AFME Response to JMLSG proposed guidance on Part II Sector 22 – cryptoasset exchange providers and custodian wallet providers

18 May 2020

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to comment on the Joint Money Laundering Steering Group (JMLSG) Guidance (referred to hereafter as "the Guidance") on Part II Sector 22 - cryptoasset exchange providers and custodian wallet providers. AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia.

AFME is registered on the EU Transparency Register, registration number 65110063986-76.

Our high-level response to the Guidance is provided below and followed by more detailed feedback.

High-Level Response:

Wherever possible, we encourage JMLSG to use **common terms and definitions** relating to crypto-assets, cryptoasset exchange providers and custodian wallet providers. These should be at a minimum aligned with the approach taken by the UK regulators (in particular, the classification of crypto assets into security tokens, e-money tokens, and unregulated tokens). The terminology should also be aligned regionally e.g. with the European Commission's (EC) approach and/or globally e.g. with the Financial Action Task Force (FATF), Financial Stability Board (FSB), Bank of International Settlements (BIS), and International Organization of Securities Commissions (IOSCO).

We consider that all the services of **crypto-asset exchange providers** should be consistently captured under the same AML/CFT legal framework. This means that competent authorities should treat relevant crypto-asset service providers on an equal footing in order to mitigate the risk of regulatory arbitrage.

We are strongly supportive of using a **risk-based approach** while applying AML/CFT measures to cryptoasset services and custodian wallet providers. This means that firms should proactively assess the current and emerging risks they face and deploy their resources accordingly. Higher and lower risk factors may be set off against each other, leading to a holistic view of money laundering/terrorist financing risk.

We encourage JMLSG to provide guidance on the type of **due diligence measures** that regulated firms should apply when establishing a new business relationship with cryptoasset exchange providers and custodian wallet providers.

JMLSG is asked to provide guidance on the AML/CFT obligations that cryptoasset exchange providers and custodian wallet providers who are dealing with **crypto-assets qualified as specified investments** are required to fulfil.

Association for Financial Markets in Europe
London Office: 39th Floor, 25 Canada Square, London E14 5LQ, United Kingdom T: +44 (0)20 3828 2700
Brussels Office: Rue de la Loi 82, 1040 Brussels, Belgium T: +32 (0)2 788 3971
Frankfurt Office: Bürohaus an der Alten Oper, Neue Mainzer Straße 75, 60311 Frankfurt am Main, Germany
T: +49 (0)69 153 258 967
www.afme.eu

AFME recommends using the same abbreviation for the term *anti money laundering and counter terrorism financing* throughout the Guidance. To this end, we propose using the abbreviation *AML/CFT* that is in line with that used by the EC. This will allow to avoid any confusion while reading various consultations/regulations/guidance issued by different countries on the subject.

Consultation response: (note that we have responded to selected paragraphs only)

Definitions

1.1. A cryptoasset is a cryptographically secured digital representation of value or contractual rights that uses a form of distributed ledger technology and can be transferred, stored or traded electronically, and for the purposes of the definition of a cryptoasset exchange provider includes a right to, or interest in, the cryptoasset (Regulation 14A(3)(a) and (c) ML Regulations).

In Annex A of the recently published Global Financial Markets Association (GFMA) response to the Basel Committee on Banking Supervision (BCBS) Discussion Paper on Designing a Prudential Treatment for Crypto-assets[1], GFMA provides an overview of different crypto-assets and their defining features.

We recommend that the JMLSG considers the types of crypto-assets that are outlined in the GFMA paper in the context of this Guidance.

The use of common terms and definitions relating to crypto-asset activities is critical for easing collaboration across jurisdictions. AFME recommends that the definitions used in this Guidance are aligned at the regional (e.g. EU) and global levels (e.g. FATF, FSB, IOSCO, BIS) wherever possible.

1.3. Some cryptoassets may be specified investments for the purposes of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001.

AFME supports this approach, which is aligned with the UK regulator's approach (please see FCA Policy Statement Guidance on Crypto-assets PS19/22[2]), regional approach (please see ESMA Advice Initial Coin Offerings and Crypto-Assets[3]) and global approach (please see IOSCO Public Report on Global Stablecoin Initiatives[4]).

JMLSG is asked to provide guidance on the AML/CFT obligations that cryptoasset exchange providers and custodian wallet providers who are dealing with crypto-assets qualified as specified investments are required to fulfil.

1.5. An asset cannot be a cryptoasset and electronic money at the same time. Monetary value stored on instruments which is exempted as specified in points (k) and (l) of Article 3 Payment Services Directive 2 is also distinguished from cryptoassets.

We note that the claim that '*an asset cannot be a cryptoasset and electronic money at the same time*' is not harmonised with the FCA's approach.

[1] Discussion Paper on Designing a Prudential Treatment for Crypto-assets, pp 11-12
[2] FCA Policy Statement Guidance on Crypto-assets PS19/22, p4
[3] ESMA Advice Initial Coin Offerings and Crypto-Assets
[4] IOSCO Public Report on Global Stablecoin Initiatives

As stated in PS19/22[5], the FCA classifies cryptoassets as:

- **Security tokens:** Cryptoassets which qualify as specified investments as set out in the Regulated Activities Order (RAO) and are regulated as such (specifically removing e-money from this definition to provide a greater distinction);
- **E-money tokens:** *'This category refers to any token that reaches the definition of e-money. These tokens are subject to the EMRs* [E-Money Regulations] *and firms must ensure they have the correct permissions and follow the relevant rules and regulations. This category formerly sat within the utility tokens category. These tokens fall within regulation*.'
- **Unregulated tokens:** All other cryptoassets (utility tokens or exchange tokens) which do not qualify as either specified investments or e-money and therefore fall outside the regulatory perimeter.

Further to the above, the FCA defines e-money tokens as cryptoassets that meet the definition of electronic money in the Electronic Money Regulations (EMRs)[6]. The criteria include:

- Electronically stored monetary value that represents a claim on the issuer;
- Issued on receipt of funds for the purpose of making payment transactions;
- Accepted by a person other than the issuer; and
- Not excluded by Regulation 3 of the EMRs.

The European Banking Authority (EBA) also considers that crypto-assets (in particular stablecoins) can qualify as e-money[7].

The FCA's final Guidance on crypto-assets also notes that in some limited instances, stablecoins will qualify as e-money and will be regulated as such[8]. Paragraph 74 of the FCA's Guidance[9] notes that '*Some tokens might be stabilised by being pegged to a fiat currency (…) Any token that is pegged to a currency, (…) and is used for the payment of goods or services on a network could potentially meet the definition of e-money'.*

In order to aid JMLSG's thinking around stablecoins in particular, please refer to the GFMA paper on the classification of crypto-assets,[10] where stablecoins are defined as: *'tokens designed to minimize/eliminate price fluctuations relative or in reference to other asset(s) which are not issued by a central bank, FMI* [Financial Market Infrastructure]*, bank, credit institution or highly-regulated depository institution. May represent a claim on the issuing entity, if any, and/or the underlying assets'.*

In respect of qualifying crypto-assets as e-money, we request that the JMLSG's Guidance is aligned at a minimum with the approach of UK regulators, and wherever possible also regionally/globally.

We also request the JMLSG to provide examples where crypto-assets may or may not qualify as e-money, including where stablecoins qualify as e-money.

1.6. Cryptoassets include both those that are centralised, i.e., issued by an administrator, and those that are decentralised.

We support the inclusion of both centralised and decentralised crypto-assets.

[5] FCA Policy Statement Guidance on Crypto-assets PS19/22, p 14
[6] The Definition of E-money
[7] EBA Report on crypto-assets pp 7, 12-15
[8] FCA Policy Statement Guidance on Crypto-assets PS 19/22, pp 45-46. Note from AFME: Not every 'stablecoin' will meet the definition of e-money, or a security token. For instance, it may be a derivative, a unit in a collective investment scheme, a debt security, e-money, or another type of specified investment. Or, it might fall outside the FCA's remit p 18
[9] https://www.fca.org.uk/publication/policy/ps19-22.pdf p 45
[10] https://www.gfma.org/correspondence/gfma-response-to-bcbs-discussion-paper-on-the-prudential-treatment-for-crypto-assets/ p 10

1.7. The definition is intended to be neutral as to the use of cryptoassets. It thus includes, amongst other types of tokens, payment, asset and utility tokens.

We suggest harmonising the typology with the FCA Cryptoasset guidance PS19/22[11] which effectively means using the same terminology such as security tokens, e-money tokens and unregulated tokens (which could include utility and exchange tokens).

1.8. The definition is broad enough to include in-game currencies. A firm will need to consider on a case-by-case basis whether activities related to the cryptoasset fall within the activities listed in paragraph 1.1. When doing so, the firm should take account of whether the cryptoasset can only be used within a specific game environment or whether it can also be exchanged for value that may then be used outside that environment (an exchange could take place either within the game and be followed by a withdrawal or on an exchange forum outside the game). A similar approach should be taken to closed-loop tokens such as loyalty reward points that may meet the definition of a cryptoasset.

We agree that in-game currencies meet the definition of cryptoassets and should be in scope. In particular, this is true if in-game currencies can be exchanged for fiat money or another cryptoasset, and/or if a secondary market exists outside the game.

We encourage JMLSG to consider whether there are any other currencies that should fall within the definition of cryptoassets e.g. currencies that are used for betting. For instance, if such tokens are used for payment/ exchange or provide access to particular goods, services or securities tokens, then they should also fall within the definition.

Additional comment to the section on cryptoassets:

We also recommend clarifying that cryptoassets can also be hybrid. A cryptoasset can, for example, have multiple characteristics at issuance (at the same time), or it can change features throughout its lifecycle.

Cryptoasset exchange provider

1.9. A cryptoasset exchange provider is a firm or sole practitioner who by way of business provides one or more of the following services, including where the firm or sole practitioner does so as creator or issuer of any of the cryptoassets involved, when providing such services— (a) exchanging, or arranging or making arrangements with a view to the exchange of, cryptoassets for money or money for cryptoassets, (b) exchanging, or arranging or making arrangements with a view to the exchange of, one cryptoasset for another, or (c) operating a machine which utilises automated processes to exchange cryptoassets for money or money for cryptoassets (Regulation 14A(1) ML Regulations).

We note that the Financial Action Task Force (FATF) provides the following definition of crypto-asset exchange providers [12].

'(…) any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- *exchange between virtual assets and fiat currencies;*

[11] FCA Cryptoasset guidance PS19/22
[12] FATF Guidance for a risk-based approach - Virtual Assets and Virtual Assets Service Providers p13-14

- *exchange between one or more forms of virtual assets;*
- *transfer of virtual assets;*
- *safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and*
- *participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.'*

In order to create a level-playing field and to effectively mitigate the risk of ML/TF, all the services of crypto-asset exchange providers should be consistently captured under the same AML/CFT legal framework. This means that competent authorities should treat relevant crypto-asset service providers on an equal footing in order to mitigate the risk of regulatory arbitrage.

We recommend that JMLSG aligns the definition of crypto-asset exchange providers with the FATF definition.

1.10. The definition of a cryptoasset exchange provider is technologically neutral.

We welcome that the definition provided is technology neutral. This is important for future-proofing regulation to ensure it can remain applicable as new technologies continue to develop.

1.11. The definition is broad, providing for exchanging as well as "arranging or making arrangements with a view to the exchange." This may include activities relating to a dedicated peer-to-peer platform. However, it is not intended to capture a firm that only provides a forum where buyers and sellers can post their bids and offers, such as a bulletin board where the availability of the assets are merely made known and the parties trade at an outside venue either through individual wallets or other wallets not hosted by the forum or a connected firm.

AFME agrees that bulletin board should not be captured by the regulation provided that parties do not trade/exchange cryptocurrencies on there.

1.12. A developer of a decentralized cryptoasset payment system could fall outside of the scope, and is more likely to do so if they derive no income from consequent transactions.

We understand that a developer of a decentralised cryptoasset payment system would not be in scope unless they provide services of an exchange, custody, making arrangements in line with paragraph 1.9 of this Guidance.

We also agree with the paragraph 1.24 of this Guidance which states that a software developer should be out of scope when solely developing or selling the application or platform.

We do not understand, however, the purpose of the wording '*and is more likely to do so if they derive no income from consequent transactions'* in this section. We propose to delete it.

Instead we propose to use the wording '*a developer of a decentralised cryptoasset payment system would not be in scope unless they provide services of an exchange, custody, making arrangements in line with paragraph 1.9 of this Guidance'.*

1.13. In determining the perimeter of regulation, the FCA will have regard to the policy objectives of the legislation as well as the definition itself. The following activities may, for example require assessment on a case-by-case basis:

- **However, issuers, creators or miners of cryptoassets may fall within the scope of regulation if they accept money or cryptoassets by way of business in exchange for the cryptoassets they issue, create or mine, including through cloud mining and initial coin offerings;**
- **Services that facilitate the issuance and trading of cryptoassets on behalf of a natural or legal person's customers are intended to be captured, although this excludes the mere provision of advice or technology services;**
- **Intermediaries acting as outsourced service providers are not likely to be in scope, as the obligation to comply remains with the outsourcing firm. Intermediaries acting in their own right would, however, need to seek registration**
- **See CP for additional bullets.**

We support the exclusion of 'mere provision of advice or technology services' when determining the perimeter of regulation.

Custodian wallet provider

1.16. 'To hold, store and transfer' in Regulation 14A(2)(b) is to be read cumulatively. This means that firms who merely hold and store cryptographic keys, but are not involved in their transfer (the owner of the cryptoassets interacting with the payment system directly), are not likely to be in scope of the definition. This includes hardware wallet manufacturers (together, these are 'non-custodian wallet providers').

AFME welcomes the differentiation between a custodian wallet provider and a non-custodian wallet provider. Third party custody services could involve safekeeping services related to the private key, or more comprehensive custody services relating to safekeeping, settlement and servicing of the asset. Self-custody is possible via a non-custodian wallet provider (please note that AFME is not advocating for self-custody of financial instruments and/or relevant monetary instruments, rather we are acknowledging that due to technological innovations consumers may have the ability to self-custody certain crypto assets in their current form).

We agree that firms who hold and store cryptographic keys would not be in scope of the definition of a custodian wallet provider, however we believe that all firms handling private keys in relation to client assets should fall under the ML Regulations.

The scope of regulation

1.20. Cryptoasset exchange providers and custodian wallet providers based in the UK are obliged entities for the purposes of the ML Regulations. They are required to register with the FCA as the relevant competent authority.

AFME supports the inclusion of cryptoasset exchange providers and custodian wallet providers as obliged entities for the purposes of the ML Regulations.

1.24. Software developers who merely sell an application or platform without engaging as a business in relevant activities are not included in scope.

AFME agrees that a software developer should be out of scope when solely developing or selling the application or platform. However, in our view they may be considered in scope if they also use the new application or platform to engage as a business in exchanging or transferring cryptoassets.

1.25. Providers of ancillary products or services to cryptoasset networks who do not engage as a business in relevant activities are not included in scope.

AFME finds that any crypto-asset services whereby the provider has access to the private key should be considered in scope, as well as other related ancillary activities such as acquiring services, onboarding and payments. We also find that in-wallet credit provision services and wallet/portfolio accounting valuation should be included in the ML Regulations.

1.26. The Wire Transfer Regulation does not currently apply to transfers in cryptoassets.

We recommend adding '*in the UK*' in the above provision, so the scope is clear. The provision should read as follows:

'The Wire Transfer Regulation does not currently apply to transfers in cryptoassets in the UK'.

1.27. Cryptoassets are property under English law, bringing them within the scope of Part 7 of the Proceeds of Crime Act 2002.

We recommend adding that cryptoassets are also brought within the scope of Part 3 of the Terrorism Act 2000[13].

What are the money laundering and terrorist financing risks in this sector?

1.30. The risk-based approach applies to the sector, which means firms should proactively assess the current and emerging risks they face and deploy their resources accordingly. Higher and lower risk factors may be set off against each other, leading to a holistic view of money laundering/terrorist financing risk.

We are strongly supportive of using the risk-based approach in order to make a good use of the existing resources.

1.32. The following are factors that give rise to money laundering and terrorist financing risks (some specific to cryptoassets, others common to a number of assets) together with indicative mitigation strategies:

Overall, we note that the factors noted in this section cover the risks that give rise to ML/TF and are in line with the FATF guidance for a risk-based approach to virtual assets and virtual assets service providers[14].

We would also like to make two additional comments on the following risk factors.

[13] Part 3 of the Terrorism Act 2000
[14] FATF Guidance for a risk-based approach to virtual assets and virtual assets service providers

• Decentralised nature:

Many decentralised exchanges require less personal information from their members and crypto-to-crypto providers are not currently mandated to conduct Know Your Customer (KYC) checks in all jurisdictions. Therefore, we note that identification and assessment of potential ML/TF risks may be impossible without all the necessary information.

• Segmentation:

We encourage JMLSG to consider a scenario in which cryptoasset service providers use a wide network of agents in the transfer/payment chain. The question would be whether cryptoasset services providers should be responsible for ensuring that their agents comply with the AML/CFT standards.

1.33. The following are specific higher-risk factors that firms should have regard to in addition to the generic higher-risk factors set out in Part I, Chapter 5.5:

Under this section, we would like to make a specific comment with regard to mining operations.

• The customer:

- **Is involved in cryptoasset mining operations (either directly or indirectly through relationships with third parties), the organisation of which gives rise to higher risk.**

JMLSG is asked to provide more guidance on when mining operations can be considered as higher risk and what specifically makes them higher risk.

In order to avoid confusion, we suggest narrowing the scope of the statement by adding the following wording:

'Is involved in cryptoasset mining operations that take place in high risk jurisdictions or relate to high risk crypto assets, for instance, privacy coins.

1.34. The following are specific lower-risk factors:

In this section, we believe that one additional lower-risk factor should be added, namely:

'Onboarding clients using non-face-to-face channels such as reliable and independent digital ID systems with appropriate risk mitigation measures'.

This recommendation is in line with the FATF guidance on digital identity stating that '*using reliable, independent digital ID systems with appropriate risk mitigation measures in place, may present a standard level of risk, and may even be lower-risk.'*[15]

[15] FATF Guidance on digital identity, p5.

Customer due diligence ('CDD')

Who is the customer?

1.44 It may be noted that where a cryptoasset exchange provider is a client of another credit or financial institution, the cryptoasset exchange provider is that institution's customer, unless there is evidence to the contrary.

The application of CDD measures (see Part I, Chapter 5)

We encourage JMLSG to provide guidance on the type of due diligence measures that regulated firms should apply when establishing a new business relationship with cryptoasset exchange providers and custodian wallet providers.

1.46 CDD measures must also be applied to occasional transactions (single or linked) of EUR 15,000 or more. However, this threshold does not apply to cryptoasset exchange providers in as far as they are operating an ATM, in which case CDD measures must be applied to all transactions.

We recommend that the threshold is lowered to USD/EUR 1, 000 if the transaction results in a cryptoasset transfer or exchange. Such threshold would align with the FATF recommendation 15[16].

1.57. Information about the destination of funds is not currently required by law, but it is good practice to collect this in order to inform the assessment of risk (e.g., geographical risk) and aid transaction monitoring processes. Where a recipient's name has been collected, sanctions obligations apply in the usual way (see paras 1.73-1.74 below).

Ongoing monitoring

AFME recommends adding a requirement to keep documents, data, or information collected under the CDD process up-to-date and relevant by undertaking reviews of existing records in line with MLR 28(11)(b)[17]. This requirement should be added especially in relation to higher-risk customers or categories of cryptoasset products or services.

Simplified due diligence ('SDD')

1.60. If cryptoasset exchange providers and custodian wallet providers determine that the business relationship or transaction presents a low degree of risk of money laundering and terrorist financing, the firm may apply SDD measures (see Part I, paragraphs 5.4.1ff).

Enhanced due diligence ('EDD')

In line with FATF Guidance for a risk based approach for virtual assets and virtual asset service providers section 105 indicates that some '*business relationships or covered VA activities in the VASP sector may have characteristics similar to cross-border correspondent banking relationships.*'[18]

[16] FATF Recommendation 15, p 71
[17] MLR 28(11)(b)
[18] FATF Guidance for a risk-based approach to virtual assets and virtual assets service providers

If covered virtual asset activities in the virtual asset service providers sector have characteristics similar to cross-border correspondent banking relationships, then financial institutions must perform some additional measures in addition to performing normal CDD measures in line with FATF Recommendation 13[19].

These additional measures include:

'a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;
(b) assess the respondent institution's AML/CFT controls;
(c) obtain approval from senior management before establishing new correspondent relationships;
(d) clearly understand the respective responsibilities of each institution; and
(e) with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.'

We encourage JMLSG to consider adding these additional measures in the context of VA activities in the VASP sector having characteristics similar to cross-border correspondent banking relationships.

AFME Contacts

Aleksandra (Ola) Wojcik
Aleksandra.Wojcik@afme.eu
+44 (0)20 3828 2734

Madeline Taylor
Madeline.Taylor@afme.eu
+44 (0)20 3828 2688

Richard Middleton
Richard.Middleton@afme.eu
+44 (0)20 3828 2709

[19] FATF Recommendation 13