BANK POLICY INSTITUTE

November 29, 2019

*Via Electronic Mail*

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

Re: Public Consultation on FATF Draft Guidance on Digital Identity

Ladies and Gentlemen:

The Bank Policy Institute[1] welcomes the opportunity to comment on the Financial Action Task Force's "Draft Guidance on Digital Identity." We appreciate the FATF's efforts in this consultation to assist public and private sector entities' interest in "determin[ing] how digital ID systems can be used to conduct certain elements of customer due diligence" under the FATF's recommendations.[2] BPI members are committed to assisting public sector efforts to detect and prevent money laundering and the financing of terrorism, and thus strongly support the fundamental principles underlying the FATF's CDD expectations.

As an initial matter, in the United States, banks are subject to robust CDD expectations, which includes requirements under Section 326 of the USA PATRIOT Act[3] that financial institutions implement a customer identification program (CIP) that includes reasonable procedures for: (i) verifying the identity of any person seeking to open an account, to the extent reasonable and practicable; (ii) maintaining records of the information used to verify the person's identity, including name, address, and other identifying information; and (iii) determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency.

While digital identity is in various stages of development around the world, including the U.S., BPI members share FATF's view that it has the potential to "strengthen[] CDD and AML/CFT controls, increas[e] financial inclusion, improv[e] customer experience, and reduc[e] costs for regulated entities." In addition to the potential gains that such technology could realize, particularly for AML and sanctions compliance-related know-your-customer expectations, U.S. financial institutions have the benefit of being able to leverage regulatory pronouncements, such as the *Joint*

---

1 The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

2 FATF "Draft Guidance on Digital Identity," October 2019, pg. 1, *available at* http://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html.

3 Section 326 was codified as 31 U.S.C. § 5318(l).

*Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing*, when exploring the potential of such technology.[4]

As an initial matter, we note that the draft guidance states that it does not cover the use of digital ID systems to verify legal representatives or beneficial owners. However, where digital IDs are available for these parties, we recommend that the final guidance reflect that regulated entities do have the ability to utilize such technology for verification purposes, as their coverage is likely to further the policy goals expressed by the FATF, particularly when such verification is required by law in a particular jurisdiction. Furthermore, the guidance raises the possibility of regulated entities internally detecting the systematic misuse of digital IDs. This is most likely to occur through the normal course of business, stemming from ongoing monitoring and related AML expectations, therefore we recommend that the FATF affirmatively note this connection in its final guidance. Finally, from a policy perspective, it will be necessary for any digital ID system to appropriately balance the accurate verification of customers with other policy interests, such as financial inclusion. While the standards for obtaining a digital ID may take different forms, as a general matter, they should reasonably correspond with expectations for other forms of ID.

From a global perspective, the interoperability of different digital ID solutions, as well as the designation or coordination of entities responsible for its standards and oversight, will similarly be an important component of the widespread adoption of digital identity as well as the ultimate realization of the AML/CFT gains expressed above. In particular, allowing governments to solely assess digital ID assurance levels, given the potential for variation of digital ID systems across jurisdictions, would make it difficult for regulated entities that operate globally to have a consistent approach to accepting digital IDs for identity verification. Therefore, we recommend that the final guidance recognize this connection and note that regulated entities are to be part of any government-sponsored digital ID assessment discussions.

While U.S. policymakers are starting to focus on the potential benefits of digital identity and whether a government-sponsored solution is achievable, it's acknowledged that the private sector will have to play an active role in the development of any digital identity solution, whether publicly or privately operated.[5] We note that some of the country cases in the FATF's draft guidance support the development of a private sector-led solution, which could potentially be leveraged, using a utility model, to assist institutions with KYC requirements, including those associated with U.S. sanctions program screening expectations. However, no matter the operator, fundamental components will need to be addressed by both the public and private sectors before the adoption of such technology is viable. This includes the information collection expectations necessary to confirm identity, the verification mechanisms, the procedures for updating and retaining such information, consumer privacy and data security protections, audit processes, expectations for using digital IDs in ongoing monitoring and, as necessary, the ability to rely on third-party or other providers.

Maintaining the flexibility to adopt and implement such technology is key to ensuring its utility. Therefore, any final guidance produced by the FATF must be principles-based and not overly prescriptive. We encourage continued discussions among and between the public and private sectors, including AML/CFT standards setters, and are willing to be of assistance to the FATF and relevant regulatory agencies as conversations on the adoption of digital identity progress.

---

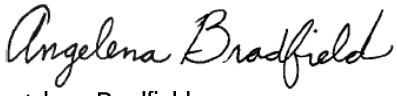
4 Board of Governors of the Federal Reserve System, et. al., "Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing," December 3, 2018, p. 2, *available at* https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf.

5 *See* Department of the Treasury, *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation*, July 2018, *available at* https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf. The report states that "[p]ublic and private sector stakeholders need to work together to develop trustworthy digital legal identity products and services for use in the financial sector and elsewhere."

* * * * *

The Bank Policy Institute appreciates the opportunity to submit comments on the FATF's draft digital identity guidance. If you have any questions, please contact the undersigned by phone at 202-589-1935 or by email at *Angelena.Bradfield@bpi.com.*

Respectfully submitted,



Angelena Bradfield
Senior Vice President, AML/BSA, Sanctions & Privacy
*Bank Policy Institute*