Practical Law™

Lucy Frew FinTech column: April 2021

by Lucy Frew, Partner, Regulatory & Risk Advisory Practice Group, Walkers

Status: **Published on 30-Apr-2021** | Jurisdiction: **United Kingdom**

This document is published by Practical Law and can be found at: **uk.practicallaw.tr.com/w-030-3053**
Request a free trial and demonstration at: **uk.practicallaw.tr.com/about/freetrial**

Lucy Frew is a Partner in Walkers' Regulatory & Risk Advisory Practice Group.

In this edition of her column, Lucy considers the public consultation on revisions to the Financial Action Task Force (FATF) guidance on a risk-based approach to virtual assets (VAs) and virtual asset service providers (VASPs) published on 19 March 2021 (Guidance), less than two years after it was originally introduced. She also considers the Kalifa Review of UK FinTech published by HM Treasury on 26 February 2021.

FATF Guidance

The FATF originally published its guidance on a risk-based approach to virtual assets (VAs) and virtual asset service providers (VASPs) in June 2019 (Guidance). Since then, it has been monitoring developments closely and has identified gaps that need to be closed. In its March 2021 consultation, the FATF proposes significant revisions to the Guidance. Many of the proposed revisions target decentralised networks, unhosted wallets and pseudonymous transactions. These characteristics are central to the virtual assets, but traditional financial regulation is ill-equipped to deal with them and the FATF has doubtless been grappling with what its approach should be. The FATF's proposed revisions to the Guidance are set to alter the landscape dramatically.

One of the challenges the FATF has faced is that traditional financial regulation is dependent on there being an identifiable person for regulators to supervise and take enforcement action against, ideally in the regulator's jurisdiction. Identifying such a person using traditional criteria may not work for decentralised models.

In addition, traditional measures to prevent money laundering, terrorism and proliferation financing and enforce international sanctions are dependent on being able to identify and verify the identity of customers and counterparties. To date, FATF is not aware of any technically proven means of identifying the person that manages or owns an unhosted (that is, private) wallet, precisely and accurately in all circumstances.

The FATF's proposed revisions seek to address these issues by requiring countries to:

- Drastically broaden the scope of virtual asset regulation.
- Identify legal or natural persons or groups of legal or natural persons who can be held responsible for decentralised networks.
- Make it much more difficult for financial institutions (FIs) and regulated VASP to deal with unhosted wallets and other unregulated persons and those in countries that have not implemented virtual assets legislation.
- Potentially treat all VA transactions as high risk.
- Apply the "travel rule" to VASPs, even where the transfer is to or from an unhosted wallet.

Scope: changes to VA and VASP definitions

The FATF now aims to clarify the definitions of VAs and VASPs, to make clear that these definitions are wide enough to ensure all relevant assets are covered by the FATF standards, either as virtual assets or as traditional financial assets. The FATF says that the expansiveness of these definitions represents a conscious choice on its part.

In particular, the owner(s) or operator(s) of a decentralised or distributed platform or application (that is, a software program) is likely to be a VASP on the basis that they are conducting the exchange or transfer of VAs as a business on behalf of a customer. Other VA services or business models potentially constituting exchange or transfer activities within the VASP definition include order-book exchange services, advanced trading services, VA escrow services and brokerage services that facilitate the issuance and trading of VAs.

The FATF standards do not apply to underlying software or technology, nor to its writing or development. However, pursuant to the proposed revised guidance, a party

directing the creation and development of the software or platform and launching it to provide financial services for profit is likely to qualify as a VASP. The FATF does not seek to capture the types of closed-loop items (for example, airline miles, credit card awards, or similar loyalty program rewards or points) that are non-transferable, non-exchangeable and non-fungible. However, non-fungible tokens (such as those representing real estate or works of art) may be VASPs if transferred on a secondary market. The FATF categorises central bank-issued digital currencies (CBDCs) as fiat currency, not as VAs.

Helpfully, the FATF makes clear that it does not intend for an asset to be both a VA and a traditional financial asset at the same time. Also, the definition of VASP only applies to entities "not covered elsewhere under the Recommendations", so VASPs should not be required to comply with both VA and traditional regulatory regimes simultaneously or, at least, not in the same jurisdiction.

The FATF also makes clear that, in determining how the definition of VASP applies, it is the facts and circumstances underlying an asset, activity or service that will determine the categorisation, rather than any labels or terminology used by market participants. In other words, regulators should focus on substance, not marketing descriptions. Regulators are likely to need significant expertise to police the perimeter, which may not be easy to come by given high private sector demand for talent and limited supply.

Identification of a regulatory target

According to the proposed revised Guidance, the decentralisation of any individual element of operations does not eliminate VASP coverage if the elements of any part of the VASP definition remain in place. When there is a need to evaluate a business model to identify a VASP, the FATF expects regulators to identify 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 possesses and controls the data on its operations, and who could shut down the product or service. The FATF is keen to ensure that one or more legal or natural persons, or groups of persons, can be held accountable.

The FATF is particularly concerned about the risks of stablecoins, particularly those with potential for mass-adoption and peer-to-peer use. It wants regulators to identify the legal or natural person(s) that drive the development and launch of stablecoins pre-release, in order to apply regulatory or supervisory action in the pre-launch phase as it may be impossible later (if, for example, the entity was dissolved at or before launch or the developer was one or more individuals). This may be easier said than done.

Unhosted wallets

Peer-to-peer transfers (between unhosted wallets) are not subject to AML/CTF obligations. Transactions to or from unhosted wallets and transactions where at an earlier stage peer to peer transactions have occurred should be considered higher risk. The FATF proposes that national regulators consider: banning or refusing to license VASPs that allow transactions to or from unhosted wallets; imposing additional requirements on those VASPs (such as enhanced recordkeeping, due diligence and more detailed risk assessments) and reporting of virtual currency transactions with unhosted wallets and/or cross-border transactions; and heightened regulatory surveillance of VASPs that enable unhosted wallet transactions.

In other words, the FATF proposes to use the regulated sector to clamp down on unregulated business. This approach has echoes of tax transparency regulation such as the US's Foreign Account Tax Compliance Act (FATCA) and the OECD's Common Reporting Standard (CRS) as implemented by countries throughout the world, which similarly used the regulated sector to extend tax authorities' reach over persons who might otherwise be beyond it.

Application of the "travel rule"

FATF's revisions to the Guidance clarify how VASPs must comply with the travel rule (a version of wire transfer requirements adapted to VAs) for all transactions, including those with unhosted wallets. The wire transfer rule imposes requirements on VASPs to obtain, hold and submit required and accurate originator and required beneficiary information. Information includes originators' and beneficiaries' accurate (verified) full names; account numbers (which in the VA context, could mean the "wallet address" of the VA and the "public key" of the customer); physical (geographical) accurate (verified) addresses, national identity numbers, customer identification numbers (so, not a transaction number) or date and place of birth.

The FATF reiterates that the required information need not be communicated as part of (or incorporated into) the transfer on the blockchain itself provided it is submitted "immediately and securely" and is available on request to appropriate authorities. The Guidance already provides examples of existing technologies that might serve as a foundation for enabling the identification of beneficiaries of VA transfers, as well as the transmission of required originator and beneficiary information, in near real-time before a VA transfer is conducted on a DLT platform. The FATF has not proposed to update the 2019 examples and this is an area where industry feedback would be particularly valuable.

Because the required information identifying the originator and beneficiary can be held separately to the VA transfer system (for example, the blockchain), the VA transfer can be completed even with such information missing or without screening the transfer to identify suspicious and prohibited transactions. VASPs should consider remediation measures: such as putting a customer wallet on hold until screening is completed and it is confirmed that no concern is raised, or arranging to receive a VA transfer with a wallet that links to a customer wallet and moving the transferred VA to their customer's wallet only after the screening is completed and if no concern is raised.

The proposed revised Guidance makes clear that a VASP needs to undertake counterparty VASP due diligence before they transmit the required information to their counterparty (although not necessarily prior to each transfer). VASPs will also be also required to maintain records, monitor transactions and report suspicious activities. The FATF says that countries should ensure both originating and beneficiary VASPs screen customers and transactions, prohibiting transactions with designated individuals and entities, and freeze assets in order to comply with their targeted financial sanctions obligations.

Countries should treat even apparently domestic VA transfers as cross-border wire transfers, given the cross-border nature of VA activities and VASP operations. Countries should also consider requiring VASPs to treat all VA transfers as higher-risk transactions that require enhanced scrutiny and limitations.

Some jurisdictions will require their VASPs to comply with the travel rule before other jurisdictions (the "sunrise issue"). This can be a challenge for VASPs 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 VASPs can require travel rule compliance from beneficiaries by contract or business practice.

A VA transfer can be directly settled on the blockchain between wallet addresses alone, without the need for an intermediary. In instances in which a VA transfer is between only one regulated entity and an unhosted wallet, countries should still ensure that the regulated entity adheres to the travel rule with respect to its customer (whether originator or the beneficiary, as the case may be). The FATF does not expect VASPs and FIs, when originating a VA transfer, to submit the required information to individuals who are not obliged entities. However, VASPs receiving a VA transfer from an unhosted wallet, should obtain the required originator and beneficiary information from their customer. This does not solve the issue of no AML/CTF controls applying to transfers between two unhosted wallets. The FATF notes that countries may choose to impose additional limitations, controls, or prohibitions on unhosted wallets.

Enhanced due diligence

Countries should consider the risk factors associated with the VA product, service, transaction, or delivery channel, including whether the activity involves pseudonymous or "anonymous transactions", "non-face-to-face business relationships or transactions", and/or "payment[s] received from unknown or un-associated third parties". The FATF says that the fact that nearly all VAs include one or more of these features or characteristics may result in countries determining that activities in this space are inherently higher risk.

The enhanced due diligence measures that may mitigate the potentially higher risks associated with the aforementioned factors include: corroborating the identity information received from the customer, such as a national identity number, with information in third-party databases or other reliable sources; potentially tracing the customer's IP address; the use of analysis products, such as blockchain analytics; and 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. Countries also should consider obtaining additional information on the customer and intended nature of the business relationship, obtaining information on the source of funds of the customer, obtaining information on the reasons for intended or performed transactions, and conducting enhanced monitoring of the relationship and transactions.

Conclusion

The FATF's consultation on its proposed revisions to the Guidance is now closed and the amendments will be made at the FATF's June 2021 meetings. While the drafting may change before publication, the broad principles are unlikely to change.

Reactions to the proposed revisions, which have ranged from seeing it as a necessary tightening up and levelling of the playing field to a stifling of innovation in favour of incumbents, are likely to be coloured by whether one is a proponent or is sceptical of the virtual assets industry. However, rightly or wrongly, it is clear that there will be significant changes to regulation in this area, with the cost of compliance that entails. What is less clear is whether the proposed revisions will be effective or simply encourage a parallel unregulated system that minimises touch points with VASPs and FIs.

The Kalifa Review of UK FinTech has rightly been applauded for its ambition and comprehensiveness. The Review's recommendations are wide-ranging but in the specific area of policy and regulation the objective is to have world-leading FinTech policy and regulation, which builds trust in the new wave of tech-enabled

products and services. It is worth considering whether its recommendations are impacted by the FATF's proposed revisions to its Guidance on the risk-based approach to VAs and VASPs.

Overall, and while the Kalifa Review is entirely supportive of FinTech, it is broadly in favour of more regulation of virtual assets, not less. It proposes that the UK should introduce a new bespoke regime for the regulation of cryptoassets and notes that this should be flexible enough to deal with future challenges, such as how decentralised finance should be regulated. The Review notes that in January 2021, HM Treasury published a consultation paper and call for evidence on the UK's regulatory approach to cryptoassets and stablecoins (as discussed in my previous column and which pre-empts the FATF's revisions to its Guidance as discussed above) and that both the initiative and the government's stated objective of considering the case for a wider regime are welcome.

The FATF's expanded scope of the definition of VASP would mean that some VASPs come into the scope of regulation for the first time. However, the Kalifa Review does include suggestions for making the PRA and FCA rules easier to navigate and search and suggests that the rules and handbooks could be digitised and made more accessible and easily navigable. The Review also suggests that regulation is "right sized" according to the nature of the business in question and the specific risks it presents. These suggestions would certainly be helpful to the FinTech sector (and, indeed, the traditional financial sector) but are not new suggestions. While the UK has flexibility on other areas of VASP regulation, it is unlikely that there will be any "right-sizing" of the areas covered by the FATF's Recommendations and the Guidance.

Both the Kalifa Review and the Guidance discussed above highlight the need for co-operation between the public and private sectors. The Guidance creates opportunities for the FinTech and RegTech sector, likely with public sector support, to offer solutions to challenges around the travel rule and identification of persons that manage or own unhosted wallets. The Kalifa Review sees the development of digital ID as one such priority area worthy of particular support, noting that as activity increasingly becomes remote and through digital channels, and against a background of increasingly sophisticated fraud and other criminal activity, a secure method of authentication is necessary to protect the link between an individual and their assets, rights and personal safety online.

Previous attempts to establish a universal approach to digital ID have met with limited success and now multiple alternatives are emerging in competition with each other to become the standard, not only in the UK but globally. The FATF's Guidance on Digital Identity discusses different approaches for digital ID but does not provide a prescription. The Review notes that encouraging progress is being made to develop a trust framework for digital ID to verify individuals by the Cabinet Office, DCMS and the Digital Identity Strategy Board. In addition, work is being done by Companies House, the Bank of England and the Global LEI Foundation to establish a basis for digital ID verification of corporates. However, the FinTech sector and, indeed, the traditional financial sector need a digital ID solution that encompasses both individual and corporate IDs. Creating different regimes in respect of the two may be a missed opportunity. The proposed revisions to the FATF AML/CTF standards require VASPs and financial services providers to understand the ownership and control of entities' and to identify and verify the identity of their individual beneficial owners, so individual and entity IDs need to be seen together. Obviously, ownership and control are not static so digital IDs must be up to date if they are to be relied on.

The Kalifa Review makes the good point that a digital ID solution should be digital-based, rather than a digital workaround that essentially mirrors paper-based approaches. This makes sense but demands a lot from regulators in terms of either technology expertise or trust. The Kalifa Review also wants the infrastructure to be attributes-based, so the technology should allow for only relevant attributes to be checked and without the attribute itself moving around on the system, thereby reducing the proliferation of confidential information and leading to better data security and traceability. It is keen that there should be no centralised pool of data, proposing instead a distributed or federated model so that data is not concentrated in one "honey pot", giving increased security and privacy. Access to data for verification purposes should be controlled and consented to by the individual and should be limited to what is truly necessary for the data recipient to have the level of assurance that they need to transact.

It will be important to ensure that digital ID can be aligned with the FATF Guidance and its Recommendations more generally.