

November 27, 2019

Mr. David Lewis
Executive Secretary
Financial Action Task Force
2 Rue André Pascal 75116
Paris, France

RE: Public Consultation on FATF Draft Guidance on Digital Identity

Dear Mr. Lewis:

The Institute of International Finance (IIF) appreciates the opportunity to provide input to the Financial Action Task Force (FATF) as it works to address many of the key issues facing the global financial community today. As a permanent member of the FATF Private Sector Consultative Forum (PSCF), we strongly support the FATF's efforts to address how digital identity systems can be used for customer due diligence (CDD). We welcome the FATF draft guidance on digital identity and believe it will be a useful resource for financial institutions and regulators engaged in this area of technological advancement. Internationally aligned measures such as this will assist joint public and private sector efforts in identifying areas of digital identity which contribute to better Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) regimes, while at the same time enhancing financial inclusion globally.

We believe digital identities hold great promise in contributing to financial inclusion, financial crime prevention, and improved customer experience at onboarding. We particularly welcome the draft guidance clarification that non-face-to-face on-boarding may be standard risk, or even low-risk for remote customer identification and authentication.

As part of a three-part series, the IIF has so far published two papers on digital identity:

1. "Embedding Digital IDs in AML Frameworks"¹ focuses on considerations for international standard setters and regulators on how digital IDs can help CFT and AML;
2. "Responsible Digital IDs"² articulates how the emerging digital identity ecosystem can increase access to finance and financial inclusion.

Overall, we consider the draft guidance to be reasonably comprehensive in its approach, and it aligns with the key themes we have emphasized through our work in helping governments, financial institutions, and other relevant entities apply a risk-based approach to the use of digital

¹ Delle-Case, A. and Carr, B. (2019). *Digital IDs in Financial Services Part 1: Embedding in AML Frameworks*. [online] iif.com. Available at: <https://www.iif.com/Publications/ID/3534/Digital-IDs-in-Financial-Services-Part-1-Embedding-in-AML-Frameworks>.

² Khairy, A., Carr, B. and French, C. (2019). *Digital Identities in Financial Services Part 2: Responsible Digital IDs*. [online] iif.com. Available at: <https://www.iif.com/Publications/ID/3596/Digital-Identities-in-Financial-Services-Part-2-Responsible-Digital-IDs>.

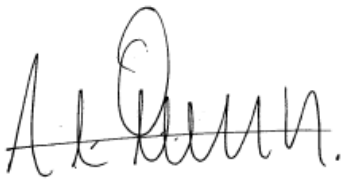
identity for CDD. However, topics such as the use of multiple reliable ID sources, creating interoperable digital IDs, and ensuring personal information security are some of the areas where there is opportunity for the guidance to be further and dynamically updated by the FATF in order to remain relevant in this increasingly transformative space.

It would also be worth providing guidance on the use of digital identity in the onboarding processes of legal persons, which would share many of the potential benefits described in this draft guidance for their use by natural persons.

Lastly, we reiterate our support for this process of public consultation by the FATF. As with other changes or updates to the standards or guidance documents issued by the FATF, we strongly believe the ultimate goals of the task force, and the wider financial, regulatory, and law enforcement community will be better advanced through the institutionalized solicitation of stakeholder feedback in a clear and transparent fashion.

As always, we stand ready to provide further information as required and would welcome the opportunity to arrange a meeting between the IIF, the FATF Secretariat and other relevant stakeholders to discuss our comments in more detail should that prove helpful. Please do not hesitate to contact me or Amin Khairy at akhairy@iif.com with any questions which may arise.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'A. Portilla', with a large, stylized initial 'A' and 'P'.

Andrés Portilla
Managing Director
Regulatory Affairs

Public Consultation on FATF Draft Guidance on Digital Identity

Key Issues:

Overall, the draft guidance correctly and adequately links key AML/CFT priorities in the context of CDD with identification concepts, and we appreciate the clear recognition that the risk-based approach to AML/CFT can be tied to levels of assurance of identification. The draft guidance gives a strong description of international standards and examples of various country models and has an important and highly welcomed focus on financial inclusion. As digital identity is an evolving technology, regulation related to the technology will need to be dynamic and agile. Having the right principles enshrined and complemented by guidelines that can be updated regularly as technology and circumstances evolve will be crucial. Hence, we recommend that the guidance be regularly (i.e., annually) reviewed and updated with the FATF's national members following similar approaches within their jurisdictions.

It should also be noted that institutions' use of digital identity should be voluntary, and they should have the choice to also use traditional physical identification or transaction monitoring if preferred.

The IIF also suggests that banks and regulated entities, and not service providers offering digital identities, be the ones supervised by authorities. We recommend that the FATF refines the guidance to focus on the appropriate regulation of banks and regulated entities, and their use of digital identity solutions which adhere to well-defined international standards and frameworks. These standards include those put forth by entities such as the National Institute of Standards and Technology and the International Organization for Standardization as mentioned in the draft guidance. The unintended consequences of regulating service providers could include stifling their ability to innovate and deploy technology which improves the robustness of digital identity solutions. Authorities would retain the right to audit use of digital identity service providers by regulated entities and would thereby have an indirect supervisory remit. Additionally, disparate national regulation could make it even more difficult for service providers to provide their solutions at scale across international borders, which could limit the effectiveness of those solutions.

Finally, it is worthwhile to mention that the FATF should remain technology neutral, highlighting good examples and not favoring any technology or specific technological requirements for digital identity to be used for AML purposes.

Our comments herein reflect areas where there is opportunity for the guidance to be further developed to remain relevant in this increasingly evolving space. The main areas we believe could be further improved are: 1. Recognizing the value of multiple reliable sources of identification; 2. Emphasizing the need for interoperable digital identity systems; 3. Asserting the importance of consumer protection; 4. Reframing the reasoning of having a two-tiered CDD process for low-income segments; 5. Highlighting the usefulness of a private to public feedback loop and; 6. Revision of the reliance framework.

1. The value of multiple reliable sources for identification

The draft guidance places a focus on a government-issued identification model, or official identification. It acknowledges federated approaches to identification that use other reliable sources; however, it limits the breadth of options by requiring only one degree of separation from a government-verified source. This can cause an over-reliance on government-approved identification models, thereby limiting financial inclusion in many countries where few citizens have official IDs. Financial inclusion could increase with the use of alternative forms of ID, such as mobile phones. For example, the number of mobile phone subscribers surpasses the number of citizens with government-issued identification in many countries. If digital ID frameworks could incorporate mobile phones into their identification approach, many more individuals could gain access to financial resources.

The draft guidance should recognize that government-sourced identification is highly valued as it has the strongest basis in law. Government-issued IDs are the most reliable sources of identification in higher risk client scenarios and are significant supportive tools for lower risk clients, products, and services. The FATF should encourage governments to provide reasonable means and methods to validate the integrity of a digital identity against government systems, and corrupted identification records (e.g., a list of lost/stolen IDs) should be made available to any regulated entity to confirm the authenticity of their records. Such information sharing should be done securely with controls on access and can alternatively be done on a case-by-case basis, with governments confirming whether a given document is invalid.

Another valuable approach would be suggesting the importance of opening access to government controlled “golden-source” data, as an important component of digital identity services. Having the FATF highlight the need for controlled access to government datasets could help drive this through the respective legislative processes of individual countries. It therefore makes sense for the FATF to highlight the importance of controlled access to government datasets as a possible essential component of multi-layered digital identity service. Some examples of these could be citizen data, immigration records, corporate registries, birth and death records, etc.

It is also important that the draft guidance recognize that a person’s identity is not limited to transaction identification and monitoring, but could potentially be formed and validated by their trusted digital relationships (such as with, *inter alia*, the government, financial systems, family members, health systems, and public utilities). Multiple reliable sources of identification should be acknowledged as important in supporting an adequate risk-based approach model and strengthening identification. The acceptance of multiple reliable sources of ID will improve issues relating to financial inclusion as it will enable low-income segments who lack government-issued IDs to be served. Hence, we recommend developing the definition of “reliable sources” and instead of putting a heavy reliance on government-issued ID models, the definition should be defined more broadly to incorporate other sources of identification. However, it is important to mention that non-governmental IDs should not be considered as having the same order of

certainty as government IDs. They are powerful supplements to official IDs but cannot replace government IDs.

In order to maintain and strengthen the current AML framework, identification with digital identity should be as secure and accurate as possible. Therefore, in our view there must at least be some state certification and supervision to guarantee reliability and that the data used for establishing the digital identity comes from a trusted or certified entity. Self-declared identities should not qualify for AML identification purposes.

2. Interoperable digital identities

The draft guidance discusses international standard setting bodies working on interoperability; however, this can be viewed as inconsistent with requiring “official identification” which is limited to government-issued or certified methods. Even though a passport or an international driver’s license may be an interoperable identity, countries with more complex systems (federated models) may be shut out of financial systems or more susceptible to criminal manipulation of systems as a “weak link.” International identity resolution is of significant value in providing traceability of international sources of funds and sources of wealth to meet customer due diligence expectations which can act as an effective tool when identifying criminals that work across multiple borders.

The guidance does a good job of highlighting the importance of having appropriate levels of assurance and confidence for digital identity providers, but with the increasing use of multiple reliable data sources, we recommend that the draft guidance acknowledge the importance of alternative data sources (other than legal/government-issued documents) that will have a substantive role in profiling, predicting customer behavior, and fostering an interoperable ecosystem. Recognizing the importance of multiple identity capture tools to assist in global interoperability is a reliable tool in a risk-based approach. There should also be a way to cross recognize digital identities issued by different vendors as they might be governed by standards that are not on par with international standards.

With the increased use of individuals’ various digital data sources, we recommend the creation of key principles to act as guidance to classify third-party authenticators/validators to ensure interoperability. Having a framework that describes how issuers, authenticators, and managers of digital identity could potentially utilize multiple data sources (through their own resources or through third-parties) will be important for detecting fraud, enhancing financial crime risk management frameworks, and furthering financial inclusion in a reliable and interoperable manner.

We suggest that this framework use a risk-based approach i.e., customers would need to be validated, authenticated, and served according to their risk profile. High-risk customers would need to provide the appropriate validation documents (high assurance levels) such as government-issued IDs while lower risk customers could be served using other documents (low assurance levels) such as e-commerce transactional data or digital bill payment histories. By

categorizing and setting principles on what can be considered high and low standard sources of identification, the FATF guidelines would be up to date with the evolving digital identity ecosystem. We also recommend creating a committee under the FATF Policy Development Group to monitor and review (with ongoing engagement with the private sector) the underlying information required for digital identification and digital KYC systems.

Having interoperable systems (whether cross-sectorial or cross-jurisdictional) will greatly enhance the ability to identify criminals and ensure a seamless transactional experience. We acknowledge that creating fully interoperable systems is something that is not easily achieved and the appetite for it can be different depending on the jurisdiction, however, clearly stating that an interoperable system will enhance the identification process would be a welcome observation in the draft guidelines.

3. Data privacy and data retention

Given that the digital ID concept is a compilation of a person's most personal information, the process through which it is generated, stored, and potentially transferred needs to be as transparent as possible.

Safeguarding customer privacy is another area we believe needs further emphasis in the draft guidance. Regulated entities should have the appropriate legal basis for processing personal data to comply with its AML/CFT legal requirements. However, when customers' personal data is processed for other purposes, gaining a customer's consent when using, sharing, and managing their personal data will be important to ensure that the data is not misused in any way. We acknowledge that for AML and CFT purposes, consent on using information creates a dilemma, however, this can be mitigated by giving people the choice to share certain datapoints based on the service they want to receive and the jurisdiction in which they are located, while at the same time providing regulated entities ways to ensure compliance.

Financial institutions value the trust their customers place in them, and any new form of interaction must ensure that the customer remains in control of his/her personal information. Regardless of who is involved in a digital ID framework, the customer must be confident that his/her information is secured, kept safe from illegitimate access, and transferred only with the customer's consent or if there is a legal basis to do so. The draft guidance does not adequately cover the concept of digital credentials within the context of self-sovereign identity. Given the additional benefits these systems could provide – especially in an environment of increasing sensitivity to data privacy and security – we would welcome further guidance or clarity on the approach to such mechanisms as self-sovereign identity in the context of CDD. Additionally, strong standards must be in place to determine to what ends information may be processed and how it can be used.

Data retention is also an area where the draft guidance could be further developed by emphasizing the importance of keeping and sharing certain traceable transactional data versus all the customers data. When creating interoperable systems, sharing information on

customers can also be done in a form of sharing the validation of a customer instead of the underlying information that led to the verification/authentication process.

4. Reframing the two-tiered CDD process reasoning

The draft guidance emphasizes a two-tiered CDD process that would apply lower standards to low-income segments. This approach, however, may introduce new risks to the system and result in entrenching differences in society and financial services. We recommend the guidance instead applies a harmonized approach to support financial inclusion.

The underlying assumption in the guidance is that newly banked and vulnerable groups often present a lower AML/CFT risk as they often conduct a limited number of basic, low-value transactions. However, we observe that these groups in fact represent a very diverse category with very different risk profiles in different jurisdictions and therefore should not be classified uniformly as lower risk clients simply because they are low income individuals. The emergence of lower tier requirements (a parallel due diligence system) to provide access to basic financial products for lower income segments could inhibit their growth and integration into the broader economy through mainstream financial services.

The financial services industry has sound policies and regulations in place to conduct proper due diligence, protect personal information, reduce the risk of data being misused by criminals, and ultimately ensure financial stability. However, the risk of running afoul of these regulations, and the will to reduce the risk of exposure to financial crime, has also contributed to de-risking practices, with firms limiting their business in certain markets and product offerings. These practices can restrict low-income segments of the population from gaining access to finance. In response, we observe that lower tier requirements have been created in some places to provide access to basic financial products while creating a parallel due diligence system for lower income segments.

Even though lower tier requirements could facilitate onboarding procedures, we believe having different standards for different income groups will de-harmonize financial services frameworks, jeopardize financial crime risk mitigation, and will not automatically result in broader access to the full suite of financial services and products. Additionally, relegating these customers to a separate system could inhibit their growth and integration into the broader economy through mainstream financial services.

5. The importance of a private/public sector feedback loop

As detailed above (point 3), the privacy and protection of the data subject is non-negotiable. To realize the potential of digital IDs to fight financial crime and illicit behavior, these rights need to be balanced against the legitimate interests of processing and sharing information to prevent illicit financial flows.

We recommend that the guidance highlight the importance of having a feedback loop between the private and public sectors to improve the digital identity framework, enhance financial crime risk management, and address financial inclusion loopholes. The cooperation between the public and private sectors to distribute relevant information about suspicious activity would allow other players in the industry to better deal with the threat of potential criminals, especially if one of the financial institutions that shares the same customer has identified an illicit behavior that needs to be reported to a financial intelligence unit (FIU).

Financial institutions are required to file suspicious activity/transaction reports (SARs/STRs) with their respective FIU, but very rarely learn of the outcome. Therefore, they rarely know if they have been right to raise a concern or if the report was unnecessary. In practice, should a customer relationship not be terminated despite a SAR/STR filing (because it would “tip-off” the customer), this customer will usually be treated as high risk. The institution will not know if this is warranted or when to remove such a flag (or terminate the relationship). A digital ID can help as it (or a reference number attached to it) can be shared with the public sector. It provides a technical “hook” that could be attached to a case file with law enforcement, which could return updates on the progress to the financial institution that filed the case, without straining resources on both sides.

Hence, we recommend that the FATF encourage the stakeholder community to continue to explore means of sharing feedback based on SARs/STRs to either confirm a filing or clear the name of a customer who might have been the subject of undue suspicion. In the latter case, there is no reason for this customer to have to suffer the negative consequences indefinitely.

6. Revision of the reliance framework

Every financial institution wanting to engage in a business relationship with the same person conducts its own full identification and CDD process, with the obvious drawbacks on efficiency, data quality, and consistency of information. Financial institutions should be able to rely on an identification performed by another regulated entity regarding the same customer. The draft guidance should suggest the assignment of a digital ID to a customer or enable the verification and sharing of the customers’ ID, assuming these have occurred according to international standards and in accordance with relevant laws and regulations on information exchange. Institutions should be able to rely on the work of others even if the original identification has occurred at an earlier stage without the intent to identify for the benefit of a third party, provided that they are comfortable with the identification standards applied or deciding to what level it wants to rely on the information.

In order to make an informed risk-based decision, it would be helpful if the standards to which the identification occurred originally are disclosed to the receiving entity. If international standard setters define the minimum standards to be applied in adequate detail, there would be less risk of losing interoperability due to diverging expectations. For financial institutions, a gradual approach of determining which national processes to deem adequate from a risk-perspective could be a way forward.

When relying on third parties such as vendors and KYC utilities to generate and transfer the digital ID or single attributes that make up the digital ID, the standards and prevention of breaches must be equal to those of financial institutions. Any third party that wants to provide the financial sector with crucial information about customers must be aware of the responsibility to produce the highest standards of quality and what the consequences of wrong data are.

Having a consistent level of data quality and care will also increase the chance of financial institutions working with such entities.

Further Specific Comments:

The specific comments below do not fall under any of the previously iterated general comments and can be considered as in-line recommendations to the draft guidance:

- Executive summary under recommendations for regulated entities (point 26): the term “enabling authorities” should be defined. Point 26 makes the case for sharing underlying information to verify and identify individuals. The underlying information of an individual can be sensitive information and should only be shared with defined enabling authorities.
- Executive summary under recommendations for digital ID providers (point 27): We recommend that if a digital ID is issued by a certified and tested service provider the need for keeping CDD records diminishes.
- Executive summary under recommendations for digital ID providers (point 28): Clarification of whether testing and certification is required for each jurisdiction where digital ID service providers operate would be helpful.
- Section 1 (point 35): More elaboration is needed on who will ensure that digital IDs are reliable and independent and how to hold service providers accountable in case digital IDs are not reliable and independent.
- Section 1 (point 36): We recommend a brief description on how large-scale digital ID systems (that do not meet appropriate levels of assurance) are identified.
- Section 2 (point 43): It is important to note that the digital ID is for the natural person and serves all individuals, regarding of whether they are account holders of beneficial owners or not.
- Section 2 (point 49): It would be helpful if we can clarify what is meant by “state” and if this means the official issuing country
- Section 5 (Point 150): Section 5 (Point 150): It would be helpful to clarify what level of assurance assessment regulated entities will be required to perform to determine the reliability and independence of the digital system. Regulators across different jurisdictions may have different standards. As such, if regulated entities are required to determine the reliability and independence of the system themselves, there should be guidance on what is considered an “acceptable” assessment that can be applied internationally.