International Banking Federation

5th Floor, One Angel Court
London EC2R 7HJ
United Kingdom
+44 7725 350 259
www.ibfed.org

Mr. David Lewis
Executive Secretary
Financial Action Taskforce (FATF)
2 rue Andre Pascal
75116 Paris
France

7 December 2020

Dear Mr Lewis,

Re: FATF questionnaire on digital transformation

The International Banking Federation (IBFed)[1] appreciates the opportunity to comment upon the FATF questionnaire on digital transformation.

As you know, the International Banking Federation (IBFed[1]) is the representative body for national and international banking federations from leading financial nations around the world. This worldwide reach enables the IBFed to function as the key international forum for considering legislative, regulatory and other issues of interest to the banking industry and its customers. We also have a keen interest in the efficiency of the global tax system.

From an international banking perspective, it is clear that there are potentially valuable financial crime use cases for technology that are not being fully utilised due to a combination of legal barriers, regulatory challenges and varied commercial risk appetite. In our comments we focus on legal and

[1] The International Banking Federation (IBFed) was formed in 2004 to represent the combined views of our national banking associations. The IBFed collectively represents more than 18,000 banks, including more than two thirds of the largest 1,000 banks in the world. IBFed member banks play a crucial role in supporting and promoting economic growth by managing worldwide assets of over 75 trillion Euros, by extending consumer and business credit of over 40 trillion Euros across the globe, and by collectively employing over 6 million people. The IBFed represents every major financial centre and its members' activities take place globally. With its worldwide reach the IBFed is a key representative of the global banking industry, actively exchanging with international standard setters and global supervisory bodies on subjects with an international dimension or with an important impact on its members.

regulatory barriers to the use of emerging technology for sharing information between regulated banking firms for AML/CFT purposes.

A significant challenge for jurisdictions around the globe, and one that is becoming increasingly important for policymakers to address, is the growing conflict between the need to share information for law enforcement purposes and the growing legal restrictions designed to protect the privacy of individuals. The ability to share information and intelligence is becoming increasingly important as technological advances increase the speed of financial transactions. This general issue is recognised by FATF Recommendation 9, which states that "Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations." More recently, the EU AML Action Plan has recognised regional differences in the legal frameworks and practical arrangements across Member States on financial crime information sharing, proposing to develop EU-level guidance on how public-private partnerships can meet data protection requirements.

Financial crime information sharing is restricted in many different markets by a misalignment of AML/CFT intelligence needs and data privacy requirements. While the specific restrictions may vary in line with local law and supervisory expectations, the overall effect is of international regulatory fragmentation with the regulatory banking sector left to manage the tension between inconsistent expectations.

- GDPR - As noted by the European Banking Authority, while EU Money Laundering Directives specify that processing of data for AML/CFT purposes is a matter of public interest, and GDPR allows processing necessary for such matters of public interest, the permitted extent of AML/CFT processing is not defined in detail. This lack of explicit alignment has led to varied national interpretations and legal uncertainty, for example over group-wide sharing of information on individual customers.

- Right to be Forgotten – Another example of this tension is where data privacy regulation grant individuals specific rights in data that is collected about them. Under certain regulations, companies are expected to provide appropriate access to the information they collect, transmit and retain about individuals. The intent is to grant individuals access to that data along with steps to allow individuals to request correction and deletion of inaccurate and unnecessary information. The tension arises from the attractiveness of such requests to fraudsters and other criminals who want to delete damaging or unfavourable information about their activities. Without clear international standards on the retention of information directly relevant to financial crime risks, there is a concern of fragmentation in national approaches and consequent inconsistencies in how international banking groups and commercial providers handle such data, which would have significant adverse impacts on both accessibility and data quality.

- Data Sharing, Pooling and Analysis - Probably no other area of banking requires such a wide range of data for decision making as AML/CFT and the prevention of financial. Machine learning and wider 'AI' technologies in particular requires the availability of large amounts of

data in order to achieve the necessary learning effects. However, such forms of data pooling raise complex data privacy issues and in many jurisdictions there is no clear and agreed legal basis for such data processing. International and regional standards in this area could support not only more effective national approaches, but could also enable cross-border information sharing, including through cross-border utilities and other innovative technological solutions and through enabling collaboration between both national-level and regional-level public-private partnerships.

This misalignment is driven by a trend of government policy silos between financial crime and data privacy. Some countries have started to address this through policy roundtables to bring together AML/CFT supervisors, data privacy authorities, the regulated sector and RegTech innovators. These policy roundtables can help to define the specific use cases and barriers to the adoption of innovative technologies, and develop the right mix of solutions across regulatory policy, clarificatory guidance and industry collaboration. Addressing policy silos through bringing financial crime and data privacy together can also support higher-level work to support technology-neutral regulation, such as through the definition of framework conditions capable of supporting diverse advanced technologies and varied business models.

- A number of jurisdictions already support AML/CFT innovation through TechSprints to collaborate on the trial and development of new technological approaches, and through regulatory sandboxes to trial new products in live supervised environments. The UK Economic Crime Plan builds on this approach through the establishment of an Innovation Working Group of government, industry, their AML/CFT supervisor and the UK data protection authority. This Group meets regularly to identify and review barriers to the adoption of innovative new financial crime solutions that could increase effectiveness and efficiency and agree solutions to addressing these barriers. These approaches have been used to explore and support the use of Privacy Enhancing Technologies, among other technologies, across a number of financial crime use cases.

International action is needed to address this misalignment, as it undermines international banking groups' ability to identify and manage financial crime risk and provide valuable intelligence to support law enforcement disruption of serious criminality. FATF best practice on information sharing is welcome but has not led to a significant mitigation of the legal and regulatory inconsistencies faced by international banking groups.

This is particularly important given that criminals and professional money launderers do not face the same legal or regulatory constraints in their use of technology. The increasing pace of digitalisation and financial innovation brings many benefits to customers, industry and wider society, but the misalignment of AML/CFT and data privacy policy has raised concerns that the legitimate private sector are falling behind in the race to exploit innovation for financial crime analysis and collaboration.

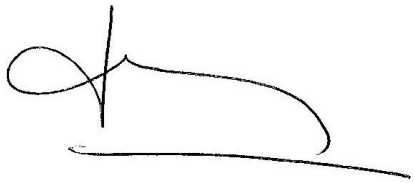
- The use of shared utilities is an example of technology-enabled information exchange between obliged entities, as highlighted by FATF in its Guidance on Private Sector Information Sharing. Combining efforts and collecting alerts from different financial institutions may enhance the effectiveness of reporting and may also develop intelligence patterns which can provide banks with the ability to prevent future crimes. In essence, one additional alert may often offer a more complete picture of another, thereby identifying criminal behaviour. Financial institutions only see a piece of the big puzzle which is often associated with complex financial crime schemes. The use of shared utilities could hence provide banks with the full pictures, which could in turn be disclosed to the FIUs.

- However, in most jurisdictions across the world, the existing AML/CFT rules most generally do not explicitly address and allow for centralisation of the transaction data collected by banks. Secure platforms hosted by trusted third parties and supported by governments under a robust legal framework may offer banks the capability to match KYC information stemming from different databases, without each bank having access to the other's datasets. They may also offer the possibility of setting up common transaction monitoring facilities allowing financial institutions to get a clearer picture of potential criminal activity. Nevertheless, in the absence of more detailed international standards, setting up such shared utilities faces many challenges, inter alia, concerning lack of legal certainty as regards outsourcing activities to third-party providers, legal grounds for processing of personal data, ensuring transparency vis-à-vis tipping off offences, and data minimisation requirements as prescribed by certain data privacy regulations.

From an international banking perspective, we consider that FATF should take explicit responsibility to address these policy silos, both directly at the international level and indirectly through demonstrating good practice for the regional and national level. We recommend that FATF should work with partners to establish international policy roundtables to bring together national, regional and international authorities on AML/CFT and data protection with the private sector.

We hope that our contribution is useful and would like to thank you for taking our input into consideration.

Yours sincerely,



Mrs Hedwige Nuyens
Managing Director
International Banking Federation