Annex 22-I

Cryptoassets Transfers ('Travel Rule')

Note: Sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance, and with the guidance set out in Part II Sector 22.

Overview

This guidance relates to the provisions of The Money Laundering Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) that implement the Travel Rule for cryptoasset transfers in the UK.[1] All cryptoasset related provisions in the MLRs apply only to crypto exchange providers and custodian wallet providers as defined in the MLRs Reg 14A (cryptoasset businesses). Part 7A of the MLRs imposes requirements on cryptoasset businesses relating to the information they must send, receive and verify as part of a cryptoasset transfer (the 'Travel Rule').

The Travel Rule requires transfers of cryptoassets to be accompanied by certain identifiable information on the originator (person who owns and allows the transfer of the cryptoasset) and the beneficiary (intended recipient of the cryptoasset). Cryptoasset businesses must take all reasonable steps to ensure that they comply with the Travel Rule requirements.

The Travel Rule forms part of wider anti-money laundering obligations to have effective procedures in place to detect and prevent money laundering, terrorist financing and proliferation financing (ML/TF/PF). The guidance is intended to assist firms to design and implement the systems and controls necessary to mitigate the risks of the transfer of cryptoassets being used in connection with ML/TF/PF.

Meanings and definitions

1. The Travel Rule (TR) obligations apply to cryptoasset transfers irrespective of the purpose of the transfer and regardless of the value. The obligations therefore apply to all payments for goods or services made in cryptoassets, except when the cryptoasset transfer is already a "transfer of funds" within the meaning of Art 3.9 of the Funds Transfer Regulation (FTR)[2].

2. A cryptoasset business (CB) is either a cryptoasset exchange provider (CEP) or a custodian wallet provider (CWP). CEPs and CWPs are defined in Reg 14A of the MLRs, and the TR obligations apply to CEPs and CWPs that are carrying on business in the UK (see also Sector 22 paras 22.9-22.16).

3. An intermediary cryptoasset business is a CB that provides cryptoasset exchange or custodian wallet services to, or for, the CB of the originator or beneficiary, but does not have a business relationship with either the originator or the beneficiary. For example, if Firm A offers custodian wallet services to customers, and Firm A has a sub-custody contract with Firm B, which makes and receives cryptoasset transfers and manages cryptographic keys on behalf of Firm A, the TR rule will apply to both firms. Firm A must collect and supply Firm B with the required information, and Firm B must ensure that the information is received from Firm A and passed on with the transfer.

---

[1] The Money Laundering Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ('MLR's) Regulations 64A-H (Part 7A).

[2] EU Regulation 2015/847 was legislatively on shored wef 1/1/2020.

4. A cryptoasset transfer means an inter-cryptoasset business transfer or an unhosted wallet transfer.

5. An inter-cryptoasset business transfer is a transaction by two or more CBs, making available a cryptoasset of an originator to a beneficiary, where at least one of the CBs must be carrying on business in the UK. It includes instances where the originator and beneficiary are the same person (e.g. when the same person has accounts with different CBs).

6. An inter-cryptoasset business transfer does not include a cryptoasset transfer where both the originator and the beneficiary are a CB acting on its own behalf (i.e. TR information must only be sent if the CB is acting on behalf of a customer).

7. Transfers per Art. 3(9) of the FTR are excluded from TR requirements for cryptoassets.

8. Transfers of cryptoassets where both the originator and beneficiary hold accounts with the same cryptoasset business are not in scope, therefore there is no requirement to obtain or send information.

9. Transfers between wallets held with different legal entities within the same group are subject to normal TR requirements – there is no exemption for intra group transfers.

Sunrise issue

10. The Financial Action Task Force (FATF) has recognised that delays in implementation and different timelines for enforcement of the TR across jurisdictions results in what is referred to as the 'sunrise issue'. This may present challenges for CBs dealing with counterparties in jurisdictions where the TR has not yet been implemented. CBs should be aware of and take account of any FCA communications on this matter.[3]

Information accompanying an inter-cryptoasset business transfer

11. The CB of the originator must ensure the following information accompanies transfers:

- The name of the originator and the beneficiary;
- The registered name of the originator or beneficiary if they are a legal entity[4] (or trading name if no registered name);
- The account number of the originator and the beneficiary (or unique transaction identifier if there is no account number). Account numbers should be and remain unique to a customer.

12. Where all CBs executing the transfers (including intermediaries) are carrying on business in the UK, the CB of the beneficiary may also request the following information which the CB of the originator must also provide within 3 working days:

(i) If the originator is a legal entity:
- Customer identification number; or

[3] See for example https://www.fca.org.uk/news/statements/fca-sets-out-expectations-uk-cryptoasset-businesses-complying-travel-rule.
[4] Where there is a relevant Legal Entity Identifier (LEI) use thereof as additional information for legal entities may be helpful.

- Address of originator's registered office (or principal place of business if none or different)

(ii) If the originator is an individual, one of the following:

- Customer identification number; or
- Address; or
- Birth certificate number, passport number or national identity card number (or individual's date and place of birth).

13. The CB of the originator must also ensure that this additional information in para 12 above accompanies transfers where at least one CB is not carrying on business in the UK (i.e. the other CB) and the transfer value (single or linked) is €1,000 or more.

14. Recipient CBs should ensure that they have taken all reasonable steps to determine the jurisdiction of the originator CBs, especially where the CB may have group entities trading under similar names in other or multiple jurisdictions (see para 41 below).

15. CBs should ensure that they have appropriate record keeping and retrieval processes to ensure the timely response to any additional requests for information.

16. All information relating to the originator must have been verified by the CB of the originator on the basis of documents or information obtained from a reliable source, independent of the person whose identity is being verified (see Part I para 5.3.181).

17. The provision of the required information must occur before or at the moment the transaction is completed. The transaction is completed when the recipient CB credits (or otherwise makes available) the cryptoassets to the beneficiary. Where the transfer is to a jurisdiction with higher requirements than those required in terms of the TR, a CB complies with its TR obligations by providing the information as required (as appropriate per paras 11, 12 and 13).

18. 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 CDD, if it does not unduly impact time required to complete the transaction, is in line with its procedures, and in keeping with a risk-based approach.

19. Technological solutions and vendors may be used by CBs to assist in achieving compliance with the TR, but the CB remains liable and retains the ultimate responsibility for its obligations in terms of the MLRs (see also Part I para 2.18). CBs may wish to consider various factors when deciding to use such solutions, including for example, data privacy, security, and interoperability.

Batch file transfers

20. Where the CB of the beneficiary is carrying on business wholly outside the UK (ie. it is not in scope of the MLRs Regs 8 and 9) information on the batch must be submitted securely and simultaneously with the transfer. A batch file transfer is a bundle of individual inter-cryptoasset business transfers from a single originator. The TR applies to each of the underlying transfers forming the bundle. The information must be verified by the CB of the originator on the basis of reliability and independence.

Missing and inaccurate information

21. When a CB receives a cryptoasset as part of an inter-cryptoasset business transfer, it must check that it has received the required information and that the information on the beneficiary matches its previously verified CDD, before making the cryptoasset available to the beneficiary.

22. CBs must ensure that they have appropriate and effective procedures to detect missing or inaccurate information, and to respond accordingly.

23. Where it cannot be ascertained whether information requirements have been complied with (such as with wallet attribution), the CB of the beneficiary may take note of paragraphs 39-43.

24. When there is missing or inaccurate information, the CB of the beneficiary must, when appropriate, request the missing information (regardless of whether the CB of the originator is subject to higher value thresholds in its jurisdiction), and consider making enquiries as to any discrepancies from any relevant parties to the transaction. The nature of discrepancies may be assessed on a risk-based approach as there may be a reasonable justification provided for the discrepancy (e.g. a truncated name exceeding character space would not require further enquiries). CBs should consider notifying the CB of the originator in the event of material discrepancies.

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).

26. These considerations will be determined by CBs with regard to their risk assessments, taking into account the ML/TF/PF risks that they have determined are posed by the customer. This determination will be within a requirement of proportionality and reasonableness, and will take note of any reasonable justification provided for the discrepancy. See further Part I Chapter 4 and Sector 22.

27. In particular firms will have regard to:

- The purpose and nature of its business relationship with the beneficiary and of the transfer;
- The value of the transfer and any linked transactions;
- The frequency of the transfers;
- The duration of its business relationship with the beneficiary; and
- Whether the TR has been implemented in the jurisdiction of the counterparty CB.

28. CBs should document steps taken to deal with failures to provide the required information, and establish a clear process of escalation, including, for example, issuing warnings and deadlines for compliance by the CB of the originator.

29. Firms must report repeated failures by a CB to provide the required information to the FCA. A risk-based approach may be used to determine what constitutes a repeated failure. This would take into account, for example, the volume and size of transactions over a period of time, or a percentage of transaction failures from a particular CB. The reporting requirement applies regardless of the CB of the originator's own jurisdictional obligations. Firms should document steps taken along with their reasonings.

Intermediaries

30. An intermediary CB must check whether all information required (see paras 11 and 12) has been received before transferring the cryptoasset. When it becomes aware of missing information it must request the information from the CB it received the transfer from. It must also consider whether to delay the onward transfer until the information is received or return the cryptoasset to the CB from which it was received. Firms must have regard to the relevant risk assessments and levels of risk as per paragraphs 26-27 above.

31. An intermediary CB must ensure that all information provided in relation to a transfer, including any requested before the transfer is made, accompanies the onward transfer, and that it sends on requested information which is received after it has transferred the cryptoasset as soon as is practicable.

Returning a transfer

32. Where the CB (intermediary or of the beneficiary) has decided to return the cryptoasset, it 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.

33. Where a CB or intermediary returns a cryptoasset to the originator (as set out above), this is not a cryptoasset transfer for the purposes of the travel rule. See Sector 22 paragraphs 22.65-22.71 regarding suspicious transactions and Part I Chapter 6.

Unhosted wallet transfers

34. CBs should adopt a risk-based approach when dealing with unhosted wallet transfers. They should obtain further information on the unhosted wallet where they have determined, by means of their risk assessments, that there is a higher risk of ML/TF/PF.

35. In assessing the level of risk arising from an unhosted wallet transfer, the firm must take into account:

- The purpose and nature of the business relationship with its customer and the unhosted wallet transfer;
- The value of the transfer and any linked transfer;
- The frequency of transfers made by or to the customer;
- The duration of the business relationship with the customer.

36. Where a CB has determined that information should be requested, it should take reasonable steps to obtain the information from its own customer. In higher risk cases, firms should consider taking further steps to ascertain the source of funds in the unhosted wallet and thereafter consider authorising the transfer only if the control over the unhosted wallet can be reasonably established through appropriate solutions (e.g. micro deposit or cryptographic signature).

37. Where a firm has determined that information should be requested and it is not provided, it must not make the unhosted wallet transfer nor make the cryptoasset available to the beneficiary.

38. A firm must still submit a Suspicious Activity Report (SAR) where appropriate (see Sector 22 paragraphs 22.22, 22.65-22.69 and Part I Chapter 6).

Wallet attribution

39. CBs should adopt a risk-based approach in attributing wallets. All reasonable steps should be taken to identify the counterparty and whether a wallet is hosted or unhosted. Steps taken should also be proportionate to the size and nature of the business and could include, but are not limited to, the following:

- Blockchain analysis where appropriate (see para 40);
- Query the wallet address using discoverability methods provided by the TR solution being used by the CB;
- Consult the CB's own address book;
- Obtain information on the wallet status and/or identity of the CB from the beneficiary.

All steps taken should be documented.

40. Blockchain analysis and other similar means may be useful in examining the transaction history, risk, volume and other characteristics of the wallet. Where no relevant information is identified or provided by this assessment, firms should adopt a risk-based approach in determining how to proceed further.

41. 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.

42. Where it is not known whether the counterparty is an intermediary CB or the CB of the originator/beneficiary, a CB may presume the latter, and must comply with any requests for further information that it receives.

43. CBs should consider rescreening wallets as part of their ongoing and wider compliance systems and controls. When the wallet attribution differs from its initial identification, CBs should consider requesting information from the counterparty CB or from their own customer. Suspicious transactions must be reported as required (see para 38).

Linked transactions

44. Linked transactions are generally transactions from the same originator to the same beneficiary that have been broken down into smaller, separate transactions over a short period of time. Firms must have policies, controls and procedures in place to detect potentially linked transactions. See Part I paragraph 5.3.7.

Transaction values

45. When assessing whether a transfer is equal to or exceeds €1,000, CBs should take the value recorded at the time the transfer is initiated by the originator and converted into Euros.

46. A standardised approach to valuing a transaction using market reference data may be used. Where a Euro trading pair does not exist with the cryptoasset, CBs may calculate the value of the transfer by undertaking a currency conversion to Euros with trading pairs that do exist.

Layer-2 solutions

47. When a cryptoasset transfer is made using a Layer-2 solution (e.g. the Lightning Network (LN)) and it meets the definition of an inter- cryptoasset business transfer or unhosted wallet transfer, it is in scope of the TR, including where the transfer is conducted off-chain.

48. Those parts of a LN transfer that are intermediate to originator and beneficiary are not in scope of the TR even where one or both nodes in the channel are CBs.

Data protection

49. A CB should note its obligations in terms of the MLRs (Reg 41) and the Data Protection Act 2018.