

## Feature

### KEY POINTS

- In the UK, HM Treasury is beginning to plan for the implementation of the Financial Action Task Force (FATF) recommendation that transfers of cryptoassets are accompanied with identifiable information on the originator and the beneficiary (the Travel Rule).
- The Travel Rule was originally designed for wire transfers. The extension of the existing regime to transfers of cryptoassets which use pseudonymous wallets is not straightforward.
- The Travel Rule creates significant practical compliance challenges for cryptoasset exchanges and custodian wallet providers, particularly as the information required to complete a transfer of cryptoassets is insufficient to comply with the Travel Rule.

Authors Meera Ragha and Diego Ballon Ossio

# Unravelling the Travel Rule: AML requirements for cryptoasset businesses

The Financial Action Task Force (FATF) recently updated its guidance for Virtual Assets and Virtual Asset Service Providers (VASPs) in October 2021 including on its Recommendation 16 that certain transfers of cryptoassets must be accompanied with identifiable originator and beneficiary information. The application of Recommendation 16 to VASPs has caused controversy, as it is regarded as being very difficult to comply with by the industry.

This article explores whether the proposed implementation of the Travel Rule in the UK addresses any of the commonly cited practical difficulties with compliance (which are particularly pronounced for unregulated firms or start-ups that may be unaccustomed to being scrutinised in this way) in light of the most recent guidance.

### ORIGINS OF THE TRAVEL RULE

The Travel Rule has its origins in wire transfers. Extending this requirement to transfers of cryptoassets raises difficult compliance obstacles. This is due to the fundamental differences between transfers of fiat currency through traditional financial institutions, and transfers of cryptoassets on a DLT platform using pseudonymous wallets.

In 2012, the FATF adopted Recommendation 16, that transfers of funds must be accompanied by certain identifiable information on the payer and payee. In the context of wire transfers, the Travel Rule has already been widely adopted, including in the UK through Regulation (EU) 2015/847 as applicable by virtue of the European Union (Withdrawal) Act 2018, the “UK Wire Transfer Regulations”. This specifies the information on the payee or payer to be included in a payment message, and the circumstances in which a payment service provider is required to verify that information.

### HOW WILL THE TRAVEL RULE WORK IN THE UK FOR TRANSFERS OF CRYPTOASSETS?

In its consultation paper dated July 2021, HM Treasury has stated that the time is now for the UK to begin planning for the implementation

of the FATF recommendation on extending the scope of the Travel Rule so that transfers of cryptoassets are accompanied with identifiable information on the originator and the beneficiary of each transfer.

This is intended to apply to: (i) cryptoasset exchange providers (including cryptoasset ATMs, peer to peer providers, issuers of new cryptoassets); and (ii) custodian wallet providers (which includes safeguarding and administering cryptoassets and/or the private cryptographic keys on behalf of customers), that are carrying on business in the UK (together, “Cryptoasset Service Providers”).

In the UK, the proposed approach is to replicate the requirements under the UK Wire Transfer Regulation for the cryptoasset sector, insofar as is possible. However, HM Treasury notes that it would not be appropriate to simply extend the regime in the UK Wire Transfer Regulation, and so it proposed to modify the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017).

At its core, Cryptoasset Service Providers will need to implement effective systems for providing certain information on the originator and beneficiary as part of transfer of cryptoassets and detecting whether the requisite information on the originator and beneficiary is missing.

### What information must accompany transfers of cryptoassets?

In line with the position under the UK Wire Transfer Regulations, the information that must accompany a transfer will depend on its value, and whether all Cryptoasset Service Providers involved in the transfer are carrying on business in the UK.

Transfers below a *de minimis* threshold (which is expected to be £1,000) only require limited beneficiary and originator information to be sent with a transfer. Where there are multiple transfers from a single originator that appear to be linked and which, taken together, exceed the threshold, then the transfer will need to be accompanied by full beneficiary and originator information.

The HM Treasury consultation proposes that the information set out in Table 1 opposite should accompany a transfer of cryptoassets.

### SOME PRACTICAL CHALLENGES WITH THE PROPOSAL

The information required to complete a transfer of cryptoassets on a DLT platform is insufficient to comply with the Travel Rule. By definition, cryptoassets are transferred on a blockchain or DLT platform and rely on the use of cryptographic keys. The only information required to complete a transfer of cryptoassets on a DLT platform is: (i) the private cryptographic key, which is required to verify the transfer from the sender’s wallet; and (ii) the wallet address of the recipient. The pseudonymous nature of wallet addresses means that it is not possible to identify: (i) the operator of the wallet; (ii) the beneficial owner of the assets in the relevant wallet; or (iii) where the operator of the recipient’s wallet is located.

This generates a fundamental problem for Cryptoasset Service Providers when designing

**Biog box**

Meera Ragma is a senior associate at Clifford Chance LLP, where she advises on UK and EU financial regulation and compliance. Meera specialises in acting for payment institutions, e-money issuers, banks and technology companies on a range of payments and fintech regulation. Meera is the co-author of the *Chambers Global Practice Guide to Fintech 2021 UK: Law and Practice*. Email: [meera.ragma@cliffordchance.com](mailto:meera.ragma@cliffordchance.com)

**TABLE 1: INFORMATION TO ACCOMPANY A TRANSFER OF CRYPTOASSETS**

	INFORMATION ON ORIGINATOR	INFORMATION ON BENEFICIARY
Transfers above the <i>de minimis</i> threshold	<ul style="list-style-type: none"> <li>■ Name</li> <li>■ Address</li> <li>■ Account number or unique transaction identifier</li> <li>■ Personal document number</li> <li>■ Customer identification number or date and place of birth.</li> </ul>	<ul style="list-style-type: none"> <li>■ Name</li> <li>■ Account number/unique transaction identifier</li> </ul>
Transfers below the <i>de minimis</i> threshold	<ul style="list-style-type: none"> <li>■ Name</li> <li>■ Account number/unique transaction identifier</li> </ul>	<ul style="list-style-type: none"> <li>■ Name</li> <li>■ Account number/unique transaction identifier</li> </ul>
If all cryptoasset service providers involved in the transaction are UK-based	<ul style="list-style-type: none"> <li>■ Account number/unique transaction identifier (subject to requirement to provide full information to beneficiary cryptoasset service provider on request)</li> </ul>	<ul style="list-style-type: none"> <li>■ Account number/unique transaction identifier</li> </ul>

their compliance framework in response to the Travel Rule. Cryptoasset Service Providers are unable to identify from the wallet address whether a counterparty to the cryptoasset transfer is an individual or another Cryptoasset Service Provider, and it is not possible to identify the location of the sender's wallet. This challenge is compounded by the fact that the originator of the transaction (likely the Cryptoasset Service Provider's client) may not have this information.

### Peer-to-peer transfers of cryptoassets

As noted, there are crucial differences between wire transfers and cryptoasset transfers, which means some transfers of cryptoassets will not be subject to the Travel Rule. Unlike wire transfers, which take place through systems accessible exclusively to financial institutions, transfers of cryptoassets can occur not just through crypto exchanges but also through other channels, including peer-to-peer transfers.

The HM Treasury consultation notes that any individual can host their own crypto wallet (which are known as “unhosted wallets”) to make and receive transfers. It is envisaged that the Travel Rule will apply only to Cryptoasset

Service Providers, not to private individuals using such unhosted wallets. Consequently, peer-to-peer transfers of cryptoassets are outside the scope of these new rules. This is intentional – the FATF recommendations expressly state that individuals are not required to comply with the Travel Rule. The recent FATF guidance provides that where a VASP transfers cryptoassets to an unhosted wallet, it should obtain the information directly from its client. This is an interesting approach given that transfers to unhosted wallets pose a heightened risk of money laundering.

There are practical difficulties for Cryptoasset Service Providers trying to determine which accompanying information should be provided, as there is no reliable way to identify whether the recipient is: (i) another provider or an individual; and (ii) located within or outside the UK. Even if the client is able to supply such information, it may not be reliable.

HM Treasury states that there is nothing to prevent a Cryptoasset Service Provider providing additional information with the transfer (such as providing the full beneficiary and originator information in circumstances where the sending Cryptoasset Service Provider does not know where the recipient is based). It is unclear whether HM Treasury has

considered the data privacy implications of such “overcompliance”, particularly in light of the fact that HM Treasury confirms that personal data received, transmitted or retained for the purposes of complying with these rules is within the scope of the UK General Data Protection Regulation (see below).

### Practical challenges of calculating the value of transfers in GBP

An additional compliance challenge has been identified by HM Treasury. As there is a *de minimis* threshold for transactions, Cryptoasset Service Providers must determine the method for calculating the value in GBP of transfers of cryptoassets. HM Treasury has acknowledged that the volatility of cryptocurrencies and illiquidity in the crypto-to-fiat exchange market mean that exchange rates can vary across the market, and HM Treasury does not propose to legislate as to how a firm is to calculate the value of a transfer; rather, the consultation has stated that firms must use a “reasonable and justifiable” approach.

In this context, HM Treasury also proposes to apply the linked transactions rule by which the Cryptoasset Service Provider must consider whether transactions are linked, and, if the combined value of the linked transactions exceeds £1,000, they must be treated as a single transaction. Given the ease by which wallets can be created and the tendency of market participants to operate multiple wallets, it may prove difficult to establish when transfers are linked.

### Missing information and sanctions screening

Unlike in the context of wire transfers, it is not possible to reject cryptoassets transactions which are made without or with unverifiable underlying information. As such, HM Treasury proposed that cryptoassets should not be made available to the beneficiary instead. The FATF guidance sets out some proposed mechanisms to achieve this, although these may be difficult to implement in practice, and would erode one of the key attractions of cryptoasset transfers, namely that such transfers are intended to be immutable.

The FATF guidance provides that sanctions screening should take place when conducting transfers of cryptoassets, which raises a

## Feature

### Biog box

Diego Ballon Ossio is a senior associate at Clifford Chance LLP, advising financial institutions and other market participants on financial market regulation and activities related to benchmarks, financial services trading and conduct requirements as well as payment services and fintech with a particular focus on cryptoassets, DLT and blockchain development. Diego gained significant experience working at the UK Financial Conduct Authority (and predecessor organisation) from 2010 to 2015. He was ranked as a “rising star” by Legal 500 for two years running. Email: [diego.ballonossio@cliffordchance.com](mailto:diego.ballonossio@cliffordchance.com)

similar issue (as cryptoassets transfers cannot be rejected if the sanctions screening has not been completed). The FATF guidance includes some examples of controls that could be implemented to address this, such as putting a wallet on hold until the relevant sanctions screening is completed, or receiving cryptoassets into a provider’s wallet that links to a customer’s wallet, and moving the transferred cryptoassets to the customer’s wallet only after the screening is completed. This would have severe ramifications for the crypto industry, as it would slow down the process for transferring cryptoassets.

It remains to be seen how these requirements would play out in real life and impact the market. There may be interesting contractual ramifications as the contractual obligation to pay for or deliver a particular cryptoasset is unlikely to be discharged until such time as the relevant Cryptoasset Service Provider makes the cryptoassets available to the recipient (not at the moment of transfer).

### Data privacy requirements

As mentioned, one of the key features of cryptoassets has been the ability to transact pseudonymously. This may be impacted by the proposed requirements, as Cryptoasset Service Providers will be required to collect, store and potentially share personal information.

Additionally, the implementation of these rules creates a centralised repository of beneficiary and originator information, which must be stored for five years, which raises data privacy concerns. The HM Treasury consultation states that personal data received, transmitted or retained for the purposes of complying with these rules is within the scope of the UK General Data Protection Regulation, and Cryptoasset Service Providers will therefore need to process it in line with the requirements of that legislation.

### ARE THERE ANY SOLUTIONS?

#### Industry-wide messaging standards are being developed

The Travel Rule was originally designed for traditional financial institutions (eg banks), and it took over a decade for this rule to be properly implemented through the development of an

industry-wide messaging standard (ie SWIFT).

In the UK, HM Treasury has stated that it has deferred bringing this rule into effect until now, but it has noted the recent technological developments that may facilitate compliance with the Travel Rule for cryptoassets.

The FATF guidance clarifies that it is not necessary for the relevant information to be attached directly to the transfer of cryptoassets on the blockchain or DLT platform itself. Instead, the information can be provided indirectly or alongside the actual blockchain transaction, using a standardised messaging system.

Not all jurisdictions will have implemented the FATF standards in the same way and to the same degree. Although the FATF has urged national regulators to engage with the private sector to develop potential solutions to facilitate compliance with the Travel Rule, in practice the FATF leaves the issue to the industry, stating that providers will have to conduct due diligence. There are also multiple private sector organisations proposing different solutions. For example, a joint working group between the Chamber of Digital Commerce, Global Digital Finance and the International Digital Asset Exchange Association has developed the InterVASP Messaging Standard Overview to provide a universal common language for the communication of required originator and beneficiary information.

While possible, it seems highly unlikely that there will be consensus in the industry on a common set of messaging standards for cryptoasset transfers. We expect that any industry messaging standards will need to be refined and developed to enable compliance with the rules that are being developed in the UK and internationally.

#### HOW WILL THE TRAVEL RULE AFFECT CRYPTOASSET SERVICE PROVIDERS THAT ARE ALREADY STRUGGLING TO COMPLY WITH THE EXISTING AML RULES?

Based on public records, many Cryptoasset Service Providers that have applied for registration under the MLR 2017 have not sufficiently demonstrated that their AML systems and controls are adequate for registration. This is underlined by the fact

that the deadline for firms operating under a temporary registration regime to obtain registration has twice been extended and is now set at 31 March 2022 as “a significantly high number” of businesses could not meet the required standards. This is likely to be due to the FCA applying high standards when assessing the AML systems and controls of Cryptoasset Service Providers.

The introduction of the Travel Rule is likely to increase the challenges that Cryptoasset Service Providers are facing in complying with AML requirements. Whilst the proposal is to implement the Travel Rule in a proportionate way (striking a balance between reducing the harms of illicit finance and supporting innovation), it remains to be seen how such proportionate implementation would operate. In any case, it is likely there will be significant compliance costs in building systems that would allow transmission of data accurately, securely and in a timely manner. This could have significant impact on the industry and customers.

The success of applying the Travel Rule to the crypto industry will largely depend on its homogenous application on a global scale. The FATF guidance has acknowledged the issues that arise due to governments not implementing the Travel Rule simultaneously. In particular, it can be a challenge for a Cryptoasset Service Provider when deciding what approach it should take in dealing with similar service providers located in jurisdictions where the Travel Rule is not yet in force. Further, to the extent that implementation is softer in certain jurisdictions, this may drive providers to these alternative locations in order to avoid having to comply with specific UK requirements.

The release of the updated FATF guidance increases the urgency for national regulators to implement the Travel Rule. Nonetheless, the FATF guidance also provides that regulators may wish to take a staged approach to enforcing the Travel Rule requirements. However, HM Treasury’s consultation in the UK is broadly aligned with the most recent guidance. It remains to be seen whether additional changes to the legislation will be made to address some differences. ■