EBF_045274
29 November 2021

EBF Position on (Recast) REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information accompanying transfers of funds and certain crypto-assets

Key EBF messages on the Proposal:

The European Banking Federation (EBF) supports the objectives of the European Commission's Anti-Money Laundering and Countering the Financing of Terrorism Package which aims to strengthen the fight against financial crime in Europe. We believe that extending the rules on information accompanying wire transfers to virtual asset service providers and crypto-to-crypto transactions would contribute to achieving a level-playing field and has the potential to improve the traceability of transactions.

The EBF also welcomes the Commission's aim to achieve consistency of the EU legislative framework with international standards, notably with the latest amendments to the recommendations of the Financial Action Task Force (FATF), and particularly FATF Recommendation 15 on new technologies which pertains to the expansion of the scope of entities subject to AML/CFT requirements to include virtual asset service providers and the mitigation of risks deriving from their activities, as well as with Recommendation 16 on wire transfers.

While we are aware of the technical challenges that crypto-asset services providers (CASPs) face in complying with funds transfer regulation, we welcome and fully support the Commission's objective of establishing a level playing field. Regardless of the technical solution that CASPs implement to achieve regulatory compliance, the ultimate outcome must be aligned with the principles of payment transparency, which the EBF sees as core to an effective fight against financial crime.

On Subject Matter and Scope (Articles 1 – 3)

- The EBF highlights the importance of extending transparency requirements to CASPs in order to enable traceability of such payment flows and to achieve a level-playing field in furtherance of the principle "same services, same rules, same obligation". Blockchain-related technical challenges that CASPs face, for example in rejecting incoming transactions, must be overcome with solutions that while possibly distinct from traditional funds transfer regulation compliance processes,

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

ultimately achieve the same desired effect – clear information on beneficiary and originator in the moment. There are a series of regulatory requirements in fighting financial crime that rely on that basic expectation, from sanctions enforcement to providing law enforcement with quality investigative leads via high-quality suspicious activity reports. The need for a level playing field in this regard must place the emphasis on common outcomes (recognising that processes may be distinct), and these outcomes should be sought through employing appropriate technical solutions and in alignment with other ongoing, inter-connected legislative initiatives on crypto assets and CASPs such as the Markets in Crypto Assets Regulation (MiCA). Dialogue should continue between the private sector and policymakers in order to determine how the newly introduced regulatory obligations could be fulfilled in a DLT environment in a manner that recognises that payment transparency and personal privacy can co-exist.

- The EBF advises that the Recast contains no regulatory expectations for service providers interacting with un-hosted wallets. In accordance with the new Article 58(1) of the proposed AML Regulation, credit institutions, financial institutions and crypto-asset service providers shall be prohibited from keeping anonymous crypto-asset wallets, but the interaction with such wallets is not addressed. In open decentralised systems, the originator's VASP is not aware whether the beneficiary's address indicated by the client corresponds to a wallet managed by another VASP or is an un-hosted wallet. In addition, the originator's VASP itself may not have sufficient information to check that the beneficiary's name – provided by its customer – is effectively the owner of the wallet that will receive the funds. In addition to creating regulatory uncertainty, this might also result in certain investors moving funds into un-hosted wallets, ultimately impeding the achievement of AML/CFT objectives. We hence propose that CASPs who make or receive a transfer from an un-hosted wallet be required to ensure that the names and addresses of the parties to the transaction are identified and stored. These CASPs should also take risk-based measures to ensure the verifiability of this information.
- The EBF stresses the importance to ensure consistent implementation of the rules set out in the Recast across jurisdictions and entities, taking into account the evolving nature of technological solutions aimed at fulfilling the travel rule. This could include assigning AML/CFT obligations to other entities in addition to the crypto-asset service providers (CASPs) if they play a critical role in supporting payment transparency behind crypto transactions. This could include, e.g. assigning AML/CFT obligations to decentralised exchanges or platforms, as well as applications that operate on a blockchain platform or similar technology.
- It is essential that legislators consider the techniques highlighted by the FATF to support the industry in complying with the travel rule, such as collaborating with the industry to identify travel rule solutions and clearly communicating regulatory expectations in this area.
- Furthermore, the EBF believes a longer implementation period should be envisaged, aligned with the time period provided for the Funds Transfer Regulation (FTR)'s original entry into force, given the novel ecosystem conditions and technical infrastructure that crypto-asset funds transfers take place within. The implementation period should recognise the inter-connectedness and inter-

dependencies with other related EU legislative initiatives such as MiCA, to ensure the appropriate technical solutions are holistic and compatible with complementary regulatory requirements.

On Obligations on Crypto-Asset Service Providers (Articles 14 – 18)

- The EBF highlights that the provision of Art. 14(4), whereby the information may not necessarily be attached directly to the crypto transfer itself, while presumably aimed at providing operational flexibility, will create distinct challenges on downstream controls, e.g. to sanctions screening and ensuring that crypto transfers are appropriately held until the information is determined to be complete.

On Information, Data Protection and Record-Retention (Articles 19 – 21)

- The EBF cautions that the crypto-asset market has important technological and structural features which differentiate it from the traditional payments infrastructure the current FTR was designed for. The blockchain supporting a particular virtual asset might not be technically adequate for storing information relating to the originator/beneficiary of the transfer pursuant to Art 14(3). The public nature of blockchain combined with the storage of personal information in it may also cause frictions with the GDPR framework. For instance, the information shared on a DLT network as part of a crypto-asset transfer will in some cases be open and accessible to other parties, raising the need for additional considerations in how data protection requirements will be fulfilled.
- Critical to the success of establishing a level playing field on payment transparency is the obligation of the CASP of the originator to provide information on the originator and the beneficiary in accordance with Article 14(1) and (2). However, given the public nature of DLT, a solution must be pursued that demonstrates how payment transparency and personal privacy are not mutually exclusive concepts, and that payment transparency does not equate with a public blockchain where an individual's identity and subsequent transactional activity should be available for anyone to see. The CASP's responsibility to know, retain and compartmentalize data on originator and beneficiary is an important one. CASPs must recognise their role and responsibilities as data controllers under the GDPR and the applicable personal data protection framework.
- Moreover, some crypto assets exist on fully decentralised networks in which they may be governed by decentralised autonomous organisations (DAOs). In these cases, it may be difficult to identify an acting crypto-asset service provider to direct information requests to and to ensure the accuracy of any information provided by those entities or by firms' clients. These actors should be considered as CASPs where they offer crypto asset services in line with FATF's Guidance on a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers[1].

[1] FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html, para. 66.

- In view of the considerations expressed above, the EBF maintains that upholding requirements regarding payment transparency to crypto-asset service providers is pivotal in ensuring the safety of the financial system, despite the existing technical challenges. Therefore, those challenges should not entail that CASPs be exempted from their obligations under the FTR or under the applicable personal data protection framework. Instead, they require an ongoing dialogue between CASPs and legislators in order to ensure the fulfillment of those obligations.

Additional comments

- The EBF highlights the low usage of the Legal Entity Identifier (LEI) code, the lack of a clear roadmap for its wider adoption, as well as the huge impact a potential mandatory requirement for requesting LEI would have on the banking industry. We therefore maintain that the LEI should remain only optional under the FTR until global standards and processes are in place which allow this information to be accurately verified on the beneficiary side.
- According to existing funds transfer regulations, the level of required information on a payment is lower when that payment is wholly domestic. For the various payment providers that promote market remittances/international transfer products for their customers, often the underlying payment from the originator is a domestic payment from the customer's bank to the payment provider's local account in a traditional bank. These "domestic" payments are then bundled with other same-day "international" payment requests from other customers in the same country, and settled via a similar account in the country of the ultimate beneficiaries. The international "leg" of this end-to-end payment is a bundled payment and will appear to the financial institution managing the transfer as a transfer for the benefit of the payment provider, not a transfer by a payment provider on behalf of an underlying customer (or customers). Payment services providers (PSPs) leverage such payment flows not only with physical persons but increasingly with small and medium-sized businesses. Whereas the unbundled payments may not be large, trends in financial crime since the development of the SWIFT message format MT202 COV indicate that very serious predicate offences can be committed with small amounts, with the ability to detect the originator and/or beneficiary behind those transfers as key to disrupting the crime. Just as MT202 COV was developed to enable a distinction between bank-to-bank and on behalf of transfers, the same general principle should apply to these small-value transfers. This scenario should be addressed explicitly in the funds transfer regulations, clearly defining roles and responsibilities while recognising that if such activity is to be permitted, the responsibility for sanctions screening and automated transaction monitoring should remain with the originating payment provider and the payment provider responsible for disaggregation, not the intermediary financial institution providing a service under open banking regulation and fair competition provisions.
- The EBF also takes the opportunity to emphasise the need to revise the FTR in order to clarify the obligations of the payer's PSP and the payee's PSP in relation to direct debits. It appears that the current FTR provisions (particularly the obligations under Articles 4 – 6, vis-à-vis Articles 7 – 9) are compatible with credit transfers processes only. For this reason, the EBF recommends that the Commission clarifies

and distinguishes the obligations for payers' PSPs and for payees' PSP also with regards to direct debits. In particular, the extent and the structure of the information obligations (which are currently only for the payer's PSP) against the checking obligations for the Payee's PSP, should be reviewed. The EBF recommends that the information obligations (Article 4) which are currently foreseen for the payer's PSP are extended and apply equally to the payee's PSP. It would be useful to clearly distinguish, in the text of the FTR, the provisions that apply to push transactions (credit transfers) and those that apply to pull transactions (direct debits), in order to identify without uncertainty the obligations applicable to the payer's and payee's PSPs (and intermediary PSPs when applicable), within the relevant context.

- Furthermore, the EBF invites the Commission to clarify that settled R-Transactions do not constitute a new transfer of funds within the meaning of Article 3 and hence that the requirements of the FTR should not apply to such R-Transactions transfers. Indeed, R-Transactions are to be considered as exceptions pertaining to the original payment transaction for which FTR obligations have been already met. This proposal will avoid unnecessary frictions in the handling of R-Transactions and significant amendments of the rules of the schemes.
- According to existing funds transfer regulations, the level of required information on a payment is lower also when that payment refers specifically to payment for "goods or services", marking a distinction with payments that are "person-to-person" and thus require full information. In practice, this lower standard is generally, but not solely applied to card payments. Advances in cross-border merchant servicing and cross-border use of direct debit/credit transfers create several payments that likely should equally be able to apply the "goods or services" justification. In parallel, some international remittances may appear as credit card purchases when they are in fact person-to-person transfers of value (against which traditional payment transparency standards should generally apply). Given the increasing volume of cross-border payments and payment types, clearer guidance is required on how to assess – via a method that can be operationalised in a high-volume payment environment – whether or not a certain type of activity qualifies under the "goods or services" category and thus can be exempt from traditional transparency standards. Such an exemption would then need to extend to the intermediary financial institution (if applicable) for sanctions screening and transaction monitoring.
- The EBF maintains that the FTR should be amended in order to create a level playing field between all payment instruments used for the purchase of goods and services. Currently only card transactions used for the purchase of goods and services fall out of scope of FTR. This is particularly relevant given the objective of the European Commission and the European Central Bank to encourage the development of instant credit transfers to use cases that include SCTInst-based solutions in the scope of the FTR exemption under Article 2(3), now applicable to "transfers of funds carried out using a payment card, an electronic money instrument or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics" provided that certain conditions are met. Indeed, SCTInst-based solutions can fit in the definition of "other digital […] device with similar characteristics" and can be used "to pay for goods or services" but not exclusively as provided for in Article 2(3)(a). Therefore, this last subparagraph would need to

be amended to make sure that SCTInst-based transactions at Point of Interaction (POI) should possibly benefit of a similar exemption under the FTR.