13 FAQs on the FATF's Updated Guidance for a Risk-Based Approach to Crypto

coinfirm

December 2021

On the 28th of October, the Financial Action Task Force (FATF) – the global intergovernmental AML watchdog organization – published its *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Coinfirm's Head of Regulatory Affairs, Barbara Halasek, explains what has changed on the FATF's stance on Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs).

Table of Contents:

What is the purpose of FATF's Guidance Update for VAs and VASPs?

The updated Guidance expands on already existing FATF guidance on crypto assets.

The Guidance:

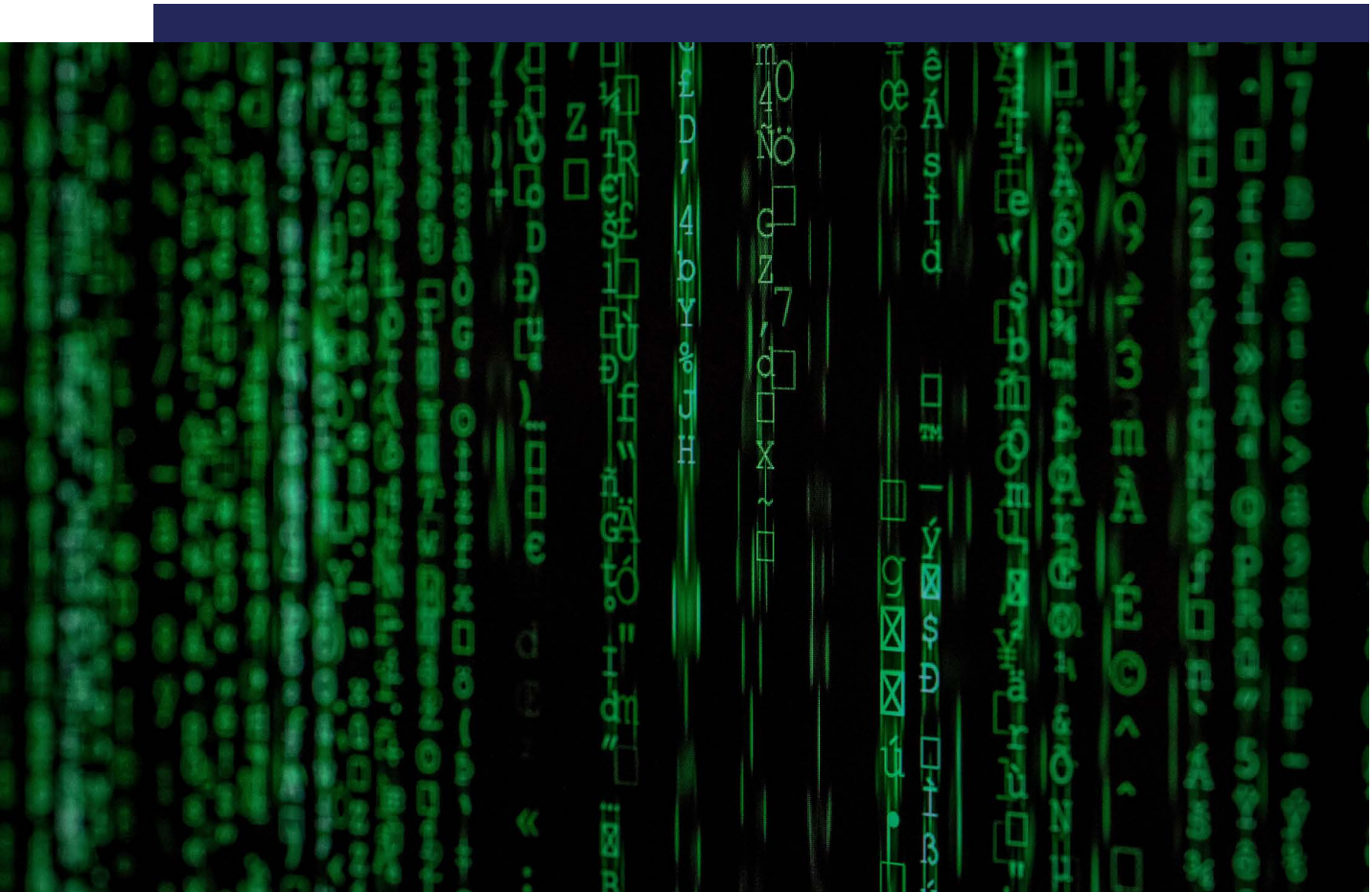
- Defines what are 'virtual assets' (VA) and explains what activities are falling in the definition of Virtual Asset Service Providers (VASPs)
- Clarifies how FATF Recommendations should be applied in the context of VAs and VASPs
- Explains the application of risk-based approach (RBA) principles in VAs

The paper includes links to other FATF papers published in relation to VAs that should be read in conjunction with this guidance.

The Guidance is addressed to countries, supervisors/ regulators and VASPs.

As FATF objectives are centered around anti-money laundering (AML) and counter-terrorist financing (CTF), the guidance does not address other regulatory matters that may be relevant to VAs and VASPs (e.g. market integrity, consumer protection etc).

The Guidance aims at clarifying the existing FATF standards rather than changing them.



What are the main areas where additional guidance was provided?

The paper expands on the Guidance from previous papers on virtual assets and provides additional clarifications in 6 specific areas. The revisions in the Guidance aim to;

(1) clarify the definitions of VAs and VASPs to make clear that these definitions are expansive and there should not be a case where a relevant financial asset is not covered by the FATF Standards (either as a VA or as another financial asset),

(2) provide guidance on how the FATF Standards apply to 'so-called' stablecoins and clarify that a range of entities involved in stablecoin arrangements could qualify as VASPs under the FATF Standards,

(3) provide additional guidance on the risks and the tools available to countries to address the ML/TF risks for peer-to-peer transactions,

(4) provide updated guidance on the licensing and registration of VASPs,

(5) provide additional guidance for the public and private sectors on the implementation of the 'Travel Rule' and

(6) include Principles of Information-Sharing and Co-operation Amongst VASP Supervisors.

The Guidance draft was published in March 2021 and subject to public consultation. The industry responded with feedback to FATF, which has resulted in some amendments to the original March draft. Most noticeably, the FATF;

- Revised the original draft language around the application of VASP definition in **DeFi**, providing more clarity on what factors should be taken into account when considering which party (if any) would qualify as VASP in DeFi arrangements,
- Polished the original draft wording around potential mitigating measures for **peer to peer** transactions
- Added an indication that non-fungible tokens may be considered as virtual asses if used for payments or investment,
- Expanded the clarification around the application of 'correspondent banking' requirements in **VASP to VASP** relationships

What is the impact of the updated Guidance?

In order to fully understand the impact on crypto businesses, a bit of background is needed around the FATF and how their Recommendations & Guidance Papers relate to national legislation.

The FATF's Recommendations on how to build an effective AML/CTF system are guiding principles for FATF member countries and for many other countries that belong to FATF-style bodies. As such, updates to FATF Recommendations typically result in changes to national regulatory requirements stipulated by law and relevant additional national measures. In the discussed Guidance, the FATF explicitly states that the Guidance *'interprets existing standards, but does not change them'*. However, even though there are no changes 'per se', some of the areas clarified are likely to prompt countries to update their regulatory frameworks in respective areas.

At Coinfirm, we believe that the following may be the focus areas resulting in widened regulatory frameworks, through changes to regulations or additional regulators' guidance or including them in the newly created frameworks (for these countries that are still to introduce AML framework for virtual assets);

- Travel Rule – this is an obvious foreseen development, especially given the repeated strong call from the FATF for all countries to introduce the Travel Rule to address the so called 'sunrise issue' (inconsistency among countries in the introduction of the Travel Rulew resulting in compliant countries' VASPs encountering challenges on how to transact with non-compliant countries' VASPs),
- Definition of VASPs and VAs – at the moment, many crypto regulatory frameworks refer only to crypto exchanges and custodians, as the requirements for stablecoins and NFTs are not always clear. The expanded definitions are already being worked on by some countries, most remarkably with the **EU's Markets in Crypto Assets (MiCA) Directive** introducing even wider scope of regulated activities or the UK issuing public consultations on how to fit stable coins in their existing virtual assets definitions, and additionally, to a lesser extent;

- Licensing and registration of VASPs – with the global nature of crypto assets and materialized risks of international funds flows, we would foresee that some countries decide to extend licensing requirement for VASPs' marketing their products to citizens of a given country (noting that this is already in place in some jurisdictions).

Download the Markets in Crypto Assets

With regards to DeFi businesses & peer-to-peer transactions, we believe that it is more likely that the countries and regulators will take an 'observe and analyze' approach at first.

For peer-to-peer (P2P) transactions, the FATF provides countries with a number of measures to address their inherent risks and simultaneously emphasizes the need for countries to understand the scope of P2P risks. We expect that the countries and regulators will probably first conduct the needed assessment of the risks in the P2P area. Alternatively, some countries and regulators may decide to introduce measures to restrict P2P payments as the risk-averse approach (e.g. through allowing licensed VASPs to send transfers only to VASP wallets). Coinfirm believes this is not the best approach, as it will shift the risk elsewhere (be it to other countries or outside of the regulators' eyes) rather than reduce it. Nevertheless, we think it may be a possible outcome for some of the countries.

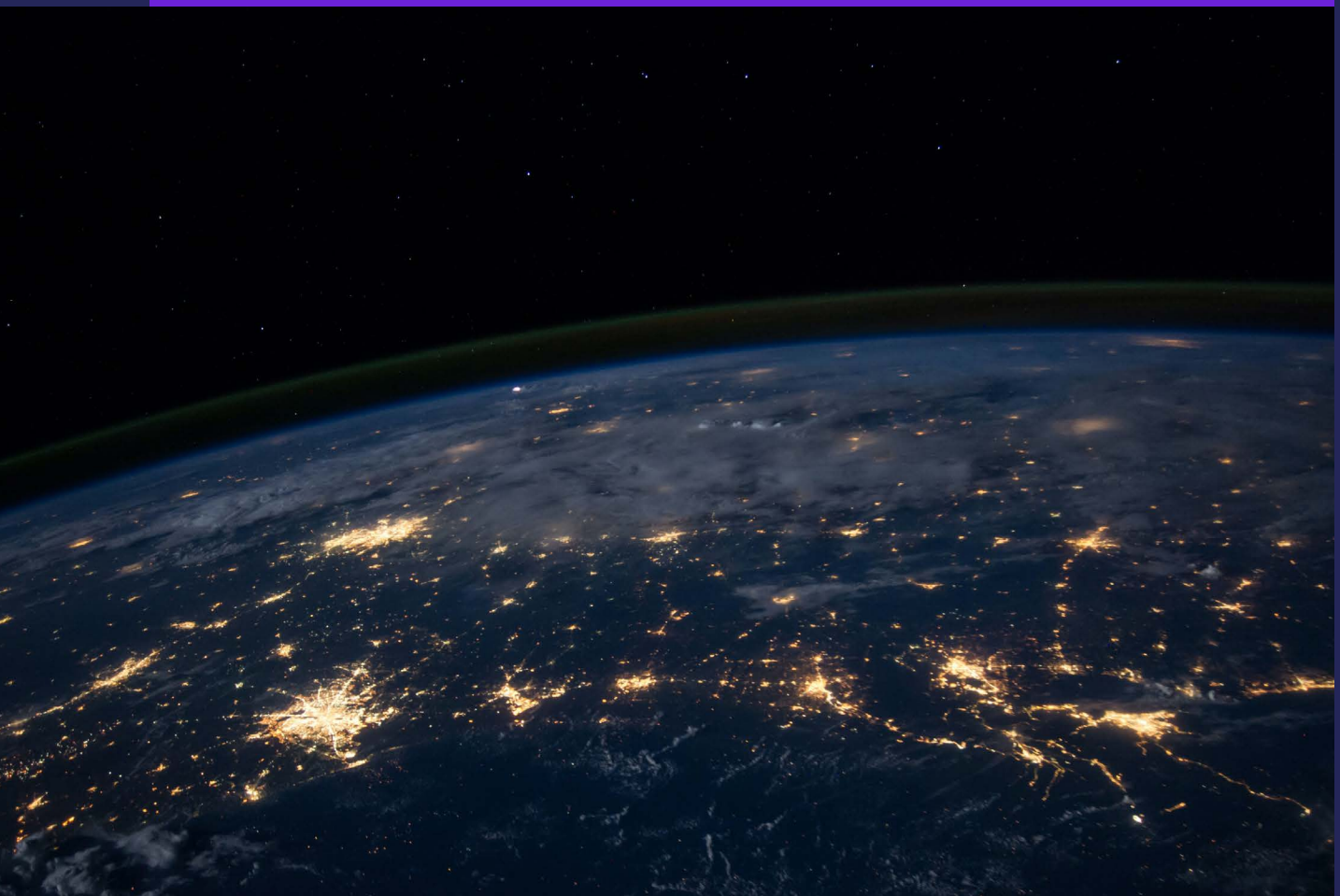
For the DeFi sector – specifically the application of the VASP definition to DeFi market players – the FATF admits there is no 'one size fits all' approach – different DeFi platforms may need to be treated differently in terms of which party (if any) qualifies as a VASP and has resulting AML obligations.

What must be noted though in relation to DeFi, is that according to the FATF Guidance paper, the existing VASP definition scope is sufficient to be applicable to DeFi platforms. Therefore, even with no changes to the existing national definitions of which businesses fall into 'obliged entities'/ AML regulated entities, there is a potential that a specific party linked to a DeFi platform can be deemed as requiring to be regulated for AML purposes.

It is difficult to predict the countries and regulators' actions on that front. As noted previously, we may expect the definitions of VASPs/ obliged entities to be updated accordingly in national legislations; however, it appears more likely that lawmakers and regulators will choose not to be explicit in terms of the application in DeFi for the time being. Coinfirm believes and has expressed a stance for a considerable time that AML regulation in DeFi is needed, hence our DeFi-specific product offerings (**AML Liquidity Pools Reports** and the **AMLT Oracle**). At the same time,
we are a strong advocate for a continuous and open dialogue on the matter of DeFi regulation. We would encourage more DeFi businesses to share insights on their AML controls to educate the wider private and public sector on AML compliance use cases in DeFi. Similarly, we would encourage regulators to analyze DeFi market players and share example use cases of 'good practices' and 'bad practices' to provide more 'hands-on' guidances of how they would apply the VASP definition in the DeFi context.

AMLT Oracle

Liquidity Pools AML Reports



What are the practical steps that crypto businesses are recommended to take?

Looking at the scope and content of the Guidance, Coinfirm would encourage crypto businesses to consider taking the following actions:

- VASP Definition: if you are not yet regulated for AML purposes: re-review your business model with the clarified VASP definition to determine if you fall in the scope of the FATF's VASP definition and your local national legislation scope of crypto regulated businesses. This is important specifically to DeFi-sector, NFT-focused businesses and stablecoins issuers where a case-by-case analysis must be performed to evaluate the applicable requirements. Even if you determine to be outside of the VASP/your local relevant definition, consider your money laundering risks. Apart from the regulatory risk, you may be facing a number of other risks, such as legal, financial or reputational. Implementing AML controls and the use of Coinfirm's tools in the framework may mitigate these risks.
- Travel Rule: if you have not yet looked into the Travel Rule requirements, it would be reasonable to start such an exercise. Your country may be quick to introduce the legal requirement (see Germany as an example) or you may still have 1-2 years until the rule makes it to your national framework, but using this time to investigate and try different solutions seems a reasonable approach. Additionally, bear in mind that the clarified Travel Rule requirements explicitly ask for Due Diligence on counterparty VASPs and sanction screenings of collected names (even in the case of unhosted wallets), which may have not been considered by those VASPs already taking care of the Travel Rule. Coinfirm has **partnered with Notabene**, who are experts on implementing the Travel Rule and offer a comprehensive solution in the matter. Additionally, for the last few years we have been risk assessing VASPs in a wide variety of categories that may form the basis of your VASP Due Diligence.
- Risk-Based Approach: the Guidance provides a number of various measures on how to apply in practice a Risk-Based Approach in crypto. We would strongly encourage crypto businesses to re-review their AML programs and evaluate whether they are truly risk based. Sooner or later, you are likely to be controlled by the regulator and having confidence around having truly risk-based as opposed to tick-box control typically pays off. Most remarkably, this will be needed in relation to peer-to-peer transfers. At Coinfirm, we have recognized that need since our beginnings, hence Coinfirm's risk rating of crypto addresses does not only consider risk indicators pertinent to the address owner (e.g. whether it is a mixer or exchange, country risk etc), but also a number of risk indicators relating to all historical transactions on the address (its exposure to illicit funds as well as behavioral patterns). As such, our solution can risk score unhosted wallets used in P2P transactions.

Can you summarize the Guidance in a few points?

We would love to and to some extend will save your time spent on reading the Guidance through summarizing the areas that we see as the most important. However, we would encourage everyone in the sector to read the Guidance. It reads well and as always with such papers – the devil is in details. The FATF has purposely spent time on selecting specific words and summarizing these carefully written 111 pages in a few bullet points but could always come with the cost of missing some elements. Nevertheless, we would like to provide a summary with regards to the guidance focus areas, respond to the questions we get most often asked with regards to the Guidance and share relevant extractss of the Guidance.

Are stablecoins considered virtual assets?

Stablecoins can qualify as a 'virtual asset' or 'financial asset';

(54)

The FATF reaffirms statements in its G20 report that a 'stablecoin' is covered by the Standards as either a VA or a financial asset (e.g., a security).

The FATF stresses throughout the entirety of the document that the determination of what constitutes a 'virtual asset' should be done based on the actual functional characteristics of a given asset as opposed to using the industry terms and labels. As such, in order to determine whether a stablecoin qualifies as 'a virtual asset', the coin should;

- Have inherent value to be traded or transferred and,
- Be used for payment or investment.

Looking at the above criteria, most stablecoins would qualify as 'virtual assets'. The caveat to bear in mind is that an asset that merely uses the technology to represent another asset, would not be considered as a 'virtual asset'. CDBDs are an example – they are meant to be virtual representations of fiat currency and as such fall outside of the remit of the 'virtual assets' definition.

(51)

[...] a digital asset that is exchangeable for another asset, such as a stablecoin that is exchangeable for a fiat currency or a VA at a stable rate, could still qualify as a VA. The key question in this context is whether the VA has inherent value to be traded or transferred and used for payment or investment or, rather, is simply a means of recording or representing ownership of something else

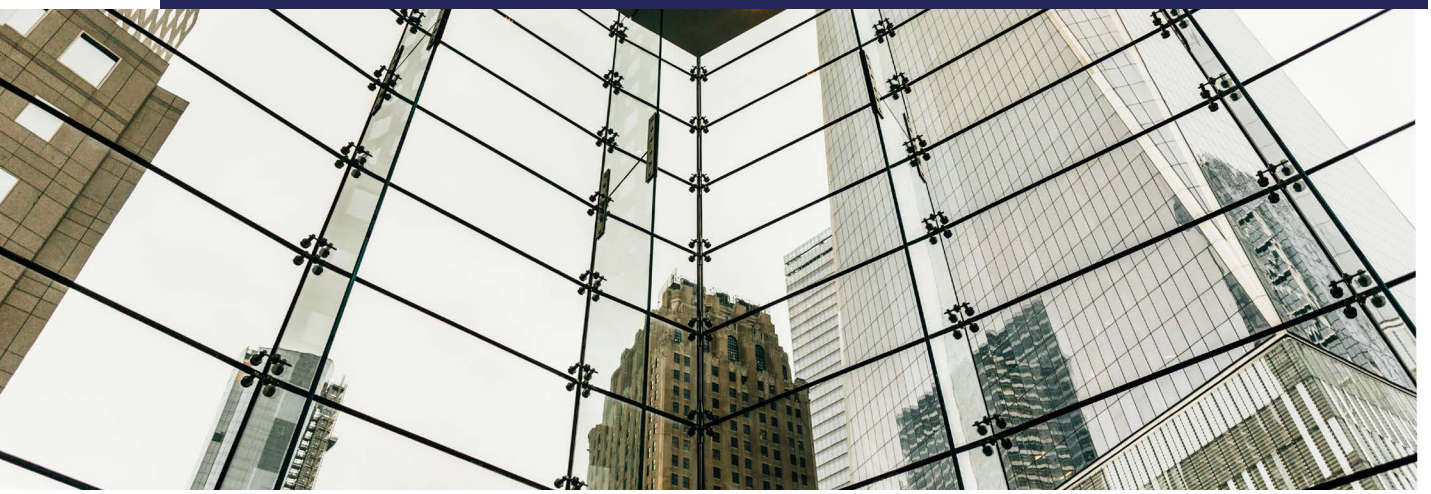
Stablecoin issuers may be considered as VASPs or financial institutions in cases where there is a central governance body. The FATF also acknowledges that decentralized stablecoins models are not impossible, yet calls countries to exercise caution in making a determination of central governance body non-existence.

(Box1)

[...] , central governance bodies of stablecoins will, in general, be covered by the FATF standards either as a VASP or a FI. When a similar function is provided with a degree of decentralisation, it is expected that countries will take a functional approach to identify obliged entities and will mitigate the relevant risks based on a RBA [...]

(139)

Supervisors should be especially cautious of claims that stablecoins involve no entity that qualifies as a VASP or other obliged entity. This is especially true in the pre-launch phase, as the process of creating and developing an asset for launch is unlikely to be able to be automated



Are NFTs considered virtual assets?

Similarly to stablecoins, Non-Fungible Token (NFTs) assets may be considered as virtual assets or financial assets, depending on their functional scope and use. NFTs may fall into the VA definition if they are *'used for payment or investment'*.

(53)

Digital assets that are unique, rather than interchangeable, and that are in practice used as collectibles rather than as payment or investment instruments, can be referred to as a Non-Fungible Tokens (NFT) or crypto-collectibles.

Such assets, depending on their characteristics, are generally not considered to be VAs under the FATF definition. However, it is important to consider the nature of the NFT and its function in practice and not what terminology or marketing terms are used. This is because the FATF Standards may cover them, regardless of the terminology. Some NFTs that on their face do not appear to constitute VAs may fall under the VA definition if they are to be used for payment or investment purposes in practice. Other NFTs are digital representations of other financial assets already covered by the FATF Standards. Such assets are therefore excluded from the FATF definition of VAs but would be covered by the FATF Standards as that type of financial asset. Given that the VA space is rapidly evolving, the functional approach is particularly relevant in the context of NFTs and other similar digital assets. Countries should therefore consider the application of the FATF Standards to NFTs on a case-by-case basis.

(84)

FATF similarly does not seek to capture the types of closed-loop items that are non-transferable, non-exchangeable, and cannot be used for payment or investment purposes. Such items might include airline miles, credit card awards, or similar loyalty program rewards or points, which an individual cannot sell onward in a secondary market outside of the closed-loop system

Are DeFi platforms and businesses considered as VASPs?

Consistently with the definition of VAs, the VASP definition should also be applied looking at the functional scope of the business as opposed to marketing labels.

(56)

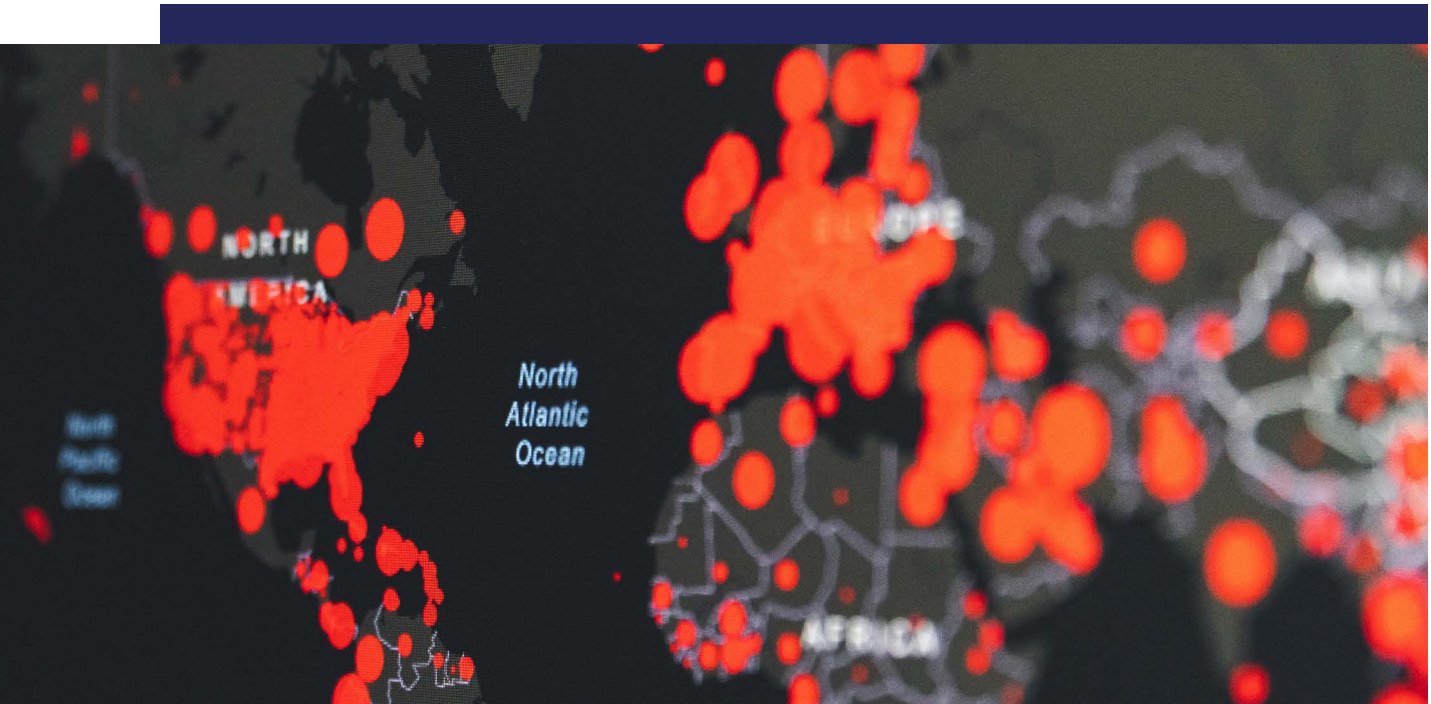
Countries should not apply their definition based on the nomenclature or terminology which the entity adopts to describe itself or the technology it employs for its activities

With that in mind, there is no single simple answer in terms of whether DeFi businesses are considered as VASPs – the answer must be derived based on the analysis of the DeFi arrangement functions and level of control maintained by parties.

First of all though, it must be noted that protocols or software are considered as potential VASPs, as a VASP can only be a natural or legal person.

(67)

A DeFi application (i.e. the software program) is not a VASP under the FATF standards, as the Standards do not apply to underlying software or technology (see paragraph 82 below). However, creators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements, even if those arrangements seem decentralized, may fall under the FATF definition of a VASP where they are providing or actively facilitating VASP services [...]



The FATF explains that in DeFi labelled projects it is possible that a party (be it a legal or natural person) maintains 'control' or 'influence'. In such instances, the party with 'control' or 'influence' should be considered as VASP (and consequently must comply with regulatory obligations for VASPs). The following factors are listed as examples of indicators to consider;

- Control or influence over assets,
- Control or influence over aspects of the service's protocol,
- Existence of an ongoing business relationship between the party and DeFi arrangement users,
- Profiting from the DeFi arrangement,
- Ability to set or change parameters to identify the owner/ operator of DeFi arrangement,
- Who can make decisions affecting operations,
- Who generated and drove the creatin and launch of the service, and,
- Who could shut down the service.

[...] there may be control or sufficient influence over assets or over aspects of the service's protocol, and the existence of an ongoing business relationship between themselves and users, even if this is exercised through a smart contract or in some cases voting protocols. Countries may wish to consider other factors as well, such as whether any party profits from the service or has the ability to set or change parameters to identify the owner/ operator of a DeFi arrangement. These are not the only characteristics that may make the owner/operator a VASP, but they are illustrative. [...]

(68)

It seems quite common for DeFi arrangements to call themselves decentralized when they actually include a person with control or sufficient influence, and jurisdictions should apply the VASP definition without respect to self-description

(93)

When there is a need to assess a particular entity to determine whether it is a VASP or evaluate a business model where VASP status is unclear, a few general questions can help guide the answer. Among these would be who profits from the use of the service or asset, who established and can change the rules, who can make decisions affecting operations, who generated and drove the creation and launch of a product or service, who maintains an ongoing business relationship with a contracting party or another person who possesses and controls the data on its operations, and who could shut down the product or service. Individual situations will vary and this list is not definitive and offers only some examples.

The FATF recognizes that there may be DeFi arrangements where no legal or natural person can be identified having sufficient control or influence to consider them as a VASP. In such circumstances, it is suggested that countries consider the option of requiring that for a DeFi arrangement to exist there must be a regulated VASP involved. In other words, there may be cases of DeFi platforms where despite no single party keeping control or influence, AML controls are exercised by a regulated party. At the face of it, the statement may appear contradictory – as exercising AML obligations without having the control over the platform can present practical challenges. However, we at Coinfirm believe in the potential of embedding AML controls in the smart contracts' language as we did with the AMLT Oracle product, which is our response to the market for managing AML risks in a decentralized manner.

(69)

Where it has not been possible to identify a legal or natural person with control or sufficient influence over a DeFi arrangement, there may not be a central owner/operator that meets the definition of a VASP.

Countries should consider, where appropriate, any mitigating actions, where DeFi services operating in this manner are known to them. [...] As an example, where no VASP is identified, countries may consider the option of requiring that a regulated VASP be involved in activities related to the DeFi arrangement in line with the country's RBA or other mitigants

In terms of the application of VASP definition functional scope to DeFi arrangements, it is most likely that the 'transfer' limb of the five VASP categories of activities would be applicable:

(62)

A person who meets these requirements will then be a VASP if it carries out one or more of the five categories of activity or operation described in the VASP definition (i.e., "exchange" of virtual/fiat, "exchange" of virtual/virtual, "transfer," "safekeeping and/or administration," and "participation in and provision of financial services related to an

(66)

Exchange or transfer services may also occur through technology commonly referred to as decentralized exchanges or platforms. A "decentralized or distributed application (DApp)," for example, is a term that refers to a software program that operates on a blockchain or similar technology. Sometimes, such applications facilitate or support other protocols, applications, or digital assets and their transfer. These applications or platforms often run on a decentralized ledger, but often still have a central party with some measure of

involvement or control, such as creating and launching a VA, developing DApp functions and user interfaces for accounts holding an administrative "key" or collecting fees.

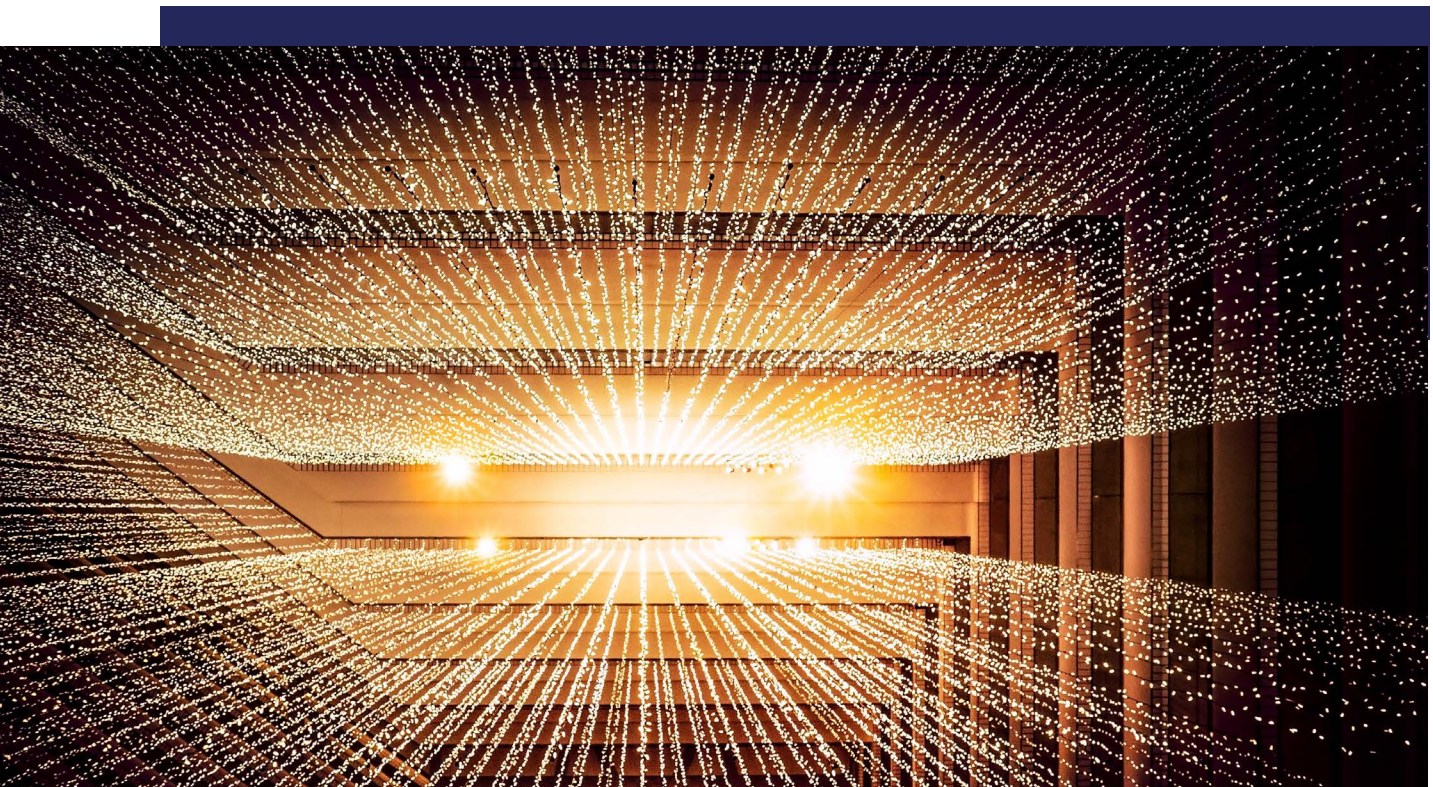
The Guidance also touches upon 'peer to peer platforms' and explains that depending on the functional set up of such a platform, there may also be a party qualifying as a VASP (despite labelling it as 'peer to peer');

(90)

Some platforms and providers offer the ability to conduct VA transfers directly between individual users. For such platforms, the broad reading of the definitions above will decide whether parties to providing such a service are VASPs on a functional basis, not on the basis of self-description or technology employed. Only entities that provide very limited functionality falling short of exchange, transfer, safekeeping, administration, control, and the provision of financial services associated with issuance will generally not be a VASP. For example, this may include websites which offer only a forum for buyers and sellers to identify and communicate with each other without offering, even in part, those services which are included in the definition of VASP.

(91)

For self-described P2P platforms, jurisdictions should focus on the underlying activity, not the label or business model. Some kinds of "matching" or "finding" services may also qualify as VASPs even if not interposed in the transaction. The FATF takes an expansive view of the definitions of VA and VASP and considers most arrangements currently in operation, even if they self-categorize as P2P platforms, may have at least some party involved at some stage of the product's development and launch that constitutes a VASP



What additional clarifications were provided around licensing and registration of VASPs?

The Guidance provides more clarity for determining in which jurisdiction(s) a VASP should be licensed or registered.

At a minimum, VASPs are to be required to license or register in the country where they were created (i.e. incorporated or registered in a commercial registry).

(125)

In accordance with INR. 15 paragraph 3, at a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created. References to creating a legal person34 include the incorporation of companies or any other mechanism that is used domestically to formalise the existence of a legal entity, such as registration in the public register, commercial register, or any equivalent register of companies or legal entities; recognition by a notary or any other public officer; filing of the company bylaws or articles of incorporation; allocation of a company tax number, etc.

Additionally, countries may require VASPs to license or register in the country where;

- They conduct operations from,
- They offer their products and/or services.

(127)

Jurisdictions may also require VASPs that offer products and/or services to customers in, or that conduct operations from, their jurisdiction to be licensed or registered in the jurisdiction. Host jurisdictions may therefore require registration or licencing of VASPs whose services can be accessed by or are made available to people residing or living within their jurisdiction, or may require VASPs that have employees or management located in their jurisdiction.

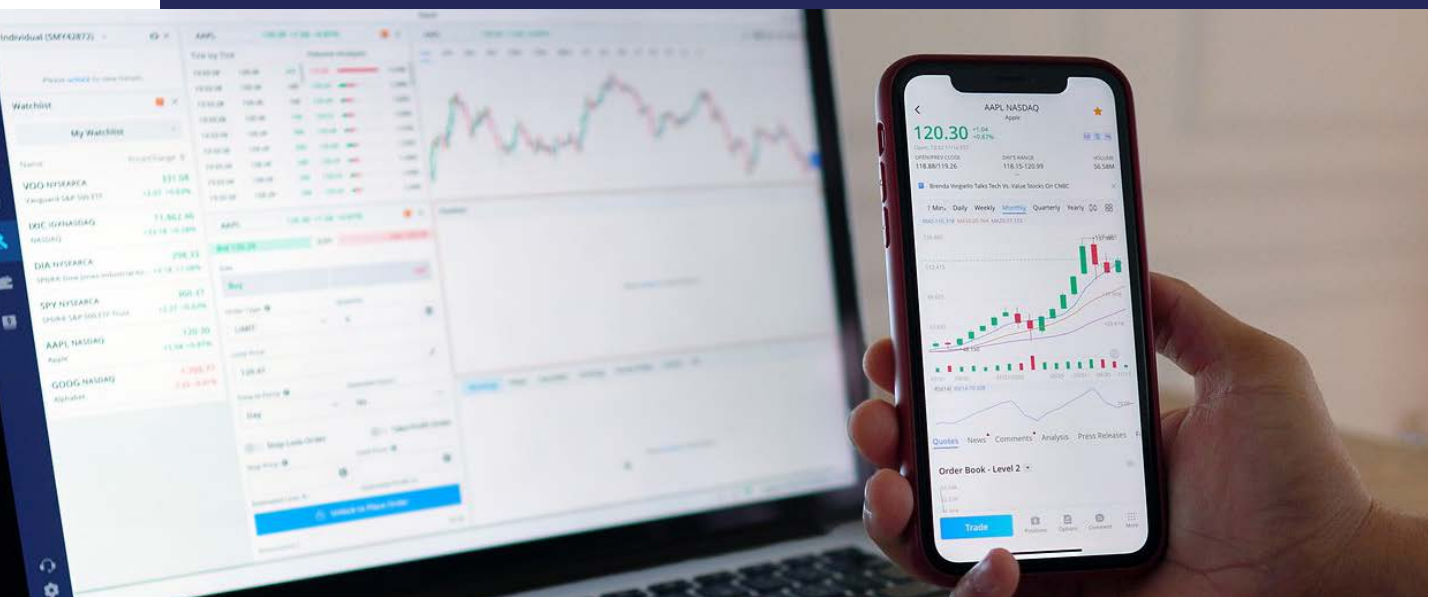
The Guidance provides the regulators with example indicators to identify whether a VASP offers their products to customers in a specific country;

128. In order to identify those VASPs offering products and/or services to customers in a jurisdiction without being incorporated in this jurisdiction, supervisors may use a set of relevant criteria. This could include the location of offices and servers (including customer-facing operations such as call centres), promotional communications targeting specific countries/markets, the language on the VASP website and/or mobile application, whether the VASP has a distribution network in a country (e.g., if it has appointed an intermediary to seek clients or physically visit clients resident in the country), and specific information asked to customers revealing the targeted country.

Are there any changes to the 'Travel Rule' requirements?

Table 1. Data requirements for ordering and beneficiary VASPs in the travel rule

Data item and required action	Ordering VASP	Beneficiary VASP
Originator Information	Required, i.e. submitting the necessary data to a beneficiary VASP is mandatory. Accurate, i.e. the ordering VASP needs to verify the accuracy as part of its CDD process.	Required, i.e. the beneficiary VASP needs to obtain the necessary data from ordering VASP. Data accuracy is not required. The beneficiary VASP may assume that the data has been verified by the ordering VASP.
Beneficiary Information	Required, i.e. submitting the necessary data to the beneficiary VASP is mandatory. Data accuracy is not required, but the ordering VASP must monitor to confirm no suspicions arise.	Required, i.e. the beneficiary VASP needs to obtain the necessary data from the ordering VASP. Accurate, i.e. the beneficiary VASP must have verified the necessary data and needs to confirm if the received data is consistent.
Actions required	Obtain the necessary information from the originator and retain a record. Screen to confirm that the beneficiary is not a sanctioned name. Monitor transactions and report when they raise a suspicion.	Obtain the necessary information from the originator and retain a record. Screen to confirm that the beneficiary is not a sanctioned name. Monitor transactions and report when they raise a suspicion.



Travel Rule requirements have been discussed in detail along with a clearly summarized obligations of the ordering and beneficiary VASP (see table below). The scope of the rule does not change; however there are two elements (that were already present in the March 2021 draft) that have not been explicitly stated out before – namely the need to conduct due diligence on ordering/ beneficiary VASPs (as applicable) and the need to also sanction screen originator/beneficiary names for transfers to unhosted wallets (where such name is not subject to verification measures).

The FATF remains technology agnostic and does not speak about specific products in the market to address Travel Rule requirements; however, the Guidance includes a useful summary of what a Travel Rule solution product should enable (see point 283).

In terms of the widely-known 'sunrise issue' problem, the FATF stipulates VASPs can require Travel Rule compliance from other VASPs through contract or business practice (as opposed to relying on legal obligations) in cases of transacting with VASPs in jurisdictions non-compliant with Travel Rule.

(200)

countries are implementing their AML/CFT frameworks for VASPs at different paces. This means that some jurisdictions will require their VASPs to comply with the travel rule prior to other jurisdictions (i.e., the 'sunrise issue'). This can be a challenge for VASPs regarding what approach they should take in dealing with VASPs located in jurisdictions where the travel rule is not yet in force. Regardless of the lack of regulation in the beneficiary jurisdiction, originating entities can require travel rule compliance from beneficiaries by contract or business practice. In general, those business decisions are made by each individual VASP based on their risk-based analysis.

The Guidance also sets out what are potential ways of addressing transfers from VASPs to unhosted wallets. First of all, it reiterates that Travel Rule obligations apply to such transfers where;

(203)

The FATF recognizes that unlike traditional fiat wire transfers, not every VA transfer may involve (or be bookended by) two obliged entities, whether a VASP or other obliged entity such as a FI. In instances in which a VA transfer involves only one obliged entity on either end of the transfer (e.g., when an ordering VASP or other obliged entity sends VAs for or on behalf the originator to a beneficiary that is not a customer of a beneficiary institution but rather an individual VA user who receives the VA transfer to an unhosted wallet), countries should still ensure that the obliged entity adheres to the requirements of Recommendation 16 with respect to their customer (the originator or the beneficiary, as the case may be).

The language further explains that in case of transfers to unhosted wallets, VASPs are to collect respective originator or beneficiary information (as applicable) from their customer.

(295)

VASPs and obliged entities may undertake transfers to non-obliged entities (i.e., unhosted wallets). In such circumstances, a VASP should obtain the required originator and beneficiary information from their customer, because they cannot obtain the relevant information from another VASP.

In such instances, despite the lack of the third parties verifying the accuracy of the information (as is the case in VASP to VASP transfers), VASPs should have sufficient controls in place to address the **sanctions** risk and suspicious activity reporting. While the Guidance explains what may raise suspicions in this context (note below the mention of the use of blockchain analytics for that purpose), it remains silent on how to deal with handling sanction screening hits results. In the absence of CDD information on the collected name, it is reasonable to assume that VASPs may face cases of numerous false positives of addresses with no information to check against (think of screening the likes of John Smith).

(212)

Although VASPs are not required to submit verified required information on the beneficiary (see Recommendation 16 above), there could be the situation where a VASP has suspicion on the accuracy of data it processes from any discrepancies that the VASP has noted. These discrepancies could be identified with the support from blockchain analytic tools; information provided by its counterparty VASP; external authorities; or based on its transaction history and records. If there are any discrepancies due to inaccurate or incomplete information provided by its customer (in case of originator VASPs), or originator VASPs (in case of beneficiary VASPs), this should be evaluated together with the transactions requested or related to the same customer in order to understand if suspicions arise

Further, in terms of the transfers to and from unhosted wallets, VASPs are presented with potential measures to address the inherent risks. At Coinfirm, we would certainly envisage that the use of blockchain analytics to address the issue of unhosted wallets would enhance the control framework (especially considering our methodology of risk scoring that looks at all interactions a given address had and its behavioral patterns).

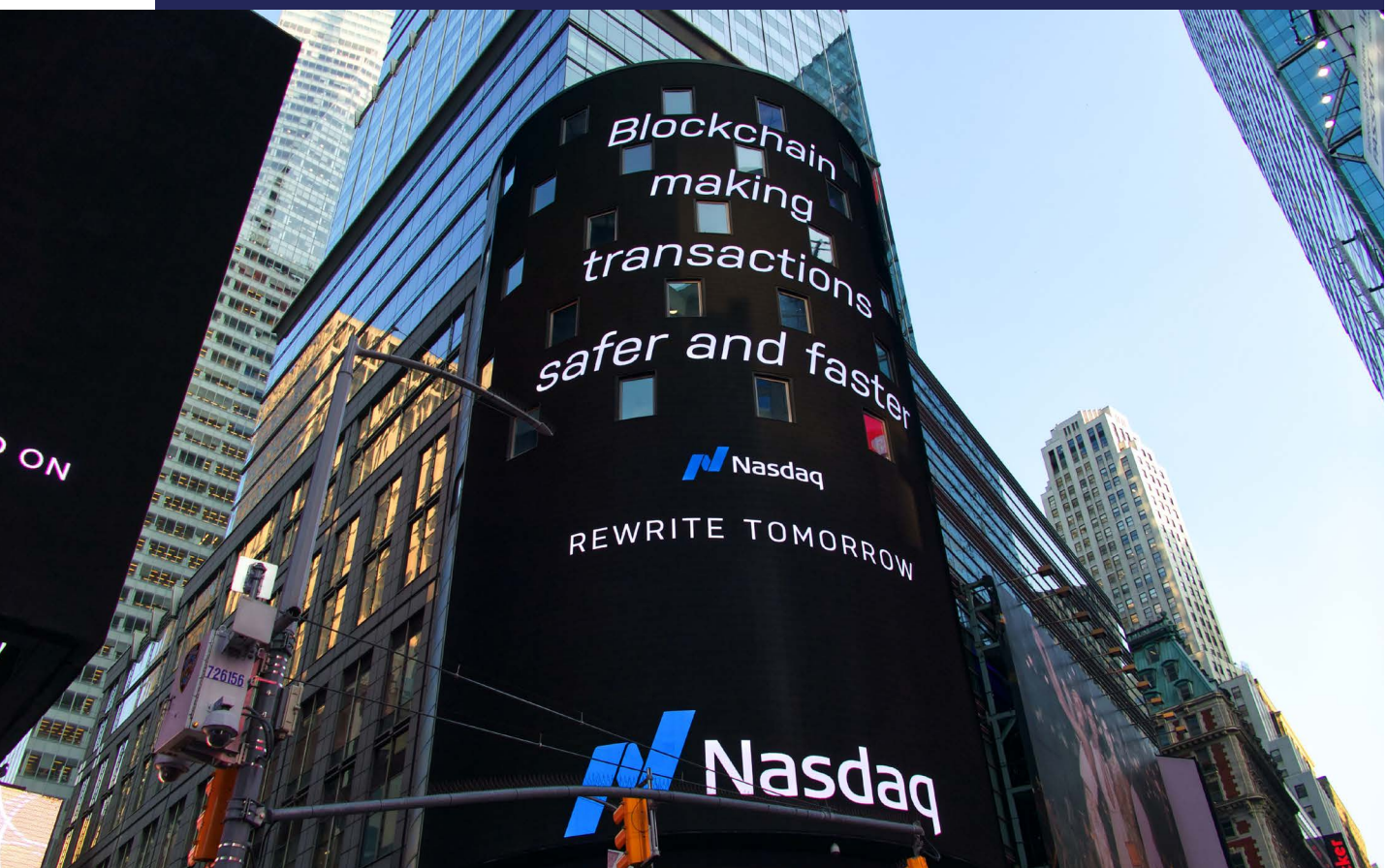
(297)

A VASP may choose to impose additional limitations, controls, or prohibitions on transactions with unhosted wallets in line with their risk analysis. Potential measures include

a. enhancing existing risk-based control framework to account for specific risks posed by transactions with unhosted wallets (e.g., accounting for specific users, patterns of observed conduct, local and regional risks, and information from regulators and law enforcement); and

b. studying the feasibility of accepting transactions only from/to VASPs and other obliged entities, and/or unhosted wallets that the VASP has assessed to be reliable.

Last, but not least, the updated Guidance on the Travel Rule outlines the need to conduct VASP Due Diligence before transacting with another VASP address (see below for more details).



What is VASP Due Diligence and VASP Correspondent Banking Diligence and when are they required?

The clarifications around the Travel Rule set out the need to conduct VASP Due Diligence for transfers from VASP-to-VASP accounts, whilst at the same time the Guidance devotes a separate part to VASP Correspondent Banking Due Diligence.

Correspondent Banking relationships in the context of VASPs is defined as the provision of VASP services by one VASP to another VASP, e.g. through the use of nested services;

(165)

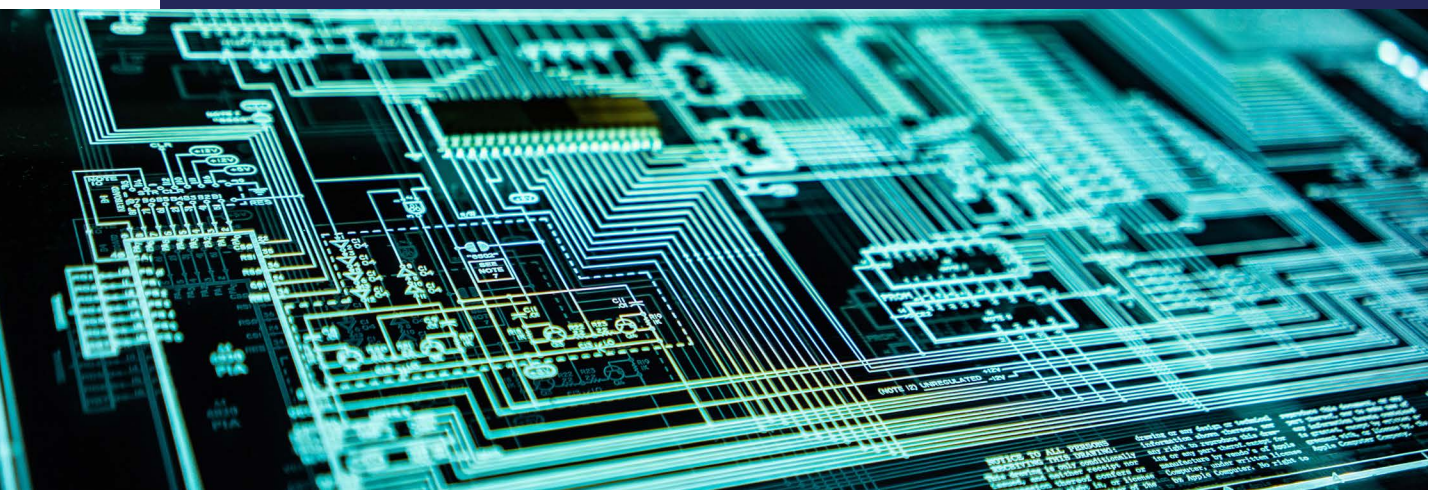
Recommendation 13 is applicable to VASPs. In this Guidance, a 'correspondent relationship' is the provision of VASP services by one VASP to another VASP or FI. Like its banking sector equivalent, such a correspondent relationship is characterised by its on-going, repetitive nature. Such a relationship could also include, for example, one VASP white-labelling its platform functionality to another VASP and also providing nested services (providing accounts to smaller VASPs for access to liquidity and trading pairs).

In the case of a Correspondent Banking type of relationship, the scope of due diligence checks is outlined in the extract below and laid out in the original Recommendation 13. Senior management approval is required prior to entering into Correspondent Banking-like relationships with a VASP. Additionally, a VASP should be satisfied that a correspondent VASP has done due diligence on their customers and is able to provide relevant CDD information on request.

(166)

In applying it to VASPs, countries should require VASPs providing services to another VASP or financial institution as part of a cross-border correspondent relationship to:

a. gather sufficient information about the other VASP or FI with which it proposes to establish a cross-border correspondent relationship, to understand fully the nature of the other VASP or financial institution's business and its AML/CFT risk control framework, including: what types of customers the other VASP or FI intends to provide services to through the cross-border correspondent relationship;



b. gather sufficient information and determine from publicly available sources the reputation of the other VASP or FI, the quality of supervision it is subject to and whether it has been subject to an ML/TF investigation or regulatory action;

c. assess the other VASP's or FI's AML/CFT controls;

d. obtain approval from senior management before establishing new cross-border correspondent relationships; and

e. with respect to accounts or custodial wallets able to be used directly by customers of the other VASP or FI to transact business on the customer's own behalf, be satisfied that the other VASP or FI has conducted CDD on such customers and is able to provide relevant CDD information on request, to the extent permitted privacy and data protection regulations in both jurisdictions.

This is separate from the Travel Rule/Recommendation 16 VASP Due Diligence. The FATF explains that in the virtual assets sector, it is possible for a transaction to occur between 2 VASPs without a VASP-to-VASP relationship – unlike in banking. In other words, it is possible to execute a transfer to another VASP without a commercial 'correspondent banking' form of relationship among VASPs. Despite the lack of the relationship and resulting Correspondent Banking Due Diligence requirements, some level of VASP DD checks is necessary to comply with the Travel Rule.

(169)

For clarity, counterparty due diligence for the purpose of complying with Recommendation 16 is distinct from the obligations applicable to cross-border correspondent relationships. Unlike the banking sector, it is possible for transfers of VA for or on behalf of another person to occur between VASPs, even in the absence of a correspondent relationship or any other relationships

In terms of the level of checks needed for Travel Rule VASP Due Diligence, the FATF refers to the scope of checks as per Recommendations 10 and 13, which in practice means typical customer due diligence requirements;

(289)

When establishing a new counterparty VASP relationship, a VASP may obtain information set out by Recommendations 10 and 13 directly from the counterparty VASP. Under the requirements of those Recommendations, this information should be verified.

Focus is being made on assessing the VASP AML controls, whilst also taking into account the robustness of the AML regulatory framework in the VASP country.

(291)

The VASP would need to assess the counterparty VASP's AML/CFT controls to avoid submitting their customer information to illicit actors or sanctioned entities and should also consider whether there is a reasonable basis to believe the VASP can adequately protect sensitive information.

While Travel Rule VASP DD and Correspondent Banking VASP DD are different in scope, most likely than not the Correspondent Banking one would meet the requirements of the Travel Rule.

What does the paper say about peer-to-peer transactions?

Peer-to-peer (P2P) transactions are one of the key focus areas of the Guidance update.

To fully grasp the Guidance and its implications, it is essential to understand what the FATF means when referring to P2P transfers;

(37)

The FATF defines peer-to-peer' (P2P) transactions as VA transfers conducted without the use or involvement of a VASP or other obliged entity (e.g., VA transfers between two unhosted wallets whose users are acting on their own behalf).

The FATF notes the inherent risks of such transfers resulting from the lack of a regulated third party involved and the global reach of these assets' movement channels. The Guidance calls for a deeper understanding of the actual risks these transfers pose;

(105)

countries should also seek to understand the ML/TF risks related to P2P transactions and how they are being used in their jurisdiction. Measures that countries should consider to assist in understanding the risks of P2P transactions include:

a. conducting outreach to the private sector, including VASPs and representatives from the P2P sector (e.g. consulting on AML/CFT requirements concerning P2P transactions);

b. training of supervisory, financial intelligence unit (FIU) and law enforcement personnel; and

c. encouraging the development of methodologies and tools, such as blockchain analytics, to collect and assess P2P market metrics and risk mitigation solutions, risk methodologies to identify suspicious behaviour, and determine whether wallets are hosted or unhosted,30 including by engaging with programmers/developers in this space

Rather than providing an explicit direction on how to address risks resulting from P2P transfers, the FATF outlines potential risk-mitigating steps that countries and VASPs can consider to address them. In terms of the risk mitigants that countries have at their disposal, they range from the extreme of effectively preventing VASPs from accepting transfers from unhosted wallets through to a number of increased controls or additional checks that the countries may decide to require of VASPs dealing with unhosted wallets;

(106)

countries may consider and implement as appropriate options to mitigate these risks at a national level. These measures may include:

a. controls that facilitate visibility of P2P activity and/or VA activity crossing between obliged entities and non-obliged entities (these controls could include VA equivalents to currency transaction reports or a record-keeping rule relating to such transfers);

b. ongoing risk-based enhanced supervision of VASPs and entities operating in the VA space with a specific focus on unhosted wallet transactions (e.g., on-site and off-site supervision to confirm whether a VASP has complied with the regulations in place concerning these transactions);

c. obliging VASPs to facilitate transactions only to/from addresses/sources that have been deemed acceptable in line with their RBA;

d. obliging VASPs to facilitate transactions only to/from VASPs and other obliged entities;

e. placing additional AML/CFT requirements on VASPs that allow transactions to/from non-obliged entities (e.g., enhanced recordkeeping requirements, EDD requirements);

f. guidance highlighting the importance of VASPs applying a RBA to dealing with customers that engage in, or facilitate, P2P transactions, supported by risk assessment, indicators or typologies publications where appropriate; and

g. issuing public guidance and advisories and conducting information campaigns to raise awareness of risks posed by P2P transactions (e.g., accounting for specific risks posed by P2P transactions through the assessment of specific users, patterns of observed conduct, local and regional risks, and information from regulators and law enforcement).

The paper also lists measures that VASPs can consider to address risks in transfers to/from unhosted wallets. Similarly to the measure available for countries, they also include de-risking through the exclusion of such transfers;

(277)

If VASPs assess the risks of transfers to/from unhosted wallets to be unacceptably high, the VASPs may consider choosing to subject such wallets to enhanced monitoring or to limit or not accept transactions with such wallets

Those VASPs deciding to continue transfers to/from unhosted wallets are encouraged to have the relevant Risk-Based Approach measures around such transfers (see also under the Travel Rule).

What are other important takeaways for crypto businesses?

Although the updates in the Guidance focus on the aforementioned 6 areas, there are many additional aspects that warrant notice.

First of all, throughout the whole Guidance, the Risk-Based Approach seems to be reiterated, both in terms of VASP obligations as well as in terms of the financial sector assessing the risks when dealing with VASPs. The language explicitly calls not to automatically de-risk the virtual asset sector by avoiding the risks (i.e. not transacting with VA-related businesses). At the same time, there are many extracts that list out and indicate inherent increases risks in VA scenarios. Reading the Guidance, the FATF appears to be saying 'VAs are not automatically high risk', simultaneously explaining multiple reasons why they do constitute increased risks as well as providing potential mitigants for the risks. Such a Risk-Based Approach is nothing new in the AML regulatory aspect and actually gives plenty of flexibility for businesses, but it must be exercised cautiously with the spirit of RBA.

(31)

Different entities within a sector may pose a higher or lower risk depending on a variety of factors, including products, services, customers, geography, business models and the strength of the entity's compliance program.

FATF does not support the wholesale and indiscriminate termination or restriction of business relationships with a particular sector (e.g., FIs terminating relationships with all VASPs regardless of the different risk profile among them)

Secondly, there appears to be an increased focus on countries with weak AML controls for VAs, which again does not come as a surprise given the results of the state of countries' VA framework implementation reported in the 2nd 12 Month Review in July 2021. Both VASPs and nation-states are encouraged to introduce measures addressing this, for example through treating VASPs from countries with weak AML standards as presenting increased AML risks;

(107)

In addition to P2P transactions, the FATF has identified other potential risks which may require further action, including; VASPs located in jurisdictions with weak or non-existent AML/CFT frameworks (which have not properly implemented AML/CFT preventive measures) and VAs with decentralised governance structures (which may not include an intermediary that could apply AML/CFT measures). These risks may require countries or

VASPs to identify VASP- or country-specific risks and implement specific safeguards for transactions that have a nexus to VASPs and countries lacking in regulation, supervision, or appropriate controls based on these risks

(137)

Furthermore, subject to their own discretion, countries may also consider designating all VASPs from countries which do not effectively implement licensing or registration requirements as higher risk, so that for a VASP to deal with a counterpart in a country without an effective licensing regime is designated high risk activity by the supervisor and may incur additional reporting requirements

Next, the Guidance reiterates how to understand thresholds below which countries may choose not to require VASPs to conduct due diligence. They apply to 'occasional' transactions rather than more consistent/ non-occasional transactions. Coinfirm particularly welcomes that clarification. Throughout our regular 'Know Your VASP' checks we have repeatedly concluded that some VASPs apply thresholds for KYC requirements regardless of the number of transactions, which poses a question of how the 'occasional' character of such relationships have been determined.

(152)

[...] countries may therefore go further than what Recommendation 10 requires by requiring CDD for VA transfers or transactions performed by VASPs (as well as other obliged entities, such as banks that engage in VA activities), including "occasional transactions", at a threshold below the USD/EUR 1 000 threshold, in line with their national legal frameworks. Such an approach is consistent with the RBA set out in Recommendation 1, provided that it is justified on the basis of the country's assessment of risks (e.g., through the identification of higher risks). Additionally, jurisdictions, in establishing their regulatory and supervisory regimes, should consider how the VASP can determine and ensure that the transactions are in fact only conducted on a one-off or occasional basis rather than a more consistent (i.e., non-occasional) basis. In determining what approach to take for occasional transactions, countries should take into account the product and services provided by VASPs in their jurisdiction. Countries may request VASPs to identify low risk, one-off VA transfers where the VASPs are able to accept the residual risk to inform the country's approach to occasional transactions in the VA space. [...]

Another element worth noticing is the guidance elaborating on Enhanced Due Diligence (EDD) measures that can be applied for higher risk scenarios specifically in virtual assets (alongside typical EDD measures known from fiat DD). Naturally, the use of blockchain analytics is listed as one of them;

(156)

In these and other cases, the EDD measures that may mitigate the potentially higher risks associated with the aforementioned factors include:

a. corroborating the identity information received from the customer, such as a national identity number, with information in third-party databases or other reliable sources;

b. potentially tracing the customer's IP address;

c. the use of analysis products, such as blockchain analytics and

d. searching the Internet for corroborating activity information consistent with the customer's transaction profile, provided that the data collection is in line with national privacy legislation.

Download the FATF's Updated Guidance for a Risk-Based Approach: VAs and VASPs

To finish the summary, we will quote yet another extract relating to the Risk-Based Approach and its implications. The regulators, banks and others in the VA industry are reminded of the fact that isolated incidents involving illicit funds do not invalidate the integrity of VASPs' AML controls. Traditional financial institutions have had fallings in their AML controls and similar cases are bound to occur in the VASP space. At the same time, VASPs are reminded that a Risk-Based Approach does not mean they are exempt from AML controls. A 'tick box' approach of formulating an AML program – but not exercising it, is not an option – neither is claiming that KYC obligations are met if the thresholds for KYC checks begin from <1 BTC deposits. As we are seeing the industry mature, we hope to see the traditional and VA sectors meeting halfway, with banks welcoming VASPs as customers and VASPs continuously strengthening their controls.

(241)

241. It is also important that competent authorities acknowledge that in a risk-based regime, not all VASPs will adopt identical AML/CFT controls and that single, unwitting and isolated incidents involving the transfer or exchange of illicit proceeds do not necessarily invalidate the integrity of a VASP's AML/CFT controls. On the other hand, VASPs should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls.

coinfirm

Founded in 2016, Coinfirm is the world leader in blockchain analytics and regulatory technology ('RegTech') solutions. The company specializes in blockchain AML ('Anti-Money laundering') services and fraud investigations and offers the industry's largest blockchain coverage, supporting 5,600+ crypto assets including Bitcoin and the ERC-20 standard.

Coinfirm's solutions are used by market leaders globally, ranging from crypto exchanges such as Binance, and protocols like XRP, to major financial institutions and governments.

In addition to the AML Platform, Coinfirm is the first to offer an AML compliance solution to DeFi in the form of AML risk assessments of Liquidity Pool. .

Headquartered in London, UK, Coinfirm retains Warsaw and Torun offices in Poland, and Tokyo, Japan. Over 250 entities have trusted the company to provide RegTech solutions to stay in compliance with the Financial Action Task Force guidance.

Since 2016 Coinfirm has been Powering the Mass Adoption of Blockchain through Data-Enabled Intelligence

AML Platform
by coinfirm

AML for Cryptocurrency

Visit us: **www.coinfirm.com**

Message us: **marketing@coinfirm.com**

@Coinfirm **@Coinfirm_io** **@Coinfirm.io**