

August 25, 2023

Joint Money Laundering Steering Group (JMLSG)
1 Angel Court
London
EC2R 7HJ

Delivered via: Carol Smit at caroljsmit@jmlsg.org.uk

Re: Consultation on the proposed addition of Annex I to Sector 22 takes account of amendments relating to cryptoasset transfers, as introduced by The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022

Notabene Inc. welcomes the opportunity to comment on the call for consultation for the “proposed addition of Annex I to Sector 22 takes account of amendments relating to cryptoasset transfers, as introduced by The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022¹”. We wanted to applaud the collaborative efforts by Joint Money Laundering Steering Group (JMLSG), the Financial Conduct Authority (FCA), and HM Treasury (HMT) in engaging with the industry to offer additional guidance to firms required to comply with the Travel Rule in UK. Notabene has a representation of 129 UK Crypto Business (CB) entities in our VASP Network².

A team member of Notabene co-chaired the CryptoUK’s Travel Rule Working Group response to the proposal, yet our company response provides additional insight and view point that we have as a solution provider and thought leader in the travel rule space. Given the breadth of the topics covered in the call for consultation, Notabene will focus primarily on lack of interoperability and closed-networks, counterparty VASP due diligence, and beneficiary VASP obligations and returning funds.

Introduction and Overview:

Notabene, the crypto industry's only pre-transaction decision making platform, helps to identify and stop high-risk activity before it occurs. The Notabene pre-transaction decision making platform offers a secure, holistic view of crypto transactions, enabling customers to automate real-time decision-making, perform counterparty sanctions screening, identify self-hosted wallets, and complete the smooth roll out of Travel Rule compliance, in line with global regulations.

Notabene was founded in 2020 with the explicit mission to enable safe and trusted crypto transactions by developing a comprehensive solution to help companies comply with the FATF’s Travel Rule. A continued strong relationship with global

¹ https://www.jmlsg.org.uk/wp-content/uploads/2023/07/JMLSG-Guidance_Sector-22-Annex-I_Board-approved-1.pdf

² <https://app.notabene.id/network>

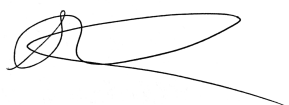
financial regulators including FATF, industry associations, and Virtual Asset Service Providers (VASPs) across multiple jurisdictions arms us with an unparalleled view of the complex and critical nature of regulatory compliance in the crypto space.

Today, many exchanges have AML/CTF processes that allows them to perform customer identification and sanctions screening of their customers as part of onboarding and ongoing customer due diligence. This helps them block sanctioned individuals from directly using their products to initiate transactions. Even with current AML and know your customer (KYC) compliance frameworks in place, VASPs can unknowingly facilitate transactions with sanctioned counterparties.

Only Travel Rule compliance gives CB's transaction-level counterparty and sanction insight, allowing them to recognize if their clients are sending transactions to sanctioned entities, wallets, or jurisdictions. CBs worldwide are in different stages of compliance, which leaves many companies vulnerable to exposure to sanctioned individuals.

We appreciate the opportunity to respond to this consultation and look forward to continued engagement and clarification.

Very truly yours,



Lana Schwartzman
Head of Regulatory and Compliance

RESPONSE TO CONSULTATION

Lack of interoperability and closed-networks	3
Counterparty VASP due diligence	4
Beneficiary VASP obligations and returning funds	5

Lack of interoperability and closed-networks

The issue of lack of interoperability and closed-networks is currently not addressed in the JMLSG Guidance or FCA communications.

Further to the comment submitted by CryptoUK, we would like to elaborate on the the issue of lack of interoperability in the context of closed-network protocols. Some of the existing technology providers are structured as closed Travel Rule protocols. In this model, there is a centralized process to decide which VASPs are able to send and receive Travel Rule data transfers through the protocol.

VASPs need to overcome two hurdles to be able to reach counterparties that exclusively use closed-network protocols for Travel Rule compliance:

1. Join those networks as a member; and
2. Integrate one or more protocols directly or integrate with an interoperable protocol / solution.

A comprehensive solution to the first hurdle is difficult to envision because membership of closed network protocols is not available to all VASPs.

On the second hurdle, once a VASP becomes a member of the closed network, they are free to technically integrate. However, managing several integrations to be able to exchange Travel Rule information with different silos of VASPs is cumbersome and prevents an effective implementation of Travel Rule compliance.

We believe that it would be beneficial to provide guidance that encourages the adoption of open travel rule protocols and sets more flexible expectations for how CBs should comply when transacting with counterparties that use non-interoperable solutions.

Counterparty VASP due diligence

As mentioned in the response submitted by CryptoUK, the UK Travel Rule legal framework does not address (and therefore JMLSG does not address) any obligation or parameters around the topic of counterparty VASP due diligence³.

Counterparty VASP due diligence is an essential part of Travel Rule compliance to avoid transacting with sanctioned or high-risk counterparties, ensuring the protection of exchanged Travel Rule information and maintaining reliable and effective Travel Rule information flows.

Hence, it would be beneficial to set expectations as to what counterparty due diligence measures are required for the purposes of transacting and engaging in Travel Rule flows. It is also relevant to specify cases where simplified due diligence measures are permissible (e.g. relying on the uniform requirements and supervision applied in the jurisdiction or region). Most relevantly, it is paramount to consider what is the nature of VASPs relationships' for transacting with one another and sharing Travel Rule information which may be distinct from cross-border correspondent relationships. Hence, the required due diligence obligations may also need to be different and more limited in scope, in line with the FATF recommendations:

*"For clarity, counterparty due diligence for the purpose of complying with Recommendation 16 is distinct from the obligations applicable to cross-border correspondent relationships. Unlike the banking sector, it is possible for transfers of VA for or on behalf of another person to occur between VASPs, even in the absence of a correspondent relationship or any other relationships. In such circumstances, the VASPs involved in the transfer may undertake counterparty due diligence to ensure they are able to comply with the travel rule and apply measures to mitigate the ML/TF risk. The existence of a correspondent relationship between two VASPs involved in a VA transfer may, however, partly or wholly fulfil the requirements for counterparty due diligence"*⁴

In this context, it is also worth mentioning that Notabene supports the approach taken by the FATF as a reasonable means to handle the conflict between AML/CTF goals and data protection. In scenarios where the risk of money laundering and terrorism financing is low, but data privacy risks are high, it is reasonable to allow VASPs to transact without sharing Travel Rule information:

³ See page 62 et. seq. of the FATF (2021), [Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers](#).

⁴ See paragraph 169 of the [Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers](#).

"VASPs should have recourse to altered procedures, including the possibility of not sending user information, when they reasonably believe a counterparty VASP will not handle it securely while continuing to execute the transfer if they believe the AML/CFT risks are acceptable. In these circumstances, VASPs should identify an alternative procedure, whose control design could be duly reviewed by their supervisors when requested."⁵

For this exception to be effective and to avoid an unintentional loophole in Travel Rule compliance, we identify three measures that would be recommendable:

1. The criteria that VASPs should use to determine that their counterparty does not have adequate safeguards for ensuring data protection needs to be specified and VASPs should be required to document their reasoning;
2. In line with recommendations in paragraph 291 of the FATF Guidance, VASPs should be required to apply alternative procedures - duly reviewed and controlled by the supervisory authorities - to achieve the goals of the Travel Rule to the extent possible;
3. Requiring the Originator VASP to collect and share beneficiary information could be enforced as a minimum requirement, considering that the Beneficiary VASP already should know this information and it would be required to match a beneficiary with the underlying account.

Beneficiary VASP obligations and returning funds

25. CBs must consider whether to delay making a cryptoasset available to the beneficiary, until the information is received, or any discrepancy resolved, or if not received or resolved within a reasonable time, to return the cryptoasset to the CB of the originator (see paras 32-33).

*32. The CB (intermediary **or** of the beneficiary) should consider the risks and complexities of returning a transfer, prior to making a return, as it may create operational challenges for CBs to reattribute it to the originator. They should make reasonable efforts to ensure that the transfer is able to be returned to the originator.*

We refer to Paragraphs 25 and 32 of the JMLSG Guidance, which in turn refer to 64D/(2)/(c) of the MLRs. These legal obligations imposed on CBs face several technical and operational limitations today.

⁵ See paragraph 291 of the [Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers](#).

If the Beneficiary CB receives a deposit without receiving the required Travel Rule data transfer, this may constitute one of the scenarios below:

1. The deposit is an unhosted wallet transfer: in this case, the requirements of 64G of the MLRs apply;
2. The transaction was received from a CB based in a jurisdiction where Travel Rule requirements **are not** in effect: in this case, according to the recent FCA statement, the CB should make “*a risk-based assessment of whether to make the cryptoassets available to the beneficiary*”. Depending on the risk-based assessment, the CB may need to return the funds;
3. The transaction was received from a CB based in a jurisdiction where Travel Rule requirements **are** in effect: in this case, the CB needs to necessarily return the funds.

Firstly, determining whether the deposit fits within scenario 1, 2 or 3 and, hence, adequately complying with the applicable legal obligations, is a challenge in itself.

- Paragraph 39 of the JMLSG guidance allows CBs to take a risk based approach in attributing wallets and requires CBs to take all “*reasonable*” steps to “*identify the counterparty and whether a wallet is hosted or unhosted*”. It would be beneficial to provide guidance that clarifies how Beneficiary CBs should proceed when, having taken the appropriate steps, CBs are still unable to attribute the wallet. In such cases, CBs are unable to determine whether the transaction fits within scenario 1, 2 or 3 and, consequently, the legal obligations that apply are unclear.
- For instance, in some cases the CB may be able to attribute the wallet to a VASP but not be able to determine the specific jurisdiction / legal entity of the counterparty (e.g., blockchain analytics attribute wallets to a VASP cluster rather than specific entities; end-customers are often also not aware of the specific legal entity that is used to process their/their counterparties’ transactions).
- Hence, our proposal is that:
 1. There is guidance that allows CBs to take a risk-based approach to deciding, considering the specific characteristics of the transaction, whether or not to allow the funds to be released to the beneficiary customer; or/and
 2. Paragraph 41 of the JMLSG Guidance is amended to include the sentence in bold: “Where a UK CB does not know if the counterparty (including any intermediaries) is a UK CB, it may treat the transaction as

a cross border transaction. **Where a UK CB does not know the counterparty's jurisdiction, it may treat the transaction as if the counterparty jurisdiction does not have Travel Rule requirements in place."**

Secondly, in cases where the CB is required to return the funds, paragraph 32 already acknowledges the complexities that this presents. However, it is not clear what is expected of CBs in cases where CBs take reasonable efforts to return the funds to the originator but conclude that they are unable to safely return the funds. It would be beneficial to provide guidance in this respect.