ID systems in ongoing due diligence or transaction monitoring should be to ensure that the benefits of digital ID identified by FATF in Section IV, Strengthening CDD, are realised, including:

- minimising weaknesses in human control measures at on-boarding, thus ensuring the identification baseline is robust and sound;
- ensuring that the customer is who they say they are during the onboarding process;
- providing access to more data points, which can enhance the understanding of customer behaviour, and enable VASPs to improve transaction monitoring and better understand when behaviour is unusual or suspicious, improving the chances of detecting potential fraud, money laundering and terrorist financing attempts; and
- improving the customer experience by allowing VASPs to carry out digital checks in the background rather than through direct customer interaction.

### a. What information do you capture under authentication at on-boarding and during authorisation for account access? Who captures this data?

Broadly speaking, three types of data are captured under digital ID authentication at on-boarding:

- biodata about the client contained in the ID (e.g., Name and Date of Birth) and ID document information (e.g., document ID number and document ID type),
- session data (e.g. IP address, geo-location, and device information data), and
- authentication test results performed by the third party provider on the captured data.

At on-boarding, the data will most likely be captured by a third party vendor and sent on to the VASP via API connection (unless the VASP has developed the technology in-house or conducts the ID verification on its own servers).

After on-boarding, during ongoing client logins, the session data and authentication results should be captured at the VASP, unless this is outsourced to a third party.

There might be additional authentication processes such as OTP and two- or multi-factor authentication. This data will most likely be stored at the VASP but, again, could be stored at a third party vendor.

b. Is the authentication data you capture relevant to ongoing anti-money laundering and counter terrorist financing due diligence and/or transaction monitoring? If yes, how?

We agree that the authentication data captured is relevant to ongoing anti-money laundering and counter terrorist financing because it is necessary for CDD and transaction monitoring.

For example, IP address, geo-location, and device information data can be collected, stored and compared on an ongoing basis during the lifecycle of the client relationship. Risk-based assessments should be updated to reflect the risks associated with the use of digital ID systems. For example, it may be appropriate to trigger alerts when the same device information is shared across multiple accounts (which could be an indication of attempted money laundering by bad actor controlling multiple accounts having previously enlisted straw persons to set up accounts) or the IP address used to login is in a different country to the customer's country of residence and historical IP address logins (which could be an indication of account takeover).

Additionally, sanctions lists have evolved and capture more data points relevant to sanctioned individuals (including virtual asset payment addresses). Digital ID systems may enable the capture and monitoring of these attributes.

The data captured will enable more informative Suspicious Activity Reports (SARs), and responses to enforcement information requests and subpoenas.

The richer and more robust dataset will likely enable future automation initiatives to better detect suspicious activities like money laundering and terror financing through techniques such as predictive analytics, machine learning and AI.

### 3. How can digital ID systems support financial inclusion?

a. How can digital ID systems with different assurance levels for identity proofing/enrolment and/or authentication be used to implement tiered CDD, allowing clients a range of account functionalities depending on the extent of CDD performed, and particularly in situations of lower risk? Please provide any practical examples

While we agree with the principle of tiered CDD, we disagree with the statement that "*Lower risk ML/TF situations may permit use of digital ID systems with lower levels of assurance for the purposes of simplified due diligence" (paragraph 164).*

Specifically, we are not convinced digital IDs with low(er) levels of assurance are appropriate for performing CDD – even in situations of lower ML/TF risk. While establishing strong assurance levels is by no means easy, alternative means for verification of identity and underlying information using "trusted referees", combined with the reliable technical authentication means described in paragraph 181, offer a pathway to higher assurance levels for digital ID systems in a financial inclusion context. The acceptance of a digital ID as the centerpiece in a CDD process should be predicated on the ID meeting a minimum, high assurance standard.

Overall, the guidelines would benefit from a more comprehensive and consistent treatment of "assurance levels" and a clear description of the difference between the various types of "lower levels of assurance". For example, paragraph 164 refers to the assurance level of a digital ID as its "technical reliability", whereas paragraph 163 implies the absence of a *permanent address* corresponds to a "lower level of assurance". The latter statement is somewhat contradicted by the evidence cited in Appendix E (NIST Digital ID Technical Standards), which states that there may be *high confidence* ID evidence is genuine, accurate and that it relates to the applicant in "*instances where an individual cannot meet conventional identity proofing requirements, such as identity evidence requirements, [as long as a] trusted referee [is] used to assist in identity proofing the applicant.*" Settling on a single FATF definition of assurance levels could make the final guidance easier to interpret.

With respect to the decision process flow described in Figure 1, we agree that an assurance assessment should take place prior to the adoption of a digital ID system. What is not reflected in this figure, however, is a distinction between a *digital ID* and a *digital ID system*. The two terms are used interchangeably but we believe they refer to different things (a system might provide adequate assurance whereas digital IDs must still be evaluated for compliance with a digital ID framework on an ongoing basis).

Finally, assurance levels of digital ID systems are not static. We would consider it helpful to add a note in the guidance about the need to regularly review the assurance assessments of digital ID frameworks – even those explicitly approved by governments. One researcher recently demonstrated the relative ease with which the passwords required to open PDF documents linked to Aadhaar identities can be guessed. It is incumbent upon regulatory bodies to consider such unforeseen risks and put in place a regular audit process for assurance assessments.

b. Have you adopted lower assurance levels for identity proofing to support financial inclusion? What additional measures do you apply to mitigate risks? Please provide any practical examples.

We are not aware of any instances where GDF members have adopted lower assurance levels for identity verification with respect to digital IDs in order to support financial inclusion. Such an approach would likely be perceived as incurring significant regulatory risk, given the nature of existing AML / CFT regulations.

However, we note that there are instances in the broader fintech industry where lower assurance levels for identity verification are mitigated by limits on customers' activity. For example, many Mobile Network Operators support customers who have limited identity documentation on a "cash in / cash out" basis.

c. How can progressive CDD via digital ID systems aid financial inclusion (i.e. establishing greater confidence in a customer's identity over time)?

We agree with the observation made in paragraph 166 that the application of progressive CDD through digital ID systems can aid financial inclusion. The expansion of digital financial services can be supported with the implementation of a tiered approach: giving customers with incomplete KYC profiles access to financial products with limits on the amounts, velocity, or volume of transactions.

We believe that adding the following two clarifications can aid in the successful application of the progressive CDD principle:

- **Potential use of machine learning to verify customer identity**
  While the guidance in paragraph 31 states that machine learning can be used to determine the validity of government identification, GDF members also view opportunities to apply machine learning to help verify a customer's identity. One method for doing this is by validating the consistency of transaction and behavioral data with customer data provided during customer onboarding. Particularly in the context of digital IDs, machine-learning algorithms can effectively sift through data and assign confidence levels to a customer's identity. Crucially, these types of analyses can facilitate the kind of automated, frictionless authentication process that customers prefer, because they don't require significant effort on the customer's part. This could encourage the adoption of digital IDs. We consider it worthwhile to add to paragraph 107 a section on how machine learning can be used to establish greater confidence in a customer's identity over time.

- **Alignment of risk models to the local context**
  One of the prerequisites for performing a simplified due diligence is an assessment of low ML/TF risk. One complication that arises in an emerging market setting is that traditional customer risk rating models (CRR) might flag low-risk customers as high-risk due to their frequent use of cash transactions and the sensitivity of traditional CRR to cash-based transactions. This can result in a large number of false positives, which makes the task of employing a progressive approach to CDD difficult. Or, worse, this might result in no robust risk assessment taking place at all or the ignoring of potential ML risk signals. We therefore recommend adding a reminder to paragraph 167 about the importance of applying CRR and adapting risk screening methods to the local context in order to encourage the responsible use of progressive CDD.

## 4. Does the use of digital ID systems for CDD raise distinct issues for implementing the FATF record-keeping requirements?

a. What records do you keep when you use digital ID systems for CDD?

As discussed in 2(a) above, beyond standard CDD record keeping requirements, record keeping should fall into three broad categories:

- biodata about the client contained in the ID (e.g., Name and Date of Birth) and ID document information (e.g., document ID number and document ID type),
- session data (e.g. IP address, geo-location, and device information data), and
- authentication test results performed by the third party provider on the captured data.

As the FATF is aware, VASPs are at various stages of maturity in terms of CDD compliance to the updated FATF Recommendation 15 issued in June 2019, as is the regulatory framework in each country. As such, it can be expected within the VASP community at this time that firms will vary on the degree to which this information is collected.

b. What are the challenges in meeting record-keeping requirements when you use digital ID systems for CDD?

One key challenge in meeting record-keeping requirements when using digital ID is storing of the underlying identity document. When using a third party digital ID service provider, on occasion all that is received back is a score on the reliability of the identity that the customer has produced. The original identity remains with the service provider. Other solutions being produced on the blockchain only provide an authentication key as evidence that the ID can be relied upon. This, then, has implications on requirements to maintain a copy of the customer's identity document; the ramifications being that in the event law enforcement requires a quick response from a VASP as to the identity of an individual to support a case of critical urgency, the VASP would be unable to provide this.

Inequality in record-keeping requirements across jurisdictions also cause issues with respect to VASPs' compliance to regulations. For example, some jurisdictions require on-soil storage which may mean for an international VASP the complexities of processing and storing such data may outweigh the benefits of entering a particular market.

Finally, security also poses an issue with regards to maintaining records for VASPs. Given the online nature of such data, and reliance on third party service providers, considerable investment should be made to ensure that such data is appropriately ring fenced and stored in a way to protect it from misuse. This is particularly prevalent as an issue for VASPs where blockchain analytics permit the lookback of transaction history on the public blockchain which, if it can be associated to an individual, could present considerable data privacy issues.

c. If you keep different records when using digital ID systems for on-boarding, does this impact other anti-money laundering and counter-terrorist financing measures (for example ongoing due diligence or transaction monitoring)?

The growth of adoption of digital ID for CDD could potentially vary the type of data available for transaction monitoring and may increase the amount of data which needs to be stored. Digital ID data obtained during onboarding can be an additional beneficial data set which could be utilised during ongoing transaction monitoring activities.

We hope you may find our response helpful. Please do not hesitate to contact our Executive Director, Teana Baker-Taylor (Teana@gdf.io) or either of our AML working group co-chairs, Malcolm Wright (malcolm@gdf.io) or Jack Gavigan (jackgavigan@z.cash) for further questions or comment.

## Consultation Response Contributors

The following table lists contributors to this response who wish to be identified. The full list of contributions from the GDF AML Working Group may be larger.

| Name | Organisation |
|---|---|
| Malcolm Wright | CCO, Diginex<br>AML Working Group Co-Lead, GDF |
| Jack Gavigan | Head of Regulatory Affairs, Electric Coin Company<br>AML Working Group Co-Lead, GDF |
| Dominic Gee | Independent Contributor |
| Simon Roberts | SCP Consultants |
| Thomas Borrel | CPO, Polymath |
| Lana Schwartzman | CCO, Paxful |
| Nicolaas Koster | Product Manager, ConsenSys |