RegCORE Client Alert

Financial Services: EU agrees new financial crime tracing and prevention rules for cryptoassets

July 2022

Financial Services

EU agrees new financial crime tracing and prevention rules for cryptoassets

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas
@pwc.com

Contact RegCORE Team
de_regcore@pwc.com

QuickTake

The EU has agreed that the so-called "travel rule", which already exists for fiat and electronic money i.e., "**traditional money transfers**" and EU and European Economic Area "payment services providers" (as such term is defined in EU legislation), will be extended to cover "transfers of cryptoassets".

In summary, the travel rule requires that information on the source of the asset and its beneficiary travels with the transaction and is stored on both sides of the transfer. Under the proposed EU reforms, this would mean that cryptoasset service providers (**CASPs**) will be obliged to provide this information to (national) competent authorities if an anti-money laundering (**AML**) and countering terrorist financing (**CTF**) investigation is started by such authorities. There are currently only two exceptions namely (1) for person-to-person transfers transacted without using a CASP and (2) or when both originator and beneficiary are CASPs acting on their own behalf. Another exclusion (as a national option and discretion) is made available for Member States to exempt these new rules to transfer of cryptoassets where the transaction is "exclusively" for the provision of goods or services where certain conditions are met. This follows the existing exemption in this area for traditional money transfers.

While this most recent announcement is certainly welcome in terms of harmonising national[1] AML/CTF rules and supervisory expectations in this area with a pan-EU regime, it will require CASPs but, equally payment services providers i.e., thus regulated financial institutions but not necessarily all non-financial services regulated entities that are nevertheless "obliged entities" for purposes of AML/CTF legislation to consider how they will meet compliance with the travel rule's obligations and supervisory expectations of competent

[1] Notably the efforts of various EU Member States such as Germany, Lithuania, Malta and France who have developed their own individual national rules and legislation mandating some form of a travel rule ahead of EU legislative reform efforts.

authorities. This Client Alert assesses this most recent development including in the context of the EU's wider forms part of wider-reaching efforts to reform existing financial crime rules applicable across the EU.

Rolling out the travel rule

The international AML standard setting body, the Financial Action Task Force (**FATF**) in 2019 first put forward its own recommendations to competent authorities (including those in the EU) on how to regulate what it terms "virtual assets" i.e., what in the EU are broadly captured as cryptoassets. FATF also introduced the concept of the travel rule. In order for FATF recommendations to be implemented in a manner to have the force of law, they need to be adopted in FATF member jurisdictions. On 20 May 2022 the G7 jurisdictions published a statement[2] confirming their intention to hold cryptoassets to the same standard as the rest of the (regulated) financial system and thus to introduce the travel rule in the legislative and regulatory frameworks in those jurisdictions.

On 20 July 2021, the European Commission published a package of legislative proposals setting out further AML/CTF legislative and institutional reforms (collectively the **AML Package**).[3] On 29 June 2022, the European Parliament announced that it had reached an agreement on amendments to the EU's AML/CTF rules to stop illicit flows and financial crime across the EU.[4] Together with its co-legislators, the European Commission and the European Council, final proposed amendments[5] to Regulation 2015/847[6] (commonly referred to as the "Funds or Wire Transfer Regulation" – **WTR**) were communicated. [7]

Specifically, this includes extending the original scope of the WTR to CASPs, thus bringing the "transfer of cryptoassets"[8] including those conducted via crypto-ATMs under the travel rule.[9] The main goal of the EU's proposed amendments to the WTR is to introduce an outcome that ensures that cryptoasset transfers, e.g., with bitcoin or e-money tokens, can be traced in the same manner as traditional money transfers and can also be blocked in case of suspicious transfers.

The proposed amendments apply to CASPs whenever their transactions, whether in fiat currency or a cryptoasset, involve a traditional wire transfer or a transfer of cryptoassets involving a CASP. As discussed below, two exceptions apply for (1) for "person-to-person transfers"[10] transacted without using a CASP and (2) or when both originator and beneficiary are CASPs acting on their own behalf. Another exclusion (as a national option and discretion) is made available for Member States to exempt these new rules to transfer of cryptoassets where the transaction is "exclusively" for the provision of goods or services where certain conditions are met. This follows the existing exemption in this area for traditional money transfers.

The final amendment to the WTR has not been published as of the date of this Client Alert. Nevertheless, the impact of these amendments may require careful preparatory planning by require CASPs but the more broader range of regulated financial institutions and those that are "obliged entities" for purposes of AML/CTF legislation to consider how they will meet compliance with the travel rule's obligations and supervisory expectations of competent authorities. The WTR amendments should be read in light of the AML Package's overall aims but equally in line with the forthcoming implementation of the EU's proposed Markets in Cryptoassets Regulation (**MiCA**) not least because the recast WTR borrows the definition of CASP from MiCA.

It is also equally important to note that a number of proposals discussed in the context of amending the WTR, specifically those from the European Parliament, were not introduced in the present final reforms to the WTR

---

[2] Available here.
[3] Press release available here.
[4] Press release available here and from the European Council available here.
[5] Formally this is done by "recasting" the existing legislation. Further information on this process is available here.
[6] Regulation (EU) 2015/847 on information accompanying transfers of funds, available here and as last amended here.
[7] Proposal available here.
[8] The publicly available text of the WTR defines this as "…any transaction at least partially carried out by electronic means on behalf of an originator through a crypto-asset service provider, with a view to making crypto-assets available to a beneficiary through a crypto-asset service provider, irrespective of whether the originator and the beneficiary are the same person and irrespective of whether the crypto-asset service provider of the originator and that of the beneficiary are one and the same."
[9] See amendment on page 54 available here.
[10] The publicly available text of the WTR defines this as "…a transaction between natural persons acting, as consumers, for purposes other than trade, business or profession, without the use or involvement of a crypto-asset service provider or other obliged entity;"

but these that have nevertheless have been earmarked to be included in the EU's reform efforts in other legislative instruments, including in the context of MiCA and/or the AML Package.

A recap on the travel rule's application to cryptoassets and the introduction of new know your customer (KYC) requirements

Under the recast WTR, CASPs and payment services providers[11] i.e., regulated financial services firms will be required to ensure that all cryptoasset transfers are accompanied by the following information:

- For the originator CASP: the originator's name, account number (where relevant), wallet address, official personal document number (such as ID card and/or passport), customer identification number or date and place of birth; and
- For the beneficiary CASP: the beneficiary's name, account number (where relevant).

Some simplifications to these new data capture and data sharing requirements may be available under the existing form of the WTR, notably in its "Recitals".[12] One such simplification relates to the type and breadth of information that must be collected and exchanged[13] for those transfers of funds within the EU. These include, as opposed to the above, the need to collect and exchange "only" the (a) the payment account number(s) or a unique transaction identifier, or (b) in the case that the transfer of funds not tied to an unhosted wallet (see observations below), the originator and beneficiary address identifiers. Importantly however, the recast WTR does not contain a simplified regime for domestic wire transfers in EU Member States. As a result, all cryptoasset transfers will be treated as cross-border transactions within the EU.

Additional requirements apply when transferring cryptoassets from the EU to outside of the EU. Transfers of cryptoassets from the EU to outside the EU therefore should include a Legal Entity Identifier (LEI).

Consequently, regardless of whether needing to provide either (i) simplified or (ii) full information related to a cryptoasset transaction, CASPs and payment services providers will each need to verify the accuracy of such information as such has been provided by their own customers. This in turn may mean that a number of KYC processes, whether during onboarding and/or throughout the lifecycle of the customer relationship, may need to have to be strengthened.

Before finalising a transaction and making the relevant cryptoassets available to the receiving party, CASPs will have to verify that the source of the asset is not subject to restrictive measures or sanctions, and that there is no risk of money laundering or terrorism financing. This requirement ties into the broader overarching obligations applicable to CASPs to implement and maintain effective procedures to detect suspicious cryptoassets, in particular those suspected of being linked to illegal activities (such as fraud, extortion, ransomware or darknet marketplaces) and/or those that have passed through mixers, tumblers or other anonymising services. This is especially important for transfers involving unhosted wallets or non-EU CASPs that do not comply with the EU's standards on the travel rule.

It should be noted that a number of CASPs have already begun to undertake efforts to introduce similar measures to enhance AML risk identification, mitigation and management measures as well as more robust KYC procedures. While welcome, certain problems are likely to arise where an EU-domiciled CASP (or indeed any other regulated financial services provider), complying with the recast WTR obligations and the travel rule, is dealing with a non-EU domiciled counterparty (including non-EU unhosted wallets) that is not required to collect such (comparable) information thus yielding a mismatch on who needs to comply with what and equally the question whether they can.

Unless such mismatch is resolved, this might mean that a transaction is held up until a full AML/KYC or other due diligence exercise is completed. While this is of course nothing new in traditional financial transactions, the extent of change and compliance burden for cryptoasset market participants may cause barriers in smooth

---

[11] See Art. 1(1) of the revised Payment Services Directive (available here).

[12] In summary, a "Recital" in EU legislative instruments sets out the reasons for its operative provisions and should (in theory) avoid normative language and political argumentation. In recent years the Recitals have been used to further add guidance and context to the individual requirements set out in the Articles of the legislative instrument and many often do read as equivalent to rules themselves.

[13] Article 5(2) of the WTR allows for the payment service provider of the payer to, within three working days of receiving a request for information from the payment service provider of the payee or from the intermediary payment service provider, make available the following: (a) for transfers of funds exceeding EUR 1,000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked, the information on the payer or the payee in accordance with Article 4 WTR; (b) for transfers of funds not exceeding EUR 1,000 that do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed EUR 1,000, at least: (i) the names of the payer and of the payee; and (ii) the payment account numbers of the payer and of the payee or, where Article 4(3) of the WTR applies, the unique transaction identifier.

blockchain settlement (at least from a legal perspective) and liability for involved parties. Importantly, the wording of the recast WTR also introduces an obligation that "verifying the ownership of unhosted wallets should not cause an unduly delay the execution of intended transfers." Regrettably, there are at present, no established industry-wide set of data sharing standards and frameworks to capture, share and safeguard information needed under the travel rule that may fully respect all relevant data protection and privacy legislation.[14]

No minimum thresholds in the final version of the travel rule applicable to cryptoassets

In the past, EU legislators have observed that cryptoasset transactions often bypass certain thresholds that would have, certainly in comparable traditional money transfers, triggered tracing measures under the WTR. The European Commission had originally proposed that the travel rules' extension to cryptoassets would have followed the FATF recommendation – namely in applying it to those occasional transactions worth more than EUR 1,000.

The European Parliament along with the European Council proposed that no such minimum transfer threshold should apply. As a result, in the EU the travel rule applies to all cryptoasset transactions, thus introducing a much higher compliance burden. The EUR 1,000 threshold is however still of relevance to transactions involving unhosted wallets, as discussed below.

The trouble with unhosted wallets

Applying the travel rule gets complicated in the case of "unhosted wallets" when transactions interact with cryptoasset wallets that are administered i.e. hosted by CASPs. In other words, unhosted wallets (also referred to as "non-custodial wallets" or "self-custodied wallets")[15] are cryptoasset wallets which are held directly by their owners without using a CASP. They are generally subject to no to low KYC or customer due diligence requirements as they are software held by the customer as opposed to the CASP.

Specifically, the revisions to the WTR concerning unhosted wallets state that: "In case a customer sends or receives more than EUR 1,000 to or from their own unhosted wallet, the CASP will need to verify whether the unhosted wallet is effectively owned or controlled by that customer." In addition to verification, the recipient CASP will need to inform competent AML authorities of any transfer made to or from an unhosted wallet that is over EUR 1,000. This is a much lower threshold when compared to the EU's EUR 10,000 notification threshold for traditional money transfers and remittances.

Problems in practical compliance may arise when applying this aspect of the travel rule as it requires that the CASPs, at the receiving end of a transaction, will still need to verify the ownership and/or control of that unhosted wallet – which given the very nature of unhosted wallets (previously) being largely exempt from KYC or other customer due diligence requirements may make this difficult to verify and thus a barrier to the use of unhosted wallets more generally. Some CASPs may, in wanting to stay compliant with their obligations, choose to block transactions with unhosted wallets altogether. Some EU policymakers may not be sorry about that consequence given the overall stigma unhosted wallets have received from certain supervisory authorities and policymakers around the globe on grounds of their anonymity and susceptibility for use in furtherance of financial crime.

Lastly, the transfer information requirements under the recast WTR will not apply to person-to-person transfers conducted without a provider, such as what the various EU press release announcements referred to as "bitcoin trading platforms or among providers that are acting on their own behalf". It remains to be seen whether, and in what depth, further details on such exemptions will be released.

---

[14] This is the case even despite the efforts and very welcome work of the Travel Rule Information Sharing Alliance – further details of which are available here.

[15] Generally, this market accepted (as opposed to legally defined) term refers to software or hardware that allows to hold, store and transfer cryptoassets which is not hosted by a third party, such as a financial institution or a CASP.

Transfers of cryptoassets with missing or incomplete information on the originator or beneficiary

Under the new Art. 17 of the recast WTR, where the CASP of the beneficiary becomes aware, when receiving cryptoassets, that the required travel rule information is missing or incomplete, that CASP provider shall reject the transfer or ask for the required information on the originator and the beneficiary before or after making the cryptoassets available to the beneficiary. Any such decision must be conducted on a risk-sensitive basis.

Crucially, where a CASP repeatedly fails to provide the required information on the originator or the beneficiary, the CASP of the beneficiary is required, pursuant to Art. 17 of the recast WTR, to take steps, which may initially include the issuing of warnings and setting of deadlines, and return the transferred crypto-assets to the originator's account or address. Alternatively, the CASP of the beneficiary may hold the transferred crypto-assets without making them available to the beneficiary, pending review by the competent authority responsible for monitoring compliance with AML/CTF provisions. The CASP of the beneficiary shall report that failure, and the steps taken, to the competent authority responsible for monitoring compliance with AML/CTF provisions.

Under Art. 18 of the recast WTR, the CASP of the beneficiary is required to take into account missing or incomplete information on the originator or beneficiary when assessing whether a cryptoasset transfer, or any related transaction, is suspicious and whether it should be reported as such to the relevant financial intelligence unit in accordance with EU AML/CTF legislation.

Data protection, the travel rule and cryptoassets

By its very nature the travel rule's information gathering and data sharing requirements raise questions for market participants on how to comply with data protection as well as privacy concerns. To maintain requisite EU data protection standards and rules throughout the transaction chain, the recast WTR extends its existing provisions on data protection and confidentiality to CASPs. As with payment services providers, CASPs are required to provide clients with standard information on data protection and processing of personal data before establishing a business relationship with or prior to carrying out an occasional transaction with that client.

It nevertheless remains to be seen whether the Court of Justice of the European Union (**CJEU**) will be asked to consider whether the travel rules' aims are proportionate in light of the safeguards set in the EU's data protection and privacy legislative and regulatory framework. The CJEU has in the past adjudicated on such matters – mostly in the context of the EU Charter of Fundamental Rights[16] and may well be called upon to do so in the context of the recast WTR and how data gathered and shared is proportionate to the protections set out in the EU Charter of Fundamental Rights.

Potential further developments that may be proposed outside the recast WTR

As highlighted above, not all of the European Parliament's additional suggestions for reforms have made it into the agreed position for a recast WTR. In summary these include proposals to introduce:

1. a ban on high-risk transfers on AML/CTF grounds – a proposal that may become quite likely and may well be introduced as part of outputs from the AML Package as it could be aligned with existing EU principles on assessments of non-EU i.e., third countries in terms of their AML/CTF risk levels;

2. a "public register" for non-compliant and non-supervised CASPs and/or a "CASP blacklist" – this option may, subject to centralising the administration of such a public register and/or blacklist with either the EU's new proposed AML Authority or another European Supervisory Authority (such as the European Securities and Markets Authority) would require commitment to strengthening institutional resources. It is quite likely that some form of this proposal may be included in the finalisation of MiCA and/or the outputs flowing from the AML Package;

3. enhanced due diligence obligations – in respect of cryptoasset transfers that relate to "banking transactions" (the latter not being defined); and

[16] See notably Court Report available here in the context of the EU's Data Retention Directive and questions of proportionality with the aims of Arts. 7, 8 and 11 of the Charter of Fundamental Rights of the European Union.

4. a ban on transactions with third-country CASPs (i.e., potentially going hand in hand with proposal in bullet point 2) – that are deemed to be non-compliant with EU rules. This proposal could be capable of being advanced in some form of equivalence assessment.

Outlook

The final amendment to the WTR has not yet been published as of the date of this Client Alert. While the rules are generally welcomed by most, the compliance burden may become challenging and will require careful preparation amongst all market participants.[17] The same also applies on how to translate travel rule compliance in a manner that can also help satisfy tax data and reporting compliance obligations.

Given the interaction of the revised WTR with other EU legislative and regulatory reforms, notably MiCA and the EU's AML Package, a lot of exactly when the travel rule will be fully and formally rolled out to cryptoasset transfers is dependent on the pathways to adoption of other areas of reform. Both the European Parliament and European Council have proposed that the timeline for delivery of the WTR be decoupled from any path dependencies so that the recast WTR and thus the travel rule could apply much sooner than the other (more technical) reforms being finalised in MiCA and the AML Package.

In terms of next steps in the recast WTR's legislative process (assuming it is decoupled from MiCA and the AML Package), the European Parliament, European Council and European Commission will be jointly working on the technical aspects of the final text of the WTR. Thereafter, the text must be approved by both the Economic and Monetary Affairs and Civil Liberties and Justice Committees as well as the European Parliament as a whole before it can be published in the EU's Official Journal (the **OJ**). Once published in the OJ, the recast WTR would then enter into force 20 days after its publication in the OJ. Once the new rules enter into force, obliged entities will have 9 months to implement the travel rule, with full compliance with the recast WTR expected 18 months after its entry into force.

Given that no major surprises are expected in the detail of the WTR's amendments and extension of the travel rule, affected market participants will want to begin preparatory measures to ensure they are ready to meet regulatory requirements and supervisory expectations well in time. Consequently, market participants will equally want to take stock of and forward plan any changes to technical processes, procedures, systems and controls as well as internal policies and customer facing documentation relevant to KYC. Part of this may also include benchmarking how compliance with the EU travel rule's aims compares to similar efforts yet often differing technical details as proposed in other non-EU jurisdictions, notably the UK, the US and further afield.

About us

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from these proposals.

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's RegCORE Team via de_regcore@pwc.com or our website.

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas@pwc.com

[17] See the quotes by Assita Kanko, co-rapporteur for LIBE, or Ernest Urtasun, co-rapporteur for ECON, available here https://www.europarl.europa.eu/news/en/press-room/20220627IPR33919/cryptoassets-deal-on-new-rules-to-stop-illicit-flows-in-the-eu?xtor=AD-78-[Social_share_buttons]-[linkedin]-[en]-[news]-[pressroom]-[information-on-transfer-of-funds-and-cryptoassets].

www.pwclegal.de