Travel Rule Good Practices Guide

Authored by the CryptoUK Travel Rule Working Group

CryptoUK

Table of Contents

CryptoUK

Introduction

Objectives of the Travel Rule Good Practices Guide

The Travel Rule Good Practices Guide, developed by CryptoUK's Travel Rule Working Group, aims to empower Virtual Asset Service Providers (VASPs), cryptoasset businesses and digital asset industry participants with an understanding of the Travel Rule and how it applies in the UK. It offers an overview of how compliance is currently being approached by members of the Working Group and provides guidance on addressing the associated challenges.

CryptoUK's Travel Rule Working Group has produced this guide with multiple objectives in mind:

- To provide VASPs and industry participants with clear and comprehensive guidance on understanding the Travel Rule, its requirements and implications.
- To assist VASPs in effective compliance by offering practical advice and good practices.
- To highlight key challenges such as operational complexities and interoperability.
- To serve as an educational resource, the guide informs stakeholders about regulatory requirements and industry trends related to the Travel Rule.
- To foster collaboration and standardisation across the industry, promoting consistency in compliance approaches and facilitating smoother interactions between VASPs and regulators.

This document makes references to VASPs, as defined by the FATF in its guidance, and cryptoasset businesses (CBs), as defined in the UK's money laundering/Travel Rule regulation. This document will primarily use the term CB as it refers to definitions used in UK legislation and guidance.

VASP definition by FATF: "Virtual asset service provider means 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;
- 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."

"Cryptoasset business[1]" as defined by the UK legislation: means a cryptoasset exchange provider or a custodian wallet provider.

Disclaimer:

The information provided in the Travel Rule Good Practices Guide is intended for informational purposes only and should not be construed as legal advice. While every effort has been made to ensure the accuracy and reliability of the content, it is not a substitute for professional legal advice. Readers are encouraged to consult with qualified legal and compliance professionals regarding their specific circumstances and compliance with applicable regulations. The authors and contributors of this guide disclaim any liability for actions taken or not taken based on the information provided herein.

1 64B The Money Laundering and Terrorist Financing (Amendment) (No 2) Regulations 2022.

A Summary of The Travel Rule Working Group's Advocacy Initiatives

CryptoUK's Travel Rule Working Group was formed in 2023 to provide a forum for the trade association's members to share knowledge and best practices as companies prepared for the enforcement of the Money Laundering and Terrorist Financing (Amendment) (No.2) Regulations (MLTFR 2022), which introduced Travel Rule obligations to UK VASPs, on September 1st 2023.

The CryptoUK Working Group collaborated with all the key stakeholders, including the Electronic Money Association (EMA), the Joint Money Laundering Steering Group (JMLSG), the Financial Conduct Authority (FCA) and HM Treasury (HMT) to provide industry perspective on the draft guidance.

On August 31, 2023, the JMLSG published the final revisions to Sector 22 (cryptoasset providers and custodian wallet providers) in Part II of its guidance. This includes a new Annex I to Sector 22 relating to cryptoasset transfers, which relates to the provisions of MLRs that implement the Travel Rule for cryptoasset transfers in the UK. The JMLSG guidance provides a base from which UK VASPs can develop tailored policies and procedures for compliance with the Travel Rule.

Following its publication CryptoUK's Travel Rule Working Group elected to develop the Travel Rule Good Practices Guide to offer further information and suggested compliance approaches to the industry.

The Working Group continues to provide industry-led perspectives on the Travel Rule and compliance approaches and challenges to the regulator, policymakers and key stakeholders on a regular basis.

Should you wish to be involved in this ongoing advocacy initiative please contact the CryptoUK team.

The UK Travel Rule Regulatory Framework

In 2012, the Financial Action Task Force[2] (FATF), adopted Recommendation 16 with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds, and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator and beneficiary of wire transfers is immediately available.

In 2019, the FATF extended Recommendation 16 to virtual asset transfers which was set out in its Guidance for a Risk-Based Approach to Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs). The Travel Rule is *"the obligation to obtain, hold, and submit required originator and beneficiary information associated with VA transfers in order to identify and report suspicious transactions, take freezing actions, and prohibit transactions with designated persons and entities"*[3] (source: FATF 2021b, p. 82, para. 281). The Travel Rule's primary objective is to prevent transactions involving sanctioned entities and potential illicit activities.

On 1 September, 2023 the UK legislation to implement the Travel Rule came into force: Part 7A, Chapter 1, Regulation 64C ("Information accompanying an inter-cryptoasset business transfer") of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI 2017/692) and the Money Laundering and Terrorist Financing (Amendment)(No. 2) Regulations 2022 (the MLRs).

As a result, the UK Travel Rule applies to crypto firms that are registered with the FCA and are conducting inter-cryptoasset business[4] (i.e. UK crypto firm to another crypto firm) and unhosted wallet transfers. The obligations will mean that UK cryptoasset business (the "originator") transferring cryptoassets to another cryptoasset business (the "beneficiary") is required to collect, verify, and share information about the originator and the beneficiary to the transfer.

Under Regulation 64C, the characteristics of a particular inter-crypto asset business transfer will dictate the level of information that a cryptoasset business involved in the transaction is required to collect, verify, transmit and store on the originator and beneficiary. Specific obligations apply to unhosted wallet transfers, as further detailed in the unhosted wallets section of this guide.

2 The FATF is an international organisation founded on the initiative of the G7 that leads global action through the development of policies and the promotion of global standards to combat money laundering, as well as proliferation and terrorist financing, while assessing the effectiveness of actions taken by the countries (and more than 200 governments) that have committed to implement the FATF's global standards.

3 FATF 2021b, p. 82, para. 281.

4 "inter-cryptoasset business transfer": section 64B of the MLRs, means a transaction carried out by two or more cryptoasset businesses which involves the making available of a cryptoasset of an originator to a beneficiary, provided that at least one of the cryptoasset businesses involved in the transaction is carrying on business in the United Kingdom in respect of the transaction (whether that is a cryptoasset business acting for the originator or a cryptoasset business acting for the beneficiary or an intermediary cryptoasset business).

Current Guidance (as at February 2024)

The FCA

In August 2023, the FCA released a statement to outline its expectations for cryptoasset businesses in adopting measures to comply with the Travel Rule. It set out it's expectations that all UK crypto firms need to comply with the requirements and, more specifically, set out its expectation on where transfers are made to and from jurisdictions that have not yet implemented the Travel Rule.

The FCA stipulates that cryptoasset firms must take all reasonable steps and exercise due diligence to comply with the Travel Rule and will remain ultimately responsible to maintain compliance when they are outsourcing the information gathering, verification, and storage requirements of the Travel Rule to third-party service providers.

While FATF has called on jurisdictions to swiftly implement the Travel Rule, there remains delays in implementation and varying timelines for enforcement of the Travel Rule across jurisdictions. This has given rise to the "sunrise issue," which refers to the staggered global implementation of the Travel Rule, complicating harmonised practices and uniform enforcement. Additionally, as there are few uniform standards among the existing compliant jurisdictions, the scope of the Travel Rule, even among the compliant jurisdictions, will vary.

The JMLSG

On August 31, 2023, the Joint Money Laundering Steering Group (JMLSG) published the final revisions to Sector 22 (cryptoasset providers and custodian wallet providers) in Part II of its Guidance.

This includes a new Annex I to Sector 22 relating to cryptoasset transfers, which relates to the provisions of MLRs that implement the Travel Rule for cryptoasset transfers in the UK. The JMLSG Guidance provides a base from which UK VASPs can develop tailored policies and procedures for compliance with the Travel Rule.

Key Stakeholders

There are three key UK stakeholders:

His Majesty's Treasury (HMT)

Which serves as the relevant government department to bring forward and legislate on financial crime matters. The relevant Ministers are typically the City Minister and the Chancellor. Although noting that there are different departments within HMT dealing with cryptoassets, for aspects broader than financial crime.

The Financial Conduct Authority (FCA)

Is the UK's financial crime regulatory authority for the purposes of cryptoassets. It will set out any relevant regulatory expectations through regulatory obligations and guidance. Due to the nature of the UK's registration regime, this will typically be provided on its website, as opposed to the FCA Handbook. It operates independently of the UK Government but works in tandem with HMT to ensure effective implementation of policy and legislation.

The Joint Money Laundering Steering Group (JMLSG)

A group of industry bodies that, among other things, aims to produce guidance on compliance with the MLRs, working alongside the industry. This guidance will be approved by the Chancellor and has the same status in law as FCA guidance by the courts and is taken into consideration by the FCA in any supervisory action.

An additional key stakeholder, although at international standard-setter level, is the Financial Action Task Force (FATF).

The Financial Action Task Force (FATF)

The FATF is the leading international organisation committed to combating illegal financial activities like money laundering and terrorist financing. The core of FATF's work is its set of recommendations, which, while not legally binding, serve as an influential framework that encourages countries to take action toward compliance within their respective jurisdictions. These recommendations serve as guidelines that FATF and members of FATF-style regional bodies (FSRBs) can incorporate into their local regulations. In October 2018, expanding from its historical focus on fiat, the FATF adopted two new Glossary definitions — "virtual asset" and "virtual asset service provider" — and updated Recommendation 15.

Counterparty VASP Due Diligence

Introduction

Counterparty VASP Due Diligence (CVDD) is not a requirement in the UK Travel Rule, nor is it covered by JMLSG or FCA guidance. Nevertheless, firms have general risk-based financial crime obligations and in addition, may wish to consider CVDD, for example, where they choose to adopt a broader risk-based approach or where it is a global business complying with higher standards in other jurisdictions. This section sets out some non-exhaustive guiding principles that firms may wish to consider if intending to take such a course of action.

Our starting point for basing these principles is FATF's Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (the FATF Guidance). The FATF guidance does provide some detail in this area, but as this is a supranational body, there is some lack of clarity in how this might be interpreted. Therefore firms should consider their own interpretation of it, and align it with, amongst other things, their operational and regulatory obligations and expectations and risk appetite. For example, a firm with a global footprint may wish to adopt a higher standard to reduce operational costs, whereas a firm with a UK-only footprint may choose to consider to what extent it intends to carry on CVDD in relation to the UK Travel Rule, reflecting on any potential competitive distortions with its peers but also regulatory obligations and expectations.

- The FATF Guidance states that the purpose of CVDD is "to avoid dealing with illicit actors or sanctioned actors unknowingly". It states that "VASPs do not need to undertake the counterparty VASP due diligence process for every individual virtual asset transfer when dealing with VASPs for which they have previously conducted counterparty due diligence, unless there is a suspicious transaction history or other information (such as adverse media, published information about regulatory or criminal penalties)". It also states that it would "expect a VASP to refresh their counterparty due diligence information periodically or when risk emerges from the relationship in line with their defined RBA control structure."[5]
- Furthermore, FATF states in relation to CVDD "to clarify the scope of this Guidance, competent authorities should require VASPs to implement preventive measures … to assess the counterparty VASP, where VASPs first have a business relationship, and then review the results of the due diligence periodically."[6]
- Separately, but in addition, FATF goes on to add that "VASPs should use this due diligence process to determine whether a counterpart can reasonably be expected to protect the confidentiality of information shared with it". This is a more challenging assessment to be made and again firms will need to consider how they intend to approach this.

The extent of the due diligence, however, is a point where divergent approaches appear as these requirements are implemented at the national level, with FATF explicitly stating that CVDD "is distinct from the obligations applicable to cross-border correspondent relationships"[7] , while jurisdictions like the EU cite the "ongoing and repetitive"[8] nature of the relationship to determine that they constitute a type of correspondent relationship.

For example, some jurisdictions may have no strict CVDD obligations, as it relates to the Travel Rule, while others may suggest a detailed due diligence more akin to that applicable to correspondent banking-type obligations, whilst others may take a more in-between approach where counterparty risk is assessed, but not to the extent of correspondent banking relationships (unless of course such a relationship exists).

Other factors might come into assessing what approach to take when considering a framework for identifying and assessing counterparty risk. These may include identifying a VASP's main counterparties by volume of transactions, or those in jurisdictions that are seen as posing a higher geographical risk. Such an approach, properly documented, could allow for a tiered approach where CVDD is focussed on higher-risk or significant relationships, with transactional analytics being judged sufficient for more occasional / lower risk relationships.

In all cases, keeping the risks to be mitigated in mind ensures a more targeted and effective due diligence process and, importantly, it needs to be in line with the VASP's own risk appetite and the regulatory obligations in the jurisdictions that it is carrying on business.

5 FATF, UPDATED GUIDANCE: A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS, October 2021, paragraph 196.

6 FATF, October 2021, paragraph 198.

7 FATF, October 2021, paragraph 169.

8 REGULATION (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets, Recital 44.

Principles

Despite the absence of a standardised framework for conducting CVDD and the ensuing level of complexity this introduces, it is possible to identify some overarching principles that can guide VASPs in navigating the structure of CVDD. This section sets out an approach that a firm may wish to consider, as a whole or in part, when undertaking to develop a CVDD framework.

A crucial aspect of the CVDD process is the adoption of a risk-based approach. In line with the risks to mitigate mentioned above, this means that VASPs should take appropriate measures to conduct CVDD based on the financial crime risks potentially associated with the counterparty VASP, by understanding the counterparty's business, reputation and quality of its supervision. Likewise, they should consider the risk of a counterparty losing or misusing the Personally Identifiable Information (PII) that will be shared as part of the transfers.

To do this, VASPs have the possibility of leveraging several third-party tools and solutions to assist them in conducting CVDD, and several questionnaires exist either on a standalone basis or integrated to those solutions. However, it is important to remember that VASPs remain accountable and still responsible for ensuring the integrity and reliability of the due diligence process. Even when utilising third-party tools or solutions, VASPs should verify the information provided using a risk-based approach. Specifically, FATF clarifies that "VASPs are required to independently assess counterparty risk" and that this approach, taken primarily by closed Travel Rule networks, "does not remove the need for VASPs to independently verify the information and ensure all relevant domestic obligations are met."[9]

It is not the purpose of this guide to steer users to one or another tool or questionnaire[10], nor to set the standard of CVDD, but considering the purposes of CVDD in terms of risks to be mitigated, below is a baseline of information that a VASP may want to consider obtaining, subject to their own risk and internal policies:

- **Legal entity identification:**
    - With VASPs having operating entities in multiple jurisdictions, identifying the exact entity of the counterparty VASP can be challenging. Clarity on which legal entity is the counterparty VASP is essential for the CVDD. In the event of an intermediary VASP being identified as the most recent VASP in a transfer chain, identification of both the intermediary VASP(s) and the originating VASP may be required.
- **Regulatory status:**
    - Once the legal entity is identified, obtaining information regarding the regulatory status of the counterparty VASP becomes easier. VASPs should take into consideration the counterparty's licence/registration status, competent authority, approved activities, applicable regulations and limitations imposed by the licence/registration, as well as any regulatory action/penalty imposed by supervisory or law enforcement authorities.
- **Travel Rule status:**
    - VASPs need to assess how the counterparty VASP complies with the Travel Rule requirements. This includes considerations such as the requirements that the counterparty VASP is subject to, its Travel Rule Policies, and its treatment of unhosted wallets.
- **Personal data protection:**
    - VASPs must ensure that the Personally Identifiable Information (PII) sent to the counterparty VASP is stored securely. VASPs may want to consider how the counterparty VASP stores that information, whether it complies with GDPR or equivalent requirements, and its CVDD practices as it might send the client PII to another VASP.

9 FATF, Targeted Update on the Implementation of the FATF Standards on Virtual Assets and Virtual Assets service Providers, June 2023: paragraph 30.

10 See for example GBBC's 2023 GDF VADDQ v1.2 and TRISA TRIXO verification questionnaire. Non-exhaustive and for illustrative purposes only.

Following an initial assessment, if the VASP considers that further due diligence is required, it may also consider other elements such as:

- **Products and services provided:**
    - Some VASPs may wish to consider the range of products and services offered by the counterparty VASP, especially as certain offerings, such as privacy coins and fiat on/off ramp channels, might pose higher financial crime risk. In addition, information related to clientele, geographic coverage, and transaction volume is also valuable to infer relative levels of financial crime risk.
- **Compliance framework:**
    - VASPs need to evaluate the quality of the counterparty VASP's financial crime control program, systems and controls, including how the counterparty VASP conducts customer due diligence, the scope of on-chain and off-chain screening, record keeping practices, and the size of its compliance team.

Operationalisation / Elements to be Included in a Procedure

CVDD, however, does not stop at the initial due diligence, but must also take account of information that emerges after that, to capture changes in the risks posed by the counterparty and the nature of the counterparty relationship. In this sense, we recommend that a CVDD procedure should contain the following elements:

- **Definition of a risk-based approach:**
    - Risk factors to be considered in assessing the risks posed by counterparties and intermediaries within the transfer chain, and consideration of these risk factors during initial and ongoing due diligence.
    - Extent of due diligenceto be applied depending on the assessed risks, and approvals required for high-risk counterparts before commencing a relationship.
- **Initial due diligence:**
    - Contents of due diligence questionnaire (see section above).
    - Extent of use of third-party data/solutions/questionnaires, and controls in place to mitigate the risks of reliance on such third parties.
    - Extent of sanctions and adverse media screening.
    - Use of blockchain analytics and wallet screening capabilities to inform initial due diligence.
    - Record-keeping policy.

- **Ongoing due diligence and monitoring:**
    - Time-triggered reviews:
        - Definition of a frequency for the update of due diligence questionnaires using a risk-based approach.
    - Event-triggered reviews:
        - Definition of events that may result in increased risk and thus a need to re-rate the risk of a counterparty and, consequently, a need to refresh the initial due diligence (e.g. regulatory actions, change in regulation, results from ongoing sanctions / adverse media screening, etc).
    - Use of Travel-Rule data and relevant management information to inform the assessment of risks posed by the counterparty (e.g. request response time, quality of responses, percentage of transactions with incomplete or missing information).
    - Wallet screening and transaction monitoring to identify emerging risks or potentially suspicious activity.
- **Escalation process:**
    - Procedures to reassess the risk level of the counterparty relationship through the incorporation of data/information from ongoing monitoring of the relationship.
    - Processes for internal escalation and for outreach to the counterparty and/or intermediary to obtain additional information or comfort in case of issues/incidents, including intermediate steps/actions to take before suspending transfers.
    - Escalation process to notify the regulator in case of repeated failures, as per applicable regulatory requirements.

Withdrawal and Deposit Flow

Regulatory Framework

In the UK, the Travel Rule requirements apply to a cryptoasset business (CB) when making a deposit or withdrawal to another cryptoasset business or with an unhosted wallet. These obligations are set out in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs), in particular Chapter 2:

- Regulation 64C, for withdrawals.
- Regulation 64D for deposits.
- Regulation 64E for intermediary CBs as it relates to missing information.
- Regulation 64G for unhosted wallets.

The regulations define a "cryptoasset business" as a cryptoasset exchange provider or a custodian wallet provider.

In addition, the JMLSG provides guidance.

Please note that regulation 64A(3) specifies that cryptoasset transfers, where both the originator and the beneficiary is a cryptoasset business acting on its own behalf, are excluded from the scope of application of the Travel Rule requirements.

Withdrawal Flow

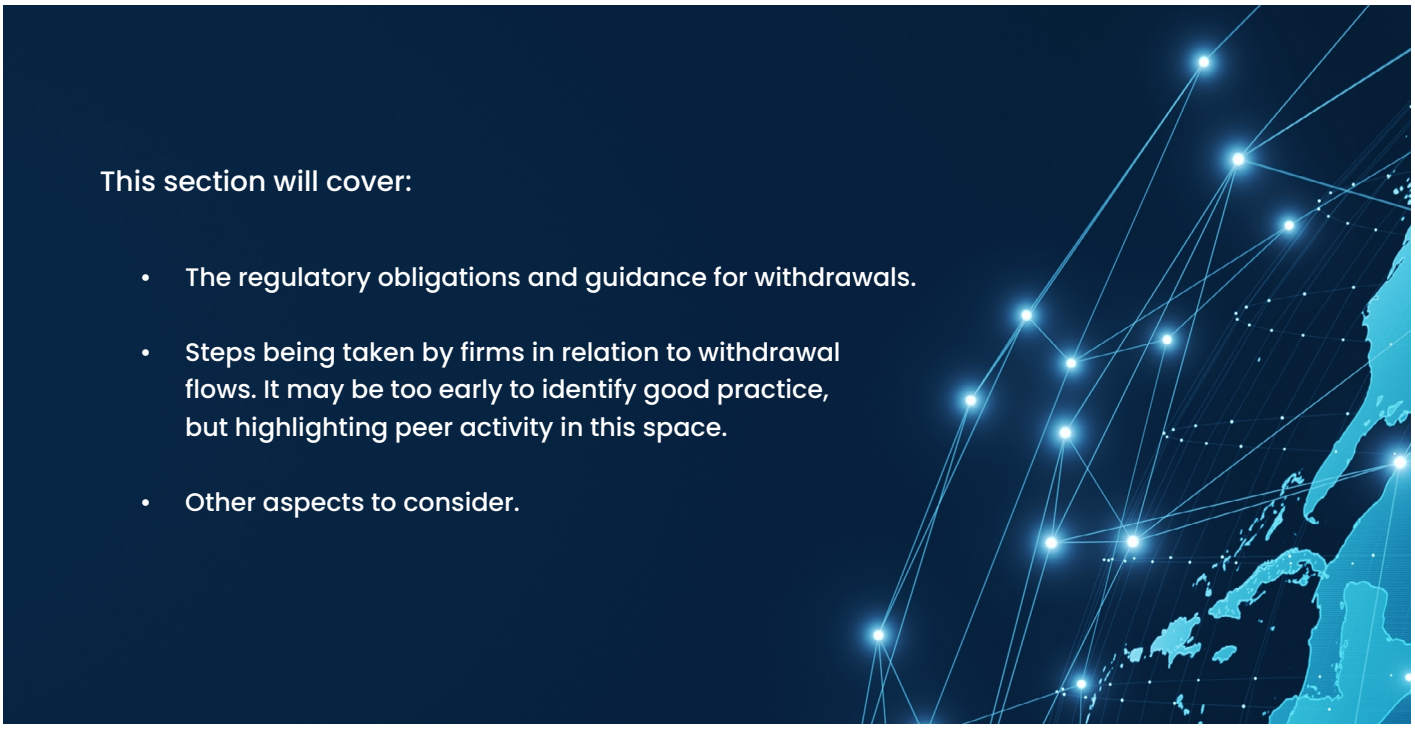
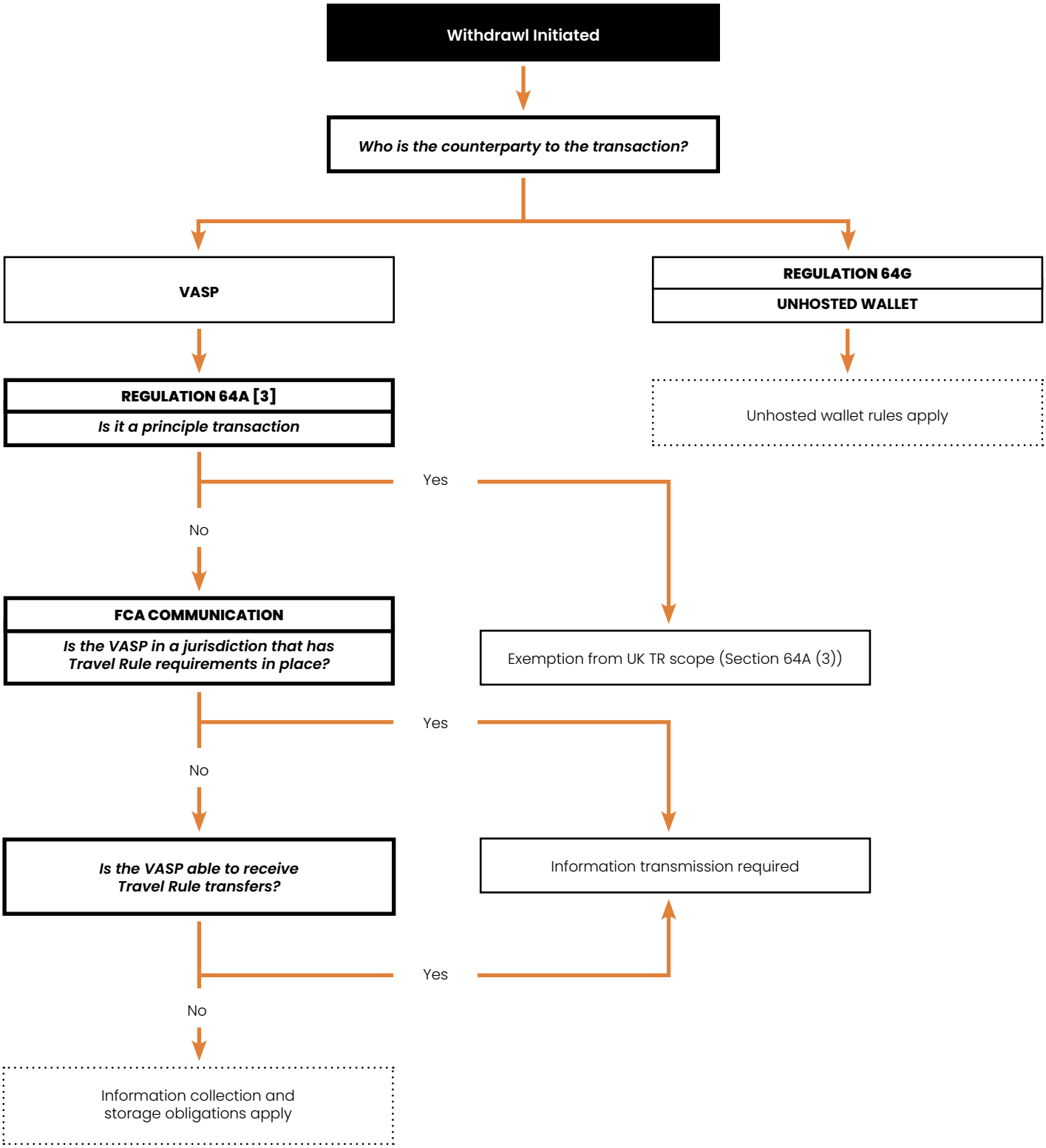


Diagram 1 below provides a visual representation of the factors that CBs should consider when determining when processing a withdrawal transaction.



Regulatory obligations and guidance

MLRs

Regulation 64C, sets out the specific information that the "originator" of an inter-crypto asset business transfer must provide before or at the time of the transfer, regardless of the transaction amount. The information transmission requirements are illustrated in the Table 1 below. This information includes:

- The name of the originator and beneficiary,
- if it is a firm, the registered name or where there is not one, the trading name and
- the account number of both parties or a unique transaction identifier in the absence of an account number.

Furthermore, if the transaction involves cryptoasset businesses operating in the UK:

- The cryptoasset business of the beneficiary can request further information, such as customer identification numbers or addresses,
- this information must be provided by the originator within three working days.

If the transaction involved a VASP/counterparty outside of the UK, a broader set of data has to be transmitted, when both of the following conditions are met:

- At least one counterparty (i.e. either the originator VASP, the beneficiary VASP, or the intermediary VASP) carries-on business outside of the UK with respect to the transaction; and
- The transfer is equal to or exceeds the equivalent in cryptoassets of 1,000 euros.[11]

Table 1: Travel rule information requirements per Regulation 64C MLRs

Required Information in Inter-crypto Asset Business Transfers		**UK Transactions**	**International Transactions <1000 EUR**	**International Transactions ≥1000 EUR UK Transactions Upon Request**
Basic Information	Name of originator *Registered name if a firm, or trading name if no registered name.*	✓	✓	✓
	Name of beneficiary *Registered name if a firm, or trading name if no registered name.*	✓	✓	✓
	Originator account number *Or unique transaction identifier if there is no account number.*	✓	✓	✓
	Beneficiary account number *Registered name if a firm, or trading name if no registered name.*	✓	✓	✓
Additional Information	One of the following data points about the originator customer: If the originator is a firm: • The customer identification number; or • the address of the originator's registered office, or, if different, or if there is none, its principal place of business; If the originator is an individual: • The customer identification number; or • the individual's address; or • the individual's birth certificate number, passport number or national identity card number; or • the individual's date and place of birth.	✗	✗	✓

11 MLTFR 2022, pg.5, para. 64C(1), (4).

JMLSG Guidance

The JMLSG provides guidance, stipulating that the originator's cryptoasset business must verify the information relating to the originator independently from a reliable source before executing the transfer. The CB of the originator is prohibited from making an inter-cryptoasset business transfer before ensuring full compliance with its information transmission obligations.

The JMLSG guidance sets out that the CB of the originator has the option to proceed with the transfer after the CB of the beneficiary has confirmed that the beneficiary information aligns with the verification of its customer due diligence (CDD). This course of action is only advisable if it does not excessively prolong the transaction completion time, adheres to established procedures, and aligns with a risk-based approach.

This provision reflects a pragmatic approach:

- CBs have the flexibility to proceed with the transaction after sending the required Travel Rule information; and
- although not obliged, are permitted to process the transaction only after both counterparties have assessed and accepted the transaction to avoid the complexities of dealing with non-compliance or discrepancies after settlement (which, in cryptoasset transfers, is immediate and irreversible).

The JMLSG:

- Emphasises the importance of record-keeping and timely response to information requests.
- Recognises the use of technological solutions for compliance, with the caveat that CBs retain liability and responsibility for their obligations under the MLRs, and
- clarifies that if a transfer involves a jurisdiction with more stringent requirements than those stipulated in the MLRs, the CB fulfils its obligations under UK law by providing the necessary information in accordance with the parameters specified in the MLRs.
- With regards to withdrawals, it recognizes the Sunrise Period[12] as a challenge for VASPs (i.e. dealing with counterparts in jurisdictions where the Travel Rule is yet to be implemented). It advises VASPs to consider any communications from the Financial Conduct Authority (FCA) on this matter:
    - The FCA's communication, of August 17, 2023[13] , sets guidance where a counterparty is in a **jurisdiction that does not yet have Travel Rule requirements in place and cannot receive the required information**. The originator UK CB must still collect, verify and store the required data in accordance with MLRs, before executing the transfer.

Steps being taken by firms in relation to withdrawal flow

Step 1: Counterparty identification

Identifying who controls the counterparty wallet is the first step in a Travel Rule–compliant transaction flow.

The qualification of the counterparty that controls the originating or beneficiary wallet will determine which Travel Rule requirements apply. Requirements vary, depending on whether the transaction is to be conducted with an unhosted wallet or a VASP. Requirements may also differ depending on whether the counterparty VASP sits in the same jurisdiction or a third country. Therefore, compliance with the Travel Rule hinges on accurate identification of the counterparty.

See also the 'Counterparty VASP Due Diligence' section of this guide for further considerations in relation to VASP due diligence.

12 JMLSG Guidance, Part II, Annex 22-I.

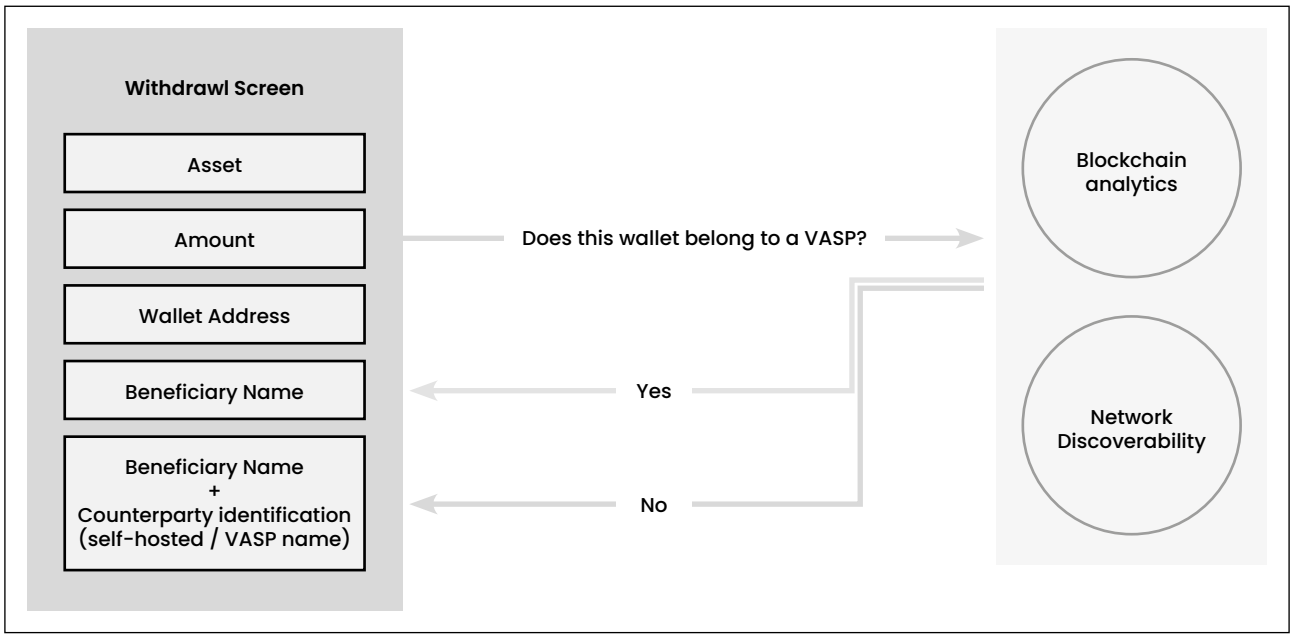
13 https://www.fca.org.uk/news/statements/fca-sets-out-expectations-uk-cryptoasset-businesses-complying-travel-rule.

Currently, VASPs rely on the following methods to identify the counterparty to the transaction:

- Blockchain analytics
- Input from their end-customer, and
- other specific discoverability methods available in their Travel Rule network.

Examples of adopted processes are illustrated below.

Example 1: Collection of counterparty type and identification from the customer only where it is not autonomously identified through the tools available to the VASP.



In example 1 the originator CB first collects the information required to execute the transaction (asset, amount, wallet address and beneficiary name). Then, this information is queried in real-time against blockchain analytics and the available network discoverability methods to:

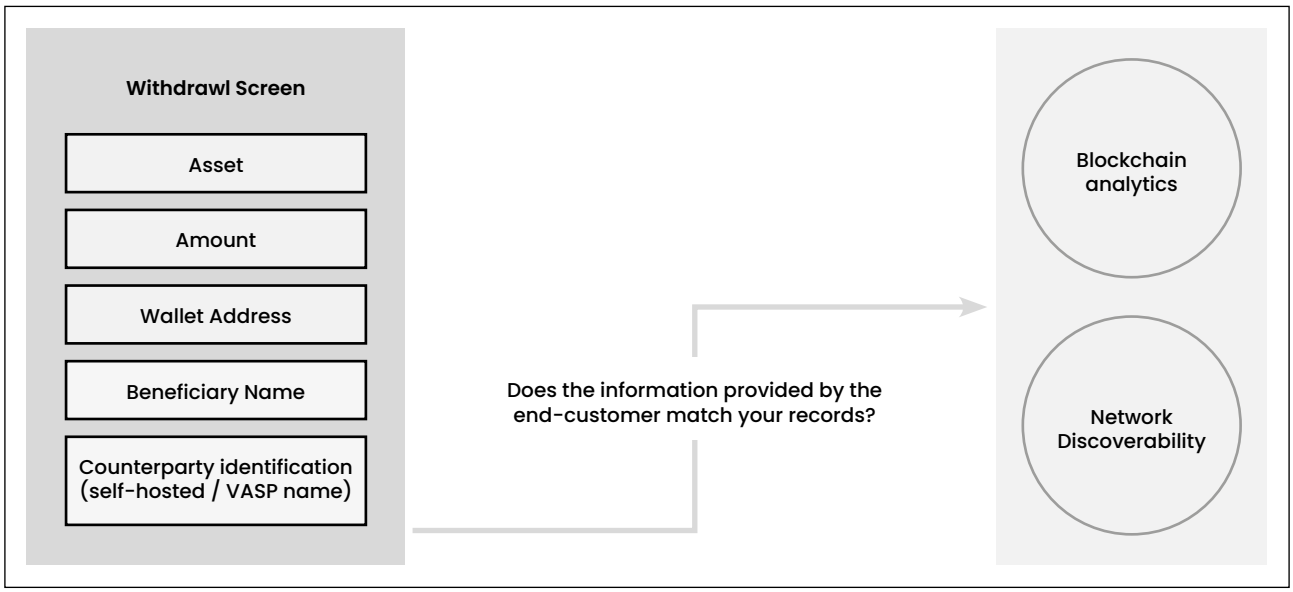
- Qualify the transaction against Travel Rule requirements (this includes, e.g. converting the transaction amount to Euros and assessing the information transmission obligations based on the applicable compliance threshold), and
- attempt to identify the counterparty to the transaction through the available methods - in this case, blockchain analytics and network discoverability.

If the CB is able to autonomously identify a counterparty VASP, it does not need to collect such information from the end-customer.

If a counterparty VASP is not identified, the CB needs to enquire the end customer about the counterparty type (i.e. is the transaction with an unhosted wallet or a VASP).

In all cases, the originator VASP will need to identify the legal entity that it intends to send the information to. This can be done in a variety of ways, and importantly through any methods available through travel rule solution providers.

Example 2: Collection of counterparty type and identification from the customer regardless of whether it is autonomously identified through the tools available to the VASP.



In example 2 the originator CB opts for collecting **all** the necessary information from the end-customer at outset, regardless of being able to autonomously identify the counterparty VASP.

In these cases CBs can then check for discrepancies between the information provided by the end-customer and the information made available by blockchain analytics providers and network discoverability methods.

Step 2: Pre-transaction risk decisions and sending of Travel Rule information

CBs can deploy a set of risk-based criteria to determine its approach to Travel Rule transfer, which includes, but is not limited to, for example:

- **Jurisdictional considerations:**
    - The regulatory landscape varies significantly across jurisdictions. CBs must navigate these differences, considering both the sender's and receiver's regulatory environments. CB's exploration of individual jurisdictions underscores the complexity, with varying standards potentially affecting data transmission decisions.
    - This may be considered alongside the CounterParty VASP Due Diligence section in this guide, and where a firm might for example, identify its key counterparties and the jurisdictions that they are based, to assess the counterparties travel rule obligations and risks but also where there are no obligations, whether the counterparty is willing to agree some level of voluntary compliance with receiving and sending Travel Rule information, in a UK GDPR compliant manner.
- **Nature of the counterparties:**
    - Depending on whether a transaction is between two CBs or an unhosted wallet, significantly influences the Travel Rule obligations.
    - Initial challenges include identifying whether the CB is within the necessary Travel Rule network, as provider interoperability is a key aspect, and if not, it is a process of identifying what mechanism of notification, sharing and verification of data, is possible in a UK GDPR compliant manner.

- **Risk profile:**
    - Transactions are assessed based on a variety of criteria, including the sender and recipient's risk profiles and the source and destination of funds.
    - A significant challenge arises when discrepancies between user-provided data and on-chain monitoring tools occur, prompting a reliance on user explanations in line with a risk-based approach.

Other aspects to consider

Automation - performing faster compliance checks

CBs increasingly leverage automated systems to manage compliance criteria efficiently, ensuring adherence to the Travel Rule across diverse jurisdictions. These systems are integral for:

- By pre-screening transactions against established criteria, these automated tools identify those requiring Travel Rule compliance. This includes evaluating the counterparty's nature and understanding jurisdictional implications, underscoring the importance of network integration and interoperability among CBs.
- Automation significantly reduces human error and expedites compliance checks. For example, when encountering newly created wallets lacking transaction history, these tools utilise all available user data and previous interactions to facilitate informed decision-making.
- Automated systems are designed to be agile, accommodating the varied implementations of the Travel Rule across jurisdictions. This adaptability ensures CBs remain compliant amidst evolving regulatory landscapes.

Process and procedures

Further examples on how CBs might want to consider enhancements to their withdrawal processes, include:

- Establishing auto-approval mechanisms for withdrawals to known and trusted CBs and setting definitive timelines for addressing missing data inquiries, CBs can enhance operational efficiency without compromising compliance.
- Leveraging blockchain analytics by pre-screening wallets for suspicious activities ahead of transactions. This proactive measure is crucial for managing the intricacies of unhosted wallets or those newly identified, addressing discrepancies between the provided user data and on-chain information.
- Faced with uncertainties such as undefined wallet statuses or potential data breaches, prioritising customer explanations backed by comprehensive due diligence (e.g., KYC/KYB) is essential. This strategy supports processing transactions irrespective of the CB's network affiliation, focusing on prioritising user data and risk assessment.

Set/agree timescales for responses

The Travel Rule requires CBs to exchange prescribed information for transactions exceeding defined thresholds. One aspect that a CB might consider to improve the overall efficiency of its processes, is to set a defined time period within which the recipient CB must acknowledge receipt of this information or respond accordingly before executing the transaction.

Response period

The Travel Rule requires the originating CB to transmit the prescribed information to the beneficiary CB. JMLSG[14] states:

"The CB of the originator may consider executing the transfer after the CB of the beneficiary has checked that the beneficiary information corresponds with verification of its counterparty due diligence (CDD), if it does not unduly impact time required to complete the transaction and is in line with its procedures."

Therefore, although not obliged, CBs are permitted to process the transaction only after both counterparties have assessed and accepted the transaction to avoid the complexities of dealing with non-compliance or discrepancies after settlement (which, in cryptoasset transfers, is immediate and irreversible). This time period is established to:

- Allow both the originating and beneficiary CBs have sufficient time to fulfil their regulatory obligations under the Travel Rule, verifying the accuracy and completeness of the information exchanged.
- Allow CBs to manage transaction flows more efficiently, reduce the need for dealing with non-compliance or risk mitigation post settlement and avoid dealing with returns of funds.

By designating a time-period, it allows for better assessment of the transaction and the information exchanged, providing an opportunity to address any discrepancies or concerns that may compromise compliance or security.

Procedure in the event of non-response

Should the beneficiary CB fail to respond within the allocated time frame, the originating CB should consider proceeding with the transaction based on a risk-based assessment, in accordance with the regulations and guidance.

Challenges and approaches to operationalisation

Interoperability

A key challenge faced by VASPs in complying with the Travel Rule is ensuring interoperability among various Travel Rule service providers.

In the context of VASPs, this means enabling transactions and data exchanges across various VASPs and networks. However, the landscape of digital asset services is diverse, with each provider often operating on its own unique network or platform. This diversity can create barriers to the smooth transfer of information required by the Travel Rule regulation.

Cross-border discrepancies

Travel Rule requirements vary significantly across jurisdictions, in particular in terms of applicable compliance thresholds and required scope of information. This has a potential impact on the ability to transact cross-borders in a Travel Rule compliant manner.

As mentioned in the Regulatory Framework section within this chapter, the JMLSG Guidance clarifies that if a transfer involves a jurisdiction with more stringent requirements than those stipulated in the MLRs, the CB fulfils its obligations by providing the necessary information in accordance with the parameters specified in the MLRs.

14 JMLSG Guidance Sector 22, Annx 22-I.

However, when confronted with these scenarios it is important for CBs to consider that their counterparts may be unable to accept transactions that are not accompanied by the full scope of information they are required to receive under the Travel Rule regulations in their jurisdiction. This should not be assumed, but rather considered and monitored. By way of example, VASPs in Canada are required to receive the beneficiary residential address. This is a data point that UK CBs are not required to collect or transmit and, as clarified in the JMLSG guidance, the fact that the beneficiary VASP is Canadian does not change the obligations of the UK CB. But this also does not change the obligations of the Canadian VASP, who may be required to reject the transaction.

It is therefore useful that CBs actively monitor their counterparties' responses to the Travel Rule transfers and obtain information about the potential reasons for rejection. As CBs learn about potential incompatibilities with certain counterparties or jurisdictions, they may wish to consider what if any follow-up actions they might take.

Deposit Flow

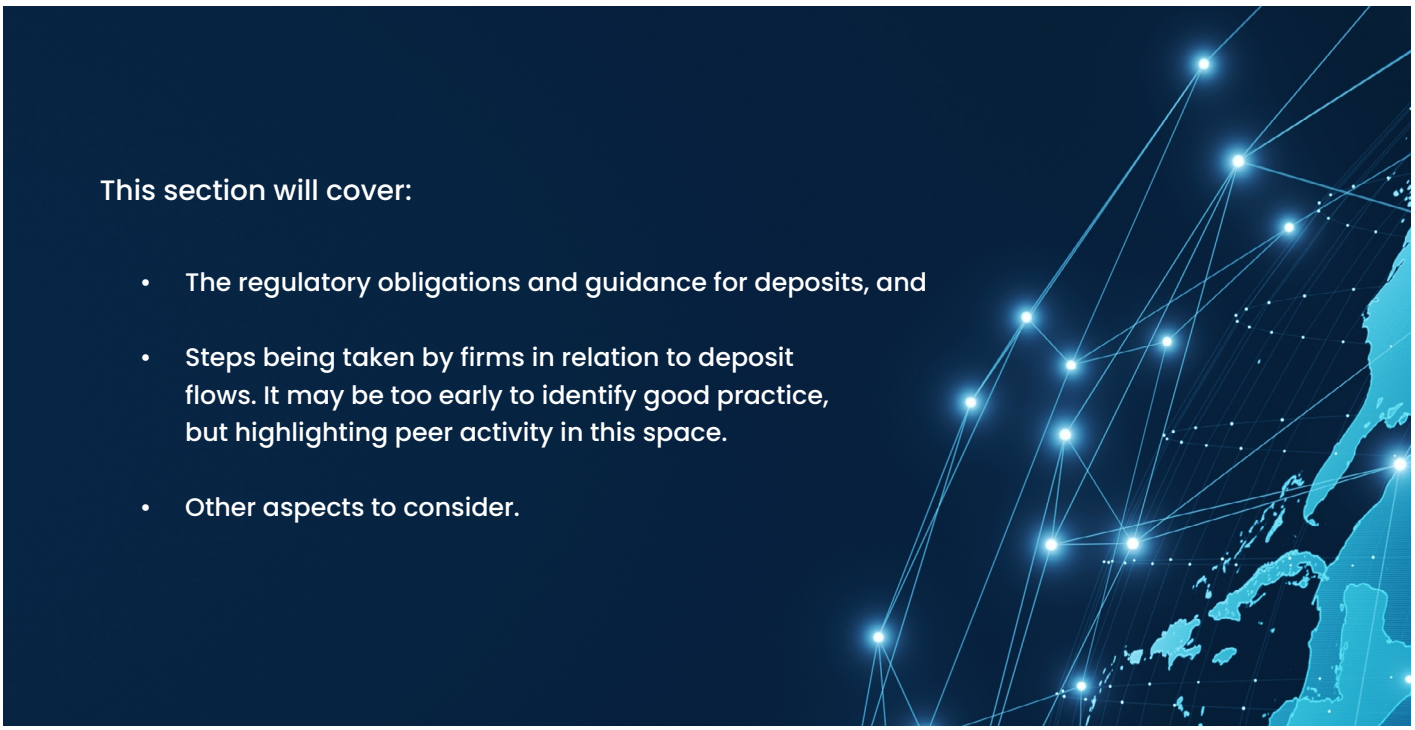
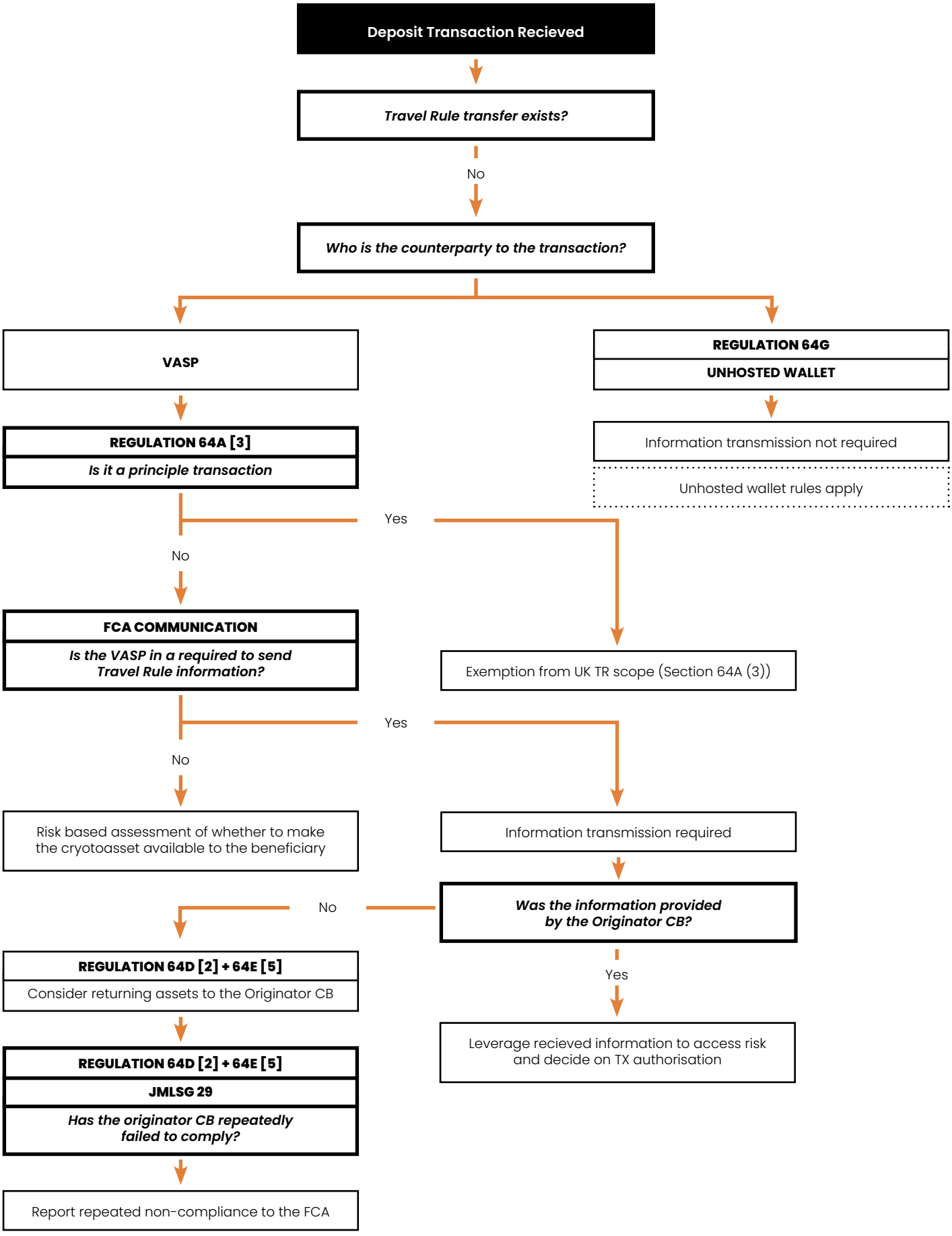


Diagram 2 below provides a visual representation of the factors that CBs should consider when determining when processing a deposit transaction.



Regulatory obligations and guidance

MLRs

Regulation 64D requires the beneficiary CB to verify received information before making cryptoassets available to the beneficiary. This verification includes ensuring that the information on the beneficiary aligns with data previously verified under customer due diligence.

If any information is missing or does not correspond to the records held by the beneficiary CB, it must request the originator CB to provide the necessary details, consider making inquiries into discrepancies, and assess the risk. The business may choose to delay making cryptoassets available to the beneficiary until resolution or, if unresolved within a reasonable time, return the cryptoassets to the originator CB.

Regulation 64E focuses on intermediary CBs involved in inter-cryptoasset transfers. Intermediary CBs are required to verify the received information before further transferring cryptoassets. If information is missing, the intermediary business must request it from the originator CB, consider delaying onward transfers until the information is received, and, if not received within a reasonable time, contemplate returning the cryptoassets to the originator CB.

Note: JMLSG provides some guidance as to a level of materiality of inaccurate data.

Both beneficiary and intermediary CBs should carry out risk assessments to guide their actions in line with regulations 18(1) and 18A(1). This assessment involves a consideration of factors, such as the purpose and nature of the business relationship with the beneficiary, the value of the inter-cryptoasset business transfer, linked cryptoasset transfers, the frequency of transfers involving the beneficiary, and the duration of the business relationship.

Note: JMLSG also suggests consideration of the counterparty cryptoasset business's jurisdiction as an additional relevant factor. CBs in alignment with their risk assessments and recognizing ML/TF/PF risks posed by customers, must ensure that their determinations are proportionate and reasonable. CBs are encouraged to document the steps taken to address failures in providing required information and establish a clear process of escalation, including the issuance of warnings and deadlines for compliance by the originator's cryptoasset business.

JMLSG Guidance

The JMLSG provides guidance on the process of returning a transfer to the originator CB. It reminds firms to consider assessing the risks and complexities of returning a cryptoasset to the originator, and clarifies that this does not constitute a cryptoasset transfer for Travel Rule purposes.

Both, beneficiary and intermediary CBs, are mandated to report instances of repeated non-compliance by other CBs to the FCA. This reporting obligation extends beyond the acknowledgment of non-compliance and requires the beneficiary and intermediary CBs to detail the steps taken in response to such failures.

Moreover, as emphasised in the JMLSG Guidance, the reporting obligation follows a risk-based approach, allowing for a determination of what constitutes repeated failure. Factors such as the volume and size of transactions over a period of time or a percentage of transaction failures from a particular cryptoasset business may be considered in this assessment. Importantly, these reporting requirements apply irrespective of the originator cryptoasset business's jurisdictional obligations.

Furthermore, the FCA's communication of August 17, 2023[15], sets out guidance for UK CBs when engaging in transactions with counterparts from jurisdictions where the Travel Rule is not yet in force. Upon receiving a transaction lacking the essential Travel Rule information, the CB is tasked with conducting a risk-based assessment. This evaluation considers the Travel Rule regulatory status in the jurisdiction where the counterparty operates, guiding the decision on whether to make the crypto-assets available to the beneficiary customer.

15 https://www.fca.org.uk/news/statements/fca-sets-out-expectations-uk-cryptoasset-businesses-complying-travel-rule.

Steps being taken by firms in relation to deposit flow

The dynamic interplay between technology and regulation necessitates a comprehensive approach to managing digital asset transactions, especially in the context of deposits, regulatory frameworks, and the application of the Travel Rule.

Some shared practices below outline the key focus for VASPs, aiming to enhance compliance while maintaining operational efficiency:

- **Qualification of deposits:**
    - VASPs should systematically identify the nature of each deposit, distinguishing between those from unhosted wallets and other VASPs. This distinction is vital for determining the required scope of information and ensuring adherence to compliance requirements.
- **Regulatory framework:**
    - Conduct an assessment of the regulatory requirements in both the sender's and receiver's jurisdictions.
- **Threshold evaluation for Travel Rule:**
    - Analyse each deposit against the set threshold for Travel Rule compliance, adjusting verification processes for transactions that meet or exceed this threshold.
- **Auto-approval processes:**
    - Automation of approval processes will make the process more efficient and scalable. Any automation should be carefully assessed that it meets the VASP's compliance framework and should be regularly reviewed to ensure that it continues to do so, and is up-to-date with current regulation/guidance.
- **Protocol for missing data requests:**
    - Establish clear protocols for requesting missing data and defining standard response periods to balance the need for compliance with operational efficiency.

Handling of incomplete / missing information

- Upon notification of a transaction, beneficiary VASPs must verify that the beneficiary's information aligns with KYC data held. If discrepancies or missing data are identified, the originating VASP should be contacted to resolve these issues, employing a risk-based approach when assessing discrepancies.
- Withhold cryptoassets from the beneficiary until all required data and enquiries are satisfactorily resolved. All decisions should be based on a risk assessment, documented thoroughly, and actions justified accordingly.
- Make a risk-based assessment before allowing the beneficiary to access the cryptoassets, considering the broader context of the transaction, including the originating and receiving jurisdictions.
- For transactions common to a beneficiary's account, a risk-based evaluation should include the purpose and nature of the business relationship, the expected source and destination of funds, the transaction values and frequency, the duration of the business relationship, and the jurisdictions involved.
- While Travel Rule solutions may automate compliance processes, the ultimate responsibility for decision-making rests with the registered entities.
- Maintaining comprehensive documentation.

Return of funds

When confronted with the obligation to return funds to the originator CB, the beneficiary CBs face additional challenges:

- CBs are exposed to liability for loss of funds - the CB cannot assume that funds can be returned to the sending wallet address, as this address may not be prepared to receive funds and, if so, the funds may be lost.
- CBs are exposed to sanction risks:
    - By returning funds without fully understanding their origin, CBs risk returning funds to sanctioned or high-risk actors.

After the on-chain transaction is settled it becomes very challenging for CBs to handle non-compliance effectively. In this respect, paragraph 32 of the JMLSG establishes that CBs "should consider the risks and complexities thereof 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 cryptoasset is able to be returned to the originator."

The strict UK Travel Rule requirement[16] is to send the Travel Rule information before or at the same time as the transaction. However, JMLSG provides guidance for a more effective and efficient approach for the UK market as a whole.

As stated in the Withdrawal Flow section above, according to JMLSG paragraph 18, and where any delay to confirm details does not unduly impact transaction latency, the originator CB may consider executing the transaction after having received a response from the the beneficiary CB that confirms that the beneficiary information matches and that the CB accepts receiving the funds.

This approach would mitigate the issue of dealing with non-compliance or discrepancies post-settlement. However, this should not be a strict approach during the sunrise period - otherwise, it may significantly impact the CB's business.

Other aspects to consider

Addressing the operational challenges of deposit compliance under the Travel Rule regulation involves navigating a complex landscape marked by interoperability issues, regulatory discrepancies across jurisdictions, and the inherent risks associated with new wallet transactions.

Effective operationalisation of compliance practices is essential for ensuring seamless communication and data exchange between a diverse array of VASPs and their networks, which is a key element to the efficient processing of deposits.

Moreover, the variability in the regulatory landscape poses additional hurdles, as VASPs must adapt their compliance efforts to meet different international standards and requirements, rendering a one-size-fits-all approach impractical. To mitigate these challenges, a CB may wish to consider:

- **A multifaceted strategy:**
    - This includes using advanced blockchain analytics and comprehensive due diligence processes specifically tailored to address the unique risks presented by deposits from newly created or unhosted wallets.
    - These analytical tools are important in verifying the integrity of transactions and ensuring compliance with the nuanced aspects of the Travel Rule.

16 Regulation 64C (9) of the MLRs.

- **Maintaining an agile compliance framework:**
    - Regularly reviewing and adjusting compliance processes in response to regulatory developments allows VASPs to remain flexible and responsive to new challenges.
    - This agility is important in a rapidly evolving regulatory environment, ensuring that VASPs can operate efficiently and compliantly.
- **Establishing and maintaining open lines of communication with regulatory bodies and other VASPs:**
    - This fosters a collaborative approach to overcoming interoperability challenges and aligning regulatory interpretations and expectations.
    - This joint stance not only aids in smoothing out the operational complexities associated with compliance but also contributes to developing a more cohesive and universally understood set of practices for managing deposits under the Travel Rule.
    - Through these concerted efforts, VASPs can navigate the complexities of deposit compliance, ensuring the integrity and security of transactions within the digital asset ecosystem, all whilst adhering to the principles and regulations set forth by national and international standards.
- **Taking steps to identify its main counterparties in relation to transactions (withdrawal and deposit):**
    - To ensure a Travel Rule compliant mechanism to transfer information in a UK GDPR compliant manner, with those key counterparties.

Unhosted Wallets

This section looks to set out some of the financial crime risks that might be posed by interacting with unhosted wallets (also known as self-hosted or non-custodial wallets) and what mitigants to these risks are being used by CBs.

This chapter considers transactions between VASPs and unhosted wallets. We look to set out some of the financial crime risks that might be posed by interacting with unhosted wallets, including anonymity, lack of intermediaries, and transaction speed, posing challenges for both VASPs and law enforcement agencies.

We include some suggestions on how to assess that risk and what mitigants a VASP may choose to consider to build an overall compliance framework. Unhosted wallets continue to be a key part of the crypto ecosystem.

Regulatory Framework

In Article 64B, the Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022 (MLRs) defined unhosted wallets as "software or hardware that enables a person to store and transfer a cryptoasset on their own behalf, and in relation to which a private cryptographic key is administered by that person".

The use of unhosted wallets has gained recent popularity which may, in part, be due to certain high profile market failures (e.g. the collapse of Celsius and FTX in 2022). Current estimates show that around 40% of crypto is held in unhosted wallets.

The legal obligation governing UK Travel Rule transactions between cryptoasset businesses and unhosted wallets is set out in Article 64G of the MLRs. Within this regulatory framework, cryptoasset businesses (CBs) involved in unhosted wallet transfers may request specific information from their customers, be it the originator or beneficiary. The specific information that should be requested for the purposes of unhosted wallets is outlined in the Table 2 on the following page.

The decision to request information is guided by the risk assessments conducted under regulations 18(1) and 18A(1), and an assessment of the potential risks of money laundering, terrorist financing, and proliferation financing associated with the unhosted wallet transfer.

The MLRs set out that, in case the information requested from the end-customer is not provided, the CB should not make the assets available to the beneficiary. In withdrawals, this prevents the CB from executing the withdrawal transaction to the unhosted wallet. In deposits, this prevents the CB from releasing the received funds to the end-customer.

Table 2: Specific information that should be requested from unhosted wallet customers

Data That Should be Requested from the Customer *Only information that is not already available to the CB needs to be collected*	**Transactions < 1000 EUR**	**Transactions ≥ 1000 EUR**
Name of originator *Registered name if a firm, or trading name if no registered name.*	✓	✓
Name of beneficiary *Registered name if a firm, or trading name if no registered name.*	✓	✓
Originator account number *Or unique transaction identifier if there is no account number.*	✓	✓
Beneficiary account number *Registered name if a firm, or trading name if no registered name.*	✓	✓
One of the following data points about the originator customer: If the originator is a firm: • The customer identification number; or • the address of the originator's registered office, or, if different, or if there is none, its principal place of business; If the originator is an individual: • The customer identification number; or • the individual's address; or • the individual's birth certificate number, passport number or national identity card number; or • the individual's date and place of birth.	✗	✓

The Joint Money Laundering Steering Group (JMLSG), Sector 22 Annex I (articles 34 et.seq) provides further guidance emphasising a risk-based approach for dealing with unhosted wallet transfers.

The JMLSG guidance reiterates that in cases determined to pose a higher risk through risk assessments, a CB should take reasonable steps to seek additional information about the unhosted wallet from their own customers. The assessment of risk takes into account various factors, including the purpose and nature of the business relationship (which should be collected at the customer onboarding stage), the value of the transfer, the frequency of transfers, and the duration of the business relationship with the customer.

Moreover, for high-risk cases, additional measures such as establishing control over the unhosted wallet through methods like micro deposit or cryptographic signature, are recommended before authorising the transfer.

Underlying Financial Crime Risks

Inherent risks associated with unhosted wallets' features

Unhosted wallets allow users to take control over ownership of their assets and not to rely on a 3rd party to hold these assets, typically therefore maintaining ownership and the private key. Arguably this is one of the benefits of distributed ledger technology to traditional finance.

Furthermore, the UK Travel Rule approach recognised the value of unhosted wallets to users and so looks to take a more proportionate approach to balance the benefits and risks of unhosted wallets.

Unhosted wallets do pose certain challenges for VASPs and law enforcement as they are typically not identifiable or always readily attributed in blockchain analytics to an individual (unless related to a sanctioned or illicit wallet).

From a financial crime perspective, some examples why a unhosted wallet poses risks of being exploited by individuals and/or organised crimes gangs (OCGs) for illicit purposes include:

- **Level of anonymity:**
    - A risk with unhosted wallets is that they create a level of anonymity.
    - This anonymity is less where the wallet can be identified by analytics, for example, to be in the control of an illicit actor.
- **No intermediaries or KYC:**
    - The ease and speed in which the unhosted wallets can be set up without any due diligence being performed,
    - and the fact that there are no intermediaries that have oversight or control over the activity being conducted through the unhosted wallets.
- **Speed of transaction:**
    - The speed at which value can be transferred on the blockchain and coupled with the lack of involvement of regulated intermediaries creates challenges to law enforcement when conducting their investigations which involve unhosted wallets.

Table 3 below provides an indicative comparison between crypto transfers and fiat transfers.

Table 3: Indicative comparison between crypto transfers and fiat transfers

	Crypto Transfers through Unhosted Wallets	Cash Based Transfers / Deposits	Fiat Wire Transfers
Speed / Velocity	Immediate	Immediate, based in physical movement.	Not immediate and dependent on processing infrastructure / timing at financial institution (FI).
Immutability	Yes - crypto transactions cannot be reversed.	No	No - mechanisms in place to recall sent funds.
Traceability	Full traceability - the blockchain facilitates full traceability until the point a serviced wallet is involved.	No	Limited - as an example Bank A wires to Bank B, who in turn wires Bank C. Bank C will only have visibility to Bank B and not Bank A.
Anonymity	Yes	Yes	No
Source of Funds Check	Yes - the blockchain facilitates transparency of where the crypto has been sent from and the various exposure types of the sending wallet exposure.	No - with cash based deposits there is no source of funds check.	Dependent upon FI's risk based approach. Wire transfers only allow for visibility of the previous leg in the transaction.

The anonymity element is the biggest threat/risk, however once the intersection with a MLR registered firm has taken place and, with the adoption of appropriate and proportionate risk based approach, the risks associated with the unhosted wallets can be mitigated.

Unlawful uses of unhosted wallets

To avoid any misconceptions it is critical to understand that cryptoassets have not introduced anything new in terms of financial crime, what it has introduced is an alternative asset class / technology which criminals can exploit.

Some examples, but not limited to, of how an unhosted wallet may be used to facilitate nefarious activity is illustrated below:

- **Smaller scale and individual exploitation:**
    - Purchasing goods/services from darknet markets, etc.
- **Larger scale financial crime:**
    - Organised criminal gangs may use non hosted wallets when moving funds as part of their off-ramping tactics.

AML Risk Assessment

As mentioned earlier in this guide, the decision to request information in relation to an transfer to an unhosted wallet is guided by the risk assessments conducted under regulations 18(1) and 18A(1), and an assessment of the potential risks of money laundering, terrorist financing, and proliferation financing associated with the unhosted wallet transfer. These are the traditional risks related to assessing financial crime risk (eg customer, product, transaction, geographical and delivery channel risk).

When considering transactional specific risk, Paragraph 22.34 of Part II Sectoral Guidance provides higher-risk factors CBs should consider when assessing their risk exposure in relation to cryptoassets more specifically.

When assessing transactional risk, it is important to remember that this risk should not be taken in isolation and should feed into KYC.

Some of the elements or tools that you might take into account when make as assessment of risk might include:

JMLSG Guidance Notes

The Joint Money Laundering Steering Group updated their Sectoral Guidance with the introduction on Annex 22-1 - Cryptoassets Transfers ('Travel Rule')[17].

As illustrated in Table 4 on the following page, paragraph 35 of Annex 22-1 provides some guidance when assessing the level of risk arising from an unhosted wallet transfer. In order to adequately assess the level of risk, one should have a basis to start from, which in this case will be the KYC information collected from the customer during the onboarding process.

17 The sectoral guidance should not be read on its own. It should be read in conjunction with Part I of JMLSG Guidance Notes and Part II Sector 22.

Table 4: JMLSG extract of guidance[18] when assessing unhosted wallet transfer risks

The Purpose and Nature of the Business Relationship with its Customer and the Unhosted Wallet Transfer
The onboarding process should establish the purpose and nature of the account being opened by the customer. The information can then be used as a basis to facilitate the identification of unusual and/or suspicious activity on the customers account.
The Value of the Transfer and Any Linked Transfer
The onboarding process should provide a CB with information related to expected value of transfers and should be continually monitored thereafter. This monitoring will facilitate the identification of unusual and/or suspicious behaviour. When monitoring linked transfers a CB should have monitoring capabilities to identify, but not limited to: • Shared devices • Shared payment methods, i.e. cards, banks accounts • Shared (residential) addresses • Shared IP addresses • One to many / many to one scenarios
The Frequency of the Transfers Made By or To the Customer
The information collected at the customer onboarding stage should form the basis of initial understanding of the frequency of transfers made by or to the customer. Other information collected at the onboarding stage, i.e. age, employment status, income etc can also be used to profile expected customer behaviour which can also be used to determine customer spend capability.
The Duration of the Business Relationship with the Customer
The longer a customer has their account with a CB, the better the CB is able to build out an improved customer profile, which in turn should be further referenced and used when monitoring customer behaviour. As the relationship matures, the CB is able to expand on the customer profile by referencing, but not limited to, the following data / information: • Device/s ID used • IP address used • Browsers and operating systems used • Payment methods used • Average transaction size

The use of blockchain analytics

Amongst other things, blockchain analytics enables the identification and attribution of wallets. CBs are then able to determine using their own risk based approach which service categories are prohibited and those which will require an investigation to determine the outcome/next steps.

Blockchain analytics provide the opportunity to assess the percentage risk exposure of a wallet. As an example, a firm will need to make its own decision on risk if illicit exposure risk to a wallet is significant and recent, one may easily conclude that there is clear intent in the behaviour of the wallet with engagement in illicit activity.

18 para 36, Annex 22-1 of JMLSG.

Furthermore when measuring transactional risk CBs may wish to consider the following, please note this list is not exhaustive:

- Proximity
- Velocity
- Pattern
- Transaction size

Thereby providing CBs with an improved understanding of its transactional risk. Noting that transactional risk should never be considered in isolation but feeds back to KYC, and the underlying risk that the CB is looking to mitigate.

Table 5: Considerations when assessing crypto transactional risk

	Areas to Consider	How?

Proximity (number of hops)	• What is the CBs proximity to the risky wallet?
	  • Is it direct/ownership exposure?
	  • I.e. is the destination wallet of the customer order the risky wallet?
	  • Is it indirect/counterparty exposure?
	  • I.e. the destination wallet of the customer order has no attribution, but has exposure to a risky wallet.
	  • Noting that indirect exposure risk should still be considered in the aggregate with the other risk factors mentioned.
		Blockchain analytics

Velocity	• How quickly has it moved across the blockchain (e.g. a matter of hours/days or years)?	Blockchain analytics
	• Is the velocity of activity aligned to the customer profile?	KYC / customer profile
Pattern	• Does it reflect a level of intended obfuscation/layering? • Is the on-chain pattern consistent with the customer profile?	Blockchain analytics
Behaviour	• Another consideration not limited solely to unhosted wallets is the direction of the activity.	Blockchain analytics
	• With certain attributions the difference between withdrawal and deposits may provide better insights as to whether the CBs customer is a potential suspect or victim of suspected nefarious activity. • Are there attempts to break down a single transaction to smaller ones in an attempt to go below certain thresholds to avoid scrutiny?	Case management systems

Indirect exposure becomes more challenging with the increased number of hops between the customers wallet and the risky wallet. Some noteworthy points in relation to indirect exposure are:

- **Privacy enhancing wallets:**
    - For example, unhosted wallets which add extra hops of history to a transaction, have built in mixing capabilities, etc.
- **Peel chains:**
    - Where funds move through multiple intermediary wallets/addresses.
    - Peel chains can occur naturally whereby nothing illicit is in play.
    - However, they can be abused by bad actors in order to obfuscate the origin of funds.

Technical Means Available to Mitigate the Risks of Transacting with Unhosted Wallets

In addition to the blockchain analytics capabilities for detecting and assessing financial crime risk, Travel Rule solutions can facilitate the identification and verification of unhosted wallets. This section explores some of these capabilities.

Note: Table 6 (on page 32) outlines, in relation to high risk transactions, some considerations when using different methodologies to verify that their own customer owns or controls a wallet address (pros and cons of micro-deposits and cryptographic signatures).

Wallet type identification

The CB must be able to identify if the address is, in fact, from an unhosted wallet, and not a CB, which would require different compliance steps.

Blockchain analytics can be helpful to inform on risk scores and identify entities such as crypto businesses or criminal organisations. It relies on a mixture of probabilistic and deterministic assessments, to determine if an address is owned by a VASP or any other actor in the ecosystem.

Analytics will typically be able to identify a wallet attributed to a VASP. However, numerous wallets are constantly being created by a VASP, and due to this analytics may not necessarily have immediately 'clustered' or attributed that wallet to the VASP. Consequently there may be some instances where a VASP wallet will display a level of similar analytics to an unhosted wallet (i.e. not clustered or labelled on the analytics solution), but the distinguishing feature may be transactional flow, for example (i.e. one is likely to show flows more akin to an exchange than an individual).

Nevertheless, it may be considered good practice for CB to rely on a combination of blockchain analytics information and their customer's self-reporting the wallet type (unhosted or custodial at another cryptoasset firm) at the time of the transfer. This allows for a level of internal verification and, potentially also, where risks arise, consider the analytics exposure to assess whether what information it provides tallies with the customer.

Wallet Ownership Verification

The objective of verifying the ownership of an unhosted wallet is to allow the CB to tie a known identity (the CB's customer) to the unhosted wallet in a transaction, which in turn will be of importance to avoid crediting funds to, or receiving funds from, an unknown third-party with unknown risk and potential exposure to sanctions. It may also be relevant for Law Enforcement Requests.

To achieve this when dealing with high-risk transactions, CBs need to request the user to take reasonable steps to evidence control (which infers to an extent to ownership) of an address. The JMLSG Guidance suggests two possible solutions to consider: a micro deposit or a cryptographic signature.

- **A cryptographic signature:**
  - Is a basic feature of every crypto wallet, but not all of them facilitate users to access it.
  - Using their unhosted wallet's private key, the owner can sign a message defined by the cryptoasset business.
  - Once the customer shares the signature, the CB can verify that it corresponds with the proposed message and the public key (wallet's address) to verify their ownership.

Example cryptographic signature process description:

1. The user is in a logged-in context of the VASPs website or app.
2. The wallet is requested to cryptographically sign a message (the message can either be a text string or a formatted piece of data. But it needs to be readable and verifiable by both humans and machines).
3. The customer reads the message and signs it using their wallet.
4. The signature is returned to VASP.
5. The signature is verified to have been signed by the customer's address.
6. The contents of the message signed are parsed and verified to match the address, customer identifier, and timestamp.

- **A micro deposit:**
  - A micro deposit is also known as a Satoshi test, penny test or microtransaction.
  - It consists of a small, mutually agreed-upon, transaction between the customer's unhosted wallet and the CB, conducted prior to the intended transfer.
  - Successful completion of a micro deposit provides evidence to the CB that the customer does control the unhosted wallet, thereby allowing the unhosted wallet address to be whitelisted.

Example micro-deposit process description:

1. A new deposit address is created for VASP and a random test amount is created.
2. The customer is requested to send a very small transaction of the test amount to the deposit address.
3. Customer sends funds.
4. Once received the funds are returned to the verified address.
5. The VASP verifies that the transaction was broadcasted and:
   a. One of the source addresses or transaction inputs matches the verified address.
   b. The amount matches the test amount.
   c. That the deposit address matches the destination account.
   d. The transaction was performed within the agreed time-window.

The mentioned methods vary in their levels of required effort from the customer and from the cryptoasset business' point of view, and so firms need to consider what approach they adopt and that it is aligned to their own RBA. Both options, when done manually, create work for the customer and are cumbersome. Although the cryptographic signature may be too difficult for non-expert crypto users, micro deposits heavily interrupt the transaction journey and are costly.

However, automated ways are available for cryptoasset businesses to request ownership proofs from customers, reducing friction at the time of transaction. Manual micro deposits involve back and forth communication with the customer and force the compliance team to review transactions and manage their deadlines, while the automated version of Satoshi tests does not require any setup or review work from the compliance team and may show the request in-product for a better user experience. Once the transaction shows in the blockchain, ownership is proven automatically.

As mentioned, manual cryptographic signatures may require a higher level of crypto expertise, which may lead to inefficiencies and failed ownership proofs. AOPP allows the user to sign a message with one click, removing the need to look for the signing functionality in the wallet, or copying and pasting data back and forth.

Some Travel Rule providers also offer dynamic and customizable front-end components that can be embedded into CBs' withdrawal and deposit flows to collect the required information about the unhosted transaction from the end-customer. Depending on the CBs' policies and risk assessments, this component can be set to trigger challenges (including automated cryptographic signatures) that allow CBs to verify that their customer controls the wallet they are transacting with.

Table 6: Pros and cons of micro-deposits and cryptographic signatures

	Cryptographic Signatures	Micro-deposits
Pros	• Reliable and secure • Immediate verification and whitelisting • Can be automated for the VASP & customer	• Reliable and secure. • Can be automated for the VASP.
Cons	• Potentially disproportionate customer friction (dependent on solution deployed).	• Potentially disproportionate customer friction (dependent on solution deployed).
	• Not all wallet types facilitate users' access to cryptographic signatures capabilities. • This affects BTC wallets in particular.	• Performing a micro deposit assumes that the customer's unhosted wallet is credited with funds. • When that is not the case, this type of verification cannot be performed.
		• Performing micro deposits may be economically inefficient due to the disproportionate network fees that may apply.
		• Manual micro deposits involve back and forth communication with the customer, demanding the compliance team to review transactions and manage their deadlines.
	• In UTXO-based wallets, a single deposit transaction might have more than one address from where the funds originate. • Thus, a CB could, in principle, need proof of ownership of all addresses on the input side, which would quickly become cumbersome and unexplainable to the user. • For CBs relying on cryptographically signed messages, the xPub key solves the problem by verifying several addresses at once, which is only available in AOPP, the automated message signing method.	• Unlike account-based blockchains (such as Ethereum), most UTXO-based wallets[19] do not provide users with the option to select a specific address from the available ones for a transaction. • This creates additional hindrances for customers proving ownership through Satoshi Tests, as they would need to inform the CB about which address to be whitelisted before the test.

19 Bitcoin, Cardano, and more.

About CryptoUK and The Travel Rule Working Group

About CryptoUK

CryptoUK is the leading trade body representing the digital asset sector in the UK, working directly with policymakers and market participants to develop balanced regulatory and governance policies in the UK and Europe.

We are the trusted voice of the UK's Web3 industry, championing the sector's growth and success, advocating for the industry in the public and private sectors, and the media.

Contact our team to learn more about our policy initiatives and member benefits.

The Travel Rule Working Group

CryptoUK would like to thank all members of the Travel Rule Working Group for the time and effort they have contributed to the creation of the Travel Rule Good Practices Guide.

Co-chairs

ELLIPTIC NOTA BENE

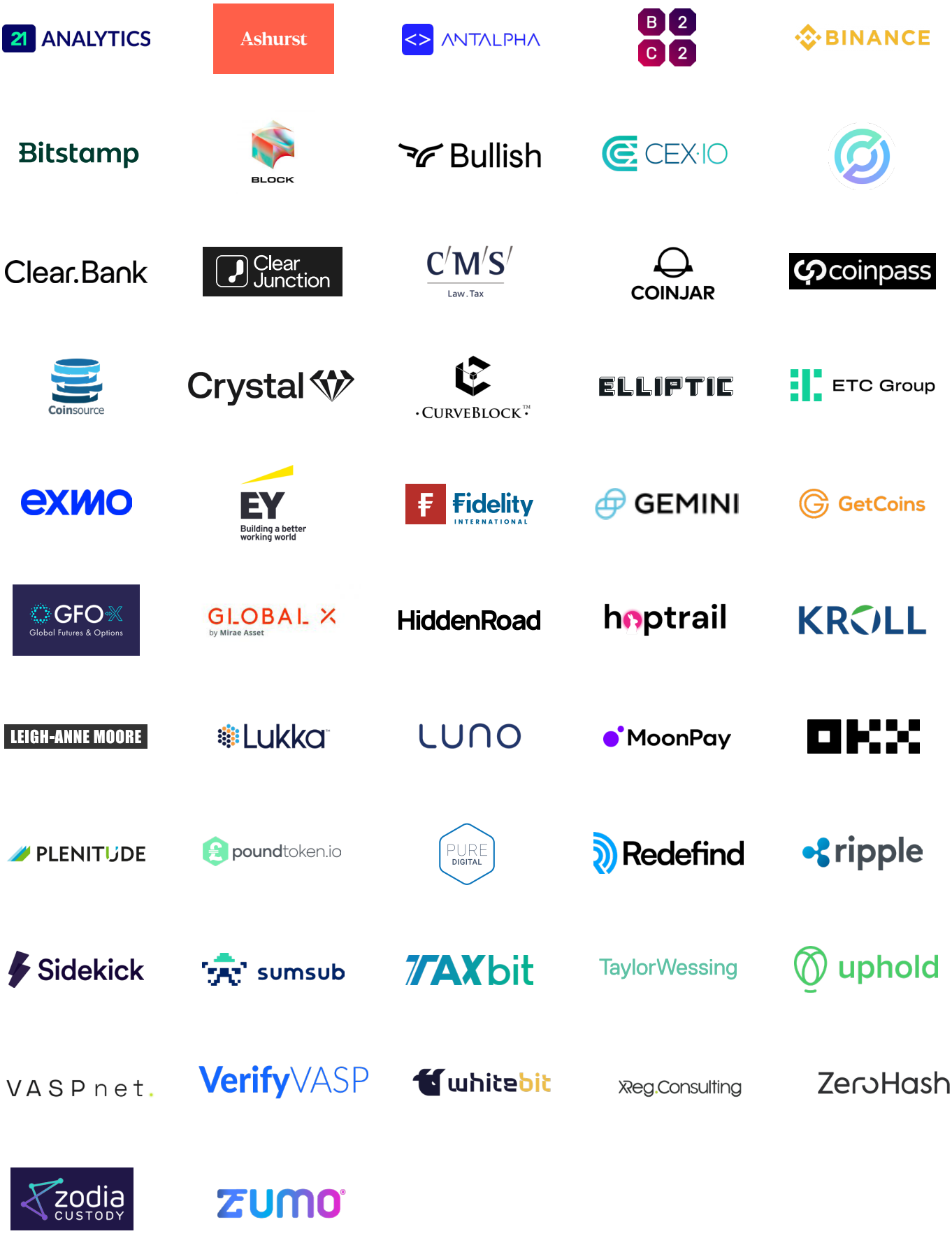
Sub-discussion Group Leads and Contributors

21 ANALYTICS Bitstamp CMS Law.Tax coinpass ELLIPTIC

GEMINI ICONOMI LUNO MoonPay NOTA BENE

PLENITUDE TaylorWessing VASPnet.

Working Group Participants



CryptoUK

Join us :
hello@cryptouk.io

Media enquiries :
media@cryptouk.io

Visit us :
cryptouk.io