GLOBAL DIGITAL FINANCE

20 April 2021

FATF.Publicconsultation@fatf-gafi.org

Comments of Global Digital Finance on the draft revised VASP Guide

Dear Sir / Madam,

Global Digital Finance ("GDF") is an industry membership body that promotes the adoption of best practices for virtual assets and digital finance technologies through the development of conduct standards in a shared engagement forum with market participants, policymakers, and competent authorities. We appreciate the opportunity to submit comments in response to the draft revised VASP guidance.[1]

Our response to the consultation is detailed on the following pages.

Executive Summary

- GDF members are appreciative of the additional clarifications provided by the Guidance, particularly in respect of the travel rule.
- However, there are concerns with regards to unintended consequences:
  - Discrepancies in the Level-Playing Field concepts may have unintended consequences, particularly for centralised VASPs who may face increasing regulatory burdens compared to other sectors. GDF recommends the level-playing field concept should be based on functional *and* operational equivalency
  - Parties may be classified as VASPs who may not, in fact, be responsible for AML/CFT governance of a given VA project so may face an unnecessary regulatory burden, alongside increasing responsibilities for supervisors.
  - Guidance towards countries may give rise to VA restrictions that are disproportionate or not appropriately assessed for inherent risk. Further the Guidance notes training for competent authorities and supervisors but not for national risk assessors. The consequences may stifle innovation, cause liquidity events, and limit advances towards financial inclusion - all of which would be detrimental to customers as well as technological developments in the financial ecosystem.
- Public Private Partnerships, as well as the role of Self-Regulatory Bodies (SRBs) should be encouraged to continue to foster a deep level of understanding by

[1] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-guidance-vasp.html

both policy makers and competent authorities, as well as the industry. Taking place at both national and international level, this will ensure regulation is right-fit and appropriate to mitigate AML risks whilst allowing innovation to flourish.

- The Guidance does not appear to correctly classify or document stablecoins, and as a result some amendments are requested in respect of how stablecoins, and guidance towards their oversight, is characterised.

- GDF proposes an innovative solution to shorten the travel rule sunrise period and accelerate licensing times utilising the existing GFIN global sandbox resources in the network. Within this solution VASPs could automatically be placed into a sandbox to operate as licensed or registered for a fixed period of time without penalties whilst they continue to implement a travel rule response.

- GDF also proposes a regulatory regime similar to MVTS whereby a VASP would have a primary supervisor where full licensing would apply, and supplementary registrations in host countries where the VASP has customers. Again, this would likely accelerate licensing / registration as well as travel rule implementation. This would require a level of regulatory equivalency that is briefly discussed in the following section.

- More clarity is sought on intermediary VASPs and scenarios on when Recommendation 13 would / would not apply.

Supervisory Network

- GDF is mindful that the FATF has numerous projects and cannot solely focus on VAs to the detriment of other financial service sectors that require attention.

- However, VAs and VASPs require more than a point-in-time Guidance, as their constant evolution, the evolution of the regulatory landscape, and the level of technical knowledge and expertise needed in order to effectively legislate for and supervise the sector requires an ongoing dialogue by all stakeholders.

- We believe that creation of a “supervisors’ network” in the context of the Travel Rule implementation as well as other VASP AML obligations is essential to ensure a harmonised approach that can support the goals described above.

- **If the FATF is, for whatever reasons, unable to continue to actively lead such ongoing dialogues, or would like to extend its capacity into the global VASP community, GDF would welcome the opportunity to provide support and as an independent global convener.**

- GDF currently runs a Regulator ONLY Forum with more than 25 jurisdictional regulators and global agencies. This “stewardship platform” between the global industry and regulators is designed as an “observation deck” for regulator-only purviews of codes and standards, and to enable the GDF community to respond to specific emerging regulatory priorities (e.g. DeFi, Stablecoins, etc.) through education, deeper dives, multi-bilaterals, or further consultative work with industry players.
- More details on this proposal are described in Paragraph 5.8.

We look forward to being part of a continued productive dialogue with the FATF and the private sector to ensure policy continues to foster responsible innovation in these quickly changing markets.

Yours faithfully,

The GDF Board

Areas of Focus

1a. Does the revised Guidance on the definition of VASP (paragraphs 47-79) provide more clarity on which businesses are undertaking VASP activities and are subject to the FATF Standards?

We appreciate and understand the rationale for providing an expansive interpretation of the definition of a VASP to include different entities and business models, such as for example, those involved with decentralized applications (”DApps”). Expanding the definition of a VASP is required to manage the risk of new technologies and new service providers. However, more clarity is required in certain areas in order to avoid bringing unintended players or activities within scope, to mitigate regulatory arbitrage and to achieve a level-playing field, a key principle underlying the application of the FATF Recommendations.

We also feel that some parts of the Guidance have moved aware from the “activities and operations” principles under which the FATF has defined VASPs. [2] This is particularly with reference to inclusion of “*any*” facilitator of VASP activities would serve to better align with the constants in the traditional financial system.

Further clarity would be especially welcome with regards to the definitions and application of VASP services and obligations to DApps and stablecoins. For example, a high level approach of encouraging developers and promoters of DApps to determine who should have AML/CFT obligations, would lead to a more effective implementation and application of the FATF Recommendations.

1.1 Examples of characteristics of ICOs (Box 3, Page 25)

In page 25, Box 3, the reference to *“any business which assists”* in reference to parties involved in an initial coin offering that would be considered a VASP, is extremely broad. We would like to see further clarity around the term ‘*any business which assists*’ to ensure that this is applied consistently across jurisdictions and avoid bringing within scope entities and service providers that do not carry out VASP related services and that should not have any AML/CFT obligations.

[2] https://www.fatf-gafi.org/glossary/u-z/

1.2 Paragraph 75

Paragraph 75 states:

> *"Launching a service as a business that offers a qualifying function, such as transfer of assets, may qualify an entity as a VASP even if that entity gives up control after launching it, consistent with the discussion of the lifecycle of VASPs below."*

This paragraph could have unintended consequences as it could lead to developers not being open or public about DApps or protocols developed. We believe that developers and promoters should be encouraged to openly develop the DApp or protocol. This allows a closer dialogue with other VASPs, local regulators as well as with the FATF. We propose that the paragraph is reworded as follows:

> *"Identifying responsible parties for managing AML/CFT risk should be seen as the responsibility of an entity launching a service as a business that offers a qualifying function, such as transfer of a virtual asset. If the entity does not adequately manage this, they may qualify an entity as a VASP even if that entity gives up control after launching it, consistent with the discussion of the life cycle of VASPs below."*

1.3 Paragraph 78

Paragraph 78 currently states:

> *"Secondary markets also exist in both the securities and commodities sectors for "goods and services" that are **fungible** and transferable."*

We believe this should read:

> *"Secondary markets also exist in both the securities and commodities sectors for "goods and services" that are **non-fungible** and transferable."*

1b. Is further guidance needed on how the FATF Standards apply to various business models, as stated in paragraphs 56-59?

1.4 Paragraph 56

We believe a reasonable definition of whom could constitute a VASP as outlined in Paragraph 56, matches what would be expected in a centralized VASP:

> *"Often, a DApp user must pay a fee to the DApp, which is commonly paid in VAs, for the ultimate benefit of the owner / operator / developer / community in order to develop / run / maintain the software. dApps can facilitate or conduct the exchange or transfer of VAs."*

This is a good step. However to avoid any unintended consequences there should be some additional exclusions protecting individual investors in DApp's who through participating in a DApp could come under the above definition. Paragraph 69 offers a good point to expand this with the bolded addition:

> *"Likewise, natural or legal persons that solely engage in the operation of a VA network* ***or DApp*** *and do not engage in or facilitate any of the activities or operations of a VASP on behalf of their customers (e.g., internet service providers that offer the network infrastructure, cloud service providers that offer the computing resources, and miners and validators that validate, create and broadcast blocks of transactions) are not VASPs under the FATF Standards, even if they conduct those activities as a business."*

This would ensure that individual investors are not classified as a VASP. VASPs engaging in this service on behalf of their customers with a DApp would still fall under the VASP definition.

1.5 Paragraph 57

We understand the goals of the updated definitions as applied to DApps, however in an attempt to be as broad as possible, we believe it reduces the ultimate effectiveness of the goals.

It is clear that many DApp operators or participants could come under the VASP definition, however, it is unclear who, based on the specifics of the DApp itself. The definitions in Paragraphs 56, 57, and 63 could be interpreted as covering all parties in a DApp. The language could be made clearer, stating that these should be strictly seen as guidance that needs to be applied based on the overall business model of the DApp and the individual participants.

The concept of DApps (which can vary greatly in nature) does not seem to be fully taken into consideration and needs further clarification. There may be forms where central parties conduct transfers of VAs on behalf of third parties, however, in a DApp, the owners own or control the nodes, i.e. there may be no central owner or controller.

For example, the owner/operator(s) of a DApp will likely fall under the definition of a VASP, as they are conducting the exchange or transfer of VAs as a business on behalf of a customer. The guidance could be more specific in this regard. Would a holder of a few DApp tokens be considered 'an owner'? More clarity is needed to outline what is the expectation in the case that more than one entity would fall into the VASP definition. For example, would both the owner and the business development entity need to fulfil VASP obligations?

An assumption could be made that it would suffice for one of them to cover VASP obligations, not to create overlap of responsibilities or duplication of reporting. We however appreciate that whilst it may be challenging to be explicit here, some boundaries of the definition should be given e.g. ownership or control above a certain threshold similar to what we see in Ultimate Beneficial Ownership ("UBO") guidelines.

Also in a DApp, the participants may operate in a distributed manner without a central physical party involved, i.e. the transactions are signed off by e.g. a notary node in an automated manner.

The provision that mentions '*business development service providers*', if applicable as is, would include every person providing services to the DApp. We would suggest removing this or providing more clarity on the definition of '*business development service providers*'.

Finally, the following sentence does not specify the extent of the decentralization. Also, the term '*VASP coverage*' seems isolated and is not further defined. This part rather confuses than clarifies and we would suggest removing.

> *"The decentralization of any individual element of operations does not eliminate VASP coverage if the elements of any part of the VASP definition remain in place."*

1.6 Paragraph 58(c)

We believe that Paragraph 58(c) lacks clarity on what is meant by a '*platform*' in the statement '*although a platform which is a pure-matching service for buyers and sellers of VAs and does not undertake any of the services in the definition of a VASP would not be a VASP*' and would benefit from further clarity.

1c. How should the Guidance further address the challenges in applying the definition of VASP to businesses which decentralize their operations across multiple parties?

Due to their transparency, DApps have potential benefits for both consumers and financial regulators. Many regulators have expressed strong interest in these benefits, in particular around financial stability and providing opportunities to engage more participants into the financial system, as long as existing requirements such as AML/CFT duties and customer protection are adequately handled.

Many DApps have thousands of parties performing different aspects of the underlying instrument, and applying AML/CFT duties to any person who is involved in a DApp could have unintended consequences of either stopping innovation amongst developers or forcing them underground.

GLOBAL DIGITAL FINANCE

2. What are the most effective ways to mitigate the money laundering and terrorist financing (ML/TF) risks relating to peer-to-peer transactions (i.e., VA transfers conducted without the use or involvement of a VASP or other obliged entity, such as VA transfers between two unhosted wallets) (see paragraphs 34-35 and 91-93)?

How are peer-to-peer transactions being used for ML/TF purposes and what options are available to identify how peer-to-peer transactions are being used? What role and implications (e.g., benefits) do peer-to-peer transactions and unhosted wallets have in VA ecosystems?

Recent studies demonstrate that cryptocurrencies have not been widely adopted by illicit actors[3] (p.21) and suggest that noncompliant VASPs pose the greatest money laundering risk in cryptocurrency markets as opposed to peer-to-peer transactions[4] (p.25), with money laundering far outweighing the size and scope of terrorist financing.

Several billion dollars of criminal proceeds that moved between 2011 and 2020 were analyzed and traced by blockchain analytics firm Elliptic who highlighted that:.

> "*Rather than circulating in unhosted wallets, over 90% of these illicit funds were sent to exchanges and other businesses that are already regulated. Of the small minority that remained in unhosted wallets most simply remains dormant, rather than being circulated in an "unregulated" part of the crypto ecosystem. There is no significant parallel illicit ecosystem that is enabled entirely by unhosted wallets and independent of regulated service providers.*"[5]

Most global ML/TF activity is layered via shell companies, so may be disguised as 'legitimate' activity prior to being introduced on blockchain. The challenge to accurately measure this activity is no different to the challenge posed in cash markets. To quote Nick Furneaux, "There is no such thing as cryptocrime"[6], it is simply another medium for financial criminals to move funds.

---

[3] See pg. 21 of Blockchain Association report on self hosted wallets. https://theblockchainassociation.org/wp-content/uploads/2020/11/Self-Hosted-Wallets-and-the-Future-of-Free-Societies.pdf

[4] Ibid, pg. 25

[5] https://www.elliptic.co/blog/us-treasury-unhosted-wallet-proposal-unnecessary-ineffective-counterproductive-says-elliptic

[6] https://www.grcworldforums.com/fincrime-world-forum/unlocking-crypto-crime-there-is-no-such-thing-as-crypto-currency-crime-a-presentation-by-nick-furneaux/1159.article

GLOBAL DIGITAL FINANCE

In 2017, the G-20 committed to advance financial inclusion worldwide and support the G-20 Global Partnership for Financial Inclusion (GPFI). The G-20 High Level Policy Guidelines on Digital Financial Inclusion for Youth, Women and SMEs published in 2020 states that the COVID-19 outbreak has amplified the critical need for digital access to affordable financial products for individuals to ensure continuity of access to financial services and sustaining remittance flows.

The potential that peer-to-peer transactions using self-hosted wallets have to bolster global financial inclusion is best exemplified by an examination of how these transactions might revolutionize global remittances, where just a 5% reduction in cost of global remittance would boost payments by $16bn[7].

Given the lack of economic incentive for traditional financial services firms to enter these markets, the prospect of financial inclusion hinges on practical regulation of peer-to-peer systems that does not create false barriers to entry across VA markets.

What specific options are available to countries and VASPs to mitigate the ML/TF risks posed by peer-to-peer transactions?

In true peer-to-peer, or unhosted wallet to unhosted wallet transactions (as opposed to transactions involving an "unknown" or "unnamed" wallet which does not necessarily mean an unhosted wallet), the risk of missing a ML/TF transaction does rise due to the lack of an obliged entity involved in the transaction, however recent reports indicate that the probability of ML/TF is lower[8].

It is worth noting that the FATF's 2020 12-Month Review questioned whether "the number and value" of peer-to-peer transactions is large enough to even be considered a material ML/TF risk. Notwithstanding this, the following should be considered:

Paragraph 35 states that a future without financial intermediaries could be potentially challenging to the effectiveness of the FATF Recommendations. As such, placing the onus on financial intermediaries such as VASPs to release and trace personal information from both customers and non-customers

[7] https://theblockchainassociation.org/wp-content/uploads/2020/11/Self-Hosted-Wallets-and-the-Future-of-Free-Societies.pdf, P42

[8] https://ciphertrace.com/wp-content/uploads/2021/01/CipherTrace-Cryptocurrency-Crime-and-Anti-Money-Laundering-Report-012821.pdf.

involved in any given VA transaction is not a sustainable approach to the mitigation of ML/TF peer-to-peer transactions. In the event such measures were to be introduced, illicit peer-to-peer users could easily engage with layering services prior to reaching a regulated VASP, thus encouraging money laundering activity rather than deterring it.

Blockchain technology is a powerful but underutilized forensic tool for governments to identify illicit activity and bring criminals to justice. One expert on the cryptocurrency ecosystem called blockchain technology a "boon for surveillance."[9]

If it is assumed that that illicit activity is on average two hops away from a VASP at present[10], then data analytics and blockchain forensics can benefit supervisors and law enforcement to mitigate the risks associated with ML/TF from peer-to-peer transactions.

By developing a comprehensive map of these wallets and their connections, and doing so early in the evolution of the industry, investigators could attribute identities to peer-to-peer activity over time. Using a similar clustering approach to Foley et al. (2018)[11] supervisors and law enforcement could facilitate identification of groups of illicit actors and develop leads for subpoena applications to VASPs.

Specific options available to mitigate ML/TF risks posed by peer-to-peer transactions include:

- Wallet mapping of existing unhosted wallet addresses visible on decentralized ledgers using blockchain forensic tools
- Standardising best Know-Your-Transaction (KYT) practices across blockchain forensic and crypto compliance tools
- Use of data analytics tools to identify suspicious activity and red flag indicators
- Development of reporting requirements for fiat on-ramps to unhosted wallets which may not be identified as VASPs under the guidance

---

[9] https://cryptoforinnovation.org/resources/Analysis_of_Bitcoin_in_Illicit_Finance.pdf
[10] https://ciphertrace.com/wp-content/uploads/2021/01/CipherTrace-Cryptocurrency-Crime-and-Anti-Money-Laundering-Report-012821.pdf
[11] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645

The fast-evolving technology creates barriers to entry for supervisors and law enforcement officials who may not currently have the skills to adequately investigate ML/TF in this space at present, and do not have the resources to invest in up-skilling their staff due to the cost of existing certifications. Public-private partnerships can be beneficial to both the industry and supervisors/law enforcement in order to avoid excessive demands being placed on VASPs.

Are the risk mitigation measures proposed in the Guidance in paragraphs 91-93 appropriate, sufficient and clear?

2.1 Paragraphs 91(a) and 91(b)

The risk mitigation measures proposed appear to be using a traditional lens to address the risks present across the VA ecosystem, and are a departure from the risk-based approach. Significantly, reverting to one size fits all approach to the VASP sector, in light of the data related to actual illicit finance risks described above, would likely add regulatory burden on this growing industry, and should instead have a thorough assessment of the value of the additional requirements, its costs, as well as the impacts on financial inclusion. As an illustration of this commitment, the recently passed Anti-money Laundering Act (AMLA) in the US has a mandate for such a study by US authorities over the course of the next year.

Further, the use of centralized regulation of obliged entities in a decentralised financial system ignores the availability of alternative technical solutions which are used in fields such as cybersecurity. The process of network analysis[12] is likely to be significantly more successful in identifying behavioral models across peer-to-peer transactions. A number of private sector service providers are already engaged in developing such services.

NYDFS has trialled the techsprint template[13] to develop viable public-private partnership (PPP) solutions that meet the needs of competent authorities engaged with the monitoring of VA markets. Some of the solutions presented were innovative from a regulatory perspective. This approach both promotes the relationship with local supervisors and non-VASP service providers, as well as encouraging regulatory innovation. This type of PPP may require a separate guidance note on how to best use data analytics in absence of a VASP or identifiable VA user being involved in peer-to-peer transactions that are observable on public distributed ledgers.

[12] https://www.frontiersin.org/research-topics/12966/cryptocurrency-transaction-analysis-from-a-network-perspective
[13] https://www.dfs.ny.gov/techsprint

2.2 Paragraph 91(c)

The denial of licencing to VASPs seems to guide competent authorities towards an extreme outcome; the equivalent in traditional finance would be denial of licencing to financial institutions that provide cash to customers. If this standard is to be introduced across the FATF Recommendations, most financial institutions would be unable to operate under these guidelines. Further, this recommendation would not be practical to implement as it is technically not possible to prevent a deposit and therefore a VASP could consequently have deposits on account that it can neither credit to customers nor return but nonetheless would affect its licensing having *"accepted"* such deposits.. We consider this guidance as overreach that may inappropriately guide policy-makers whilst harming the potential benefits of such initiatives as financial inclusion innovation. We therefore request this Paragraph to be removed.

2.3 Paragraphs 91(d) and 91(e)

91(d) & 91(e) are appropriate, sufficient and clear.

2.4 Paragraph 92

All components of Paragraph 92 are appropriate, however the wording "*Additional measures that countries may wish to consider…*" in 92 (a) and 92(c) could be made more forceful to demonstrate support for the industry.

New technology in the virtual asset industry can be complex and challenging to understand unless competent authorities and traditional institutions have, or have access to, the appropriate knowledge. Consideration should be given to changing the term "*may wish to consider*" to "*should introduce to*", changing this line to

> "*Additional measures that countries should introduce to assist in understanding and mitigating the risks of P2P transactions include*:"

2.5 Paragraph 93

If the challenge posed by VAs is linked to the technical challenges posed to analyze the amount of data generated by VAs and VASPs, there could be greater focus on initiatives like the Joint Working Group for InterVASP Messaging System[14], or a 'consortium approach'[15] which is in line with the

[14] https://intervasp.org/
[15] https://www.niceactimize.com/blog/aml-aml-consortium-approach-disrupting-financial-criminals-661/

decentralized nature of virtual assets. This could lead to more collaborative and harmonized international regulation. This approach is also more likely to address the risk identified in Paragraph 93 associated with jurisdictions with weak or non-existent AML/CFT regimes.

Section VI of the Guidance discusses information-sharing amongst supervisors, but it may be beneficial for the FATF to provide guidance to the effect that the countries provide the necessary regulatory environment for the industry to establish PPP arrangements and consortia that can benefit AML/CFT outcomes.

3. Does the revised Guidance in relation to the travel rule need further clarity (paragraphs 152-180 and 256-267)?

Are there issues relating to the travel rule where further guidance is needed? If so, where? Please provide any concrete proposals.

Does the description of counterparty VASP due diligence clarify expectations, while remaining technology neutral and not prescribing how VASPs must undertake this process (see paragraphs 172-177 and 261-265)?

GDF wishes to thank FATF for clarifying several areas that had caused differing views in the industry regarding the travel rule and practical implementation by a VASP.

There are still a few outstanding clarifications requested:

3.1 Further clarity required regarding the definition of an intermediary VASP

Paragraph 178 discusses the role of intermediary VASPs, stating:

> "*Similar to wire transfers between FIs, there may be VA transfer scenarios, either now or in the near-future, that involve "intermediary VASPs" or other intermediary obliged entities or FIs that facilitate VA transfers as an intermediate element in a chain of VA transfers*."

It appears from this Paragraph that the FATF has determined that these types of arrangements will emerge, but the industry is not yet clear as to why, despite footnote 36 in relation to Paragraph 147. To assist with understanding it would be helpful for the FATF to elaborate on this point and provide example transfer scenarios where intermediate VASPs may be involved and why, or how and why this scenario may emerge in the near-future.

3.2 Paragraph 147/261 Inconsistencies

The opening statements of Paragraph 147 state:

> "*To the extent that relationships in the VASP sector currently have or may in the future have characteristics similar to cross-border correspondent banking relationships, countries should implement the preventive measures set forth in Recommendation 13 to VASPs (and other obliged entities operating in the VA space) that develop such relationships*."

The final sentence of the same Paragraph states:

> *"If the relationship is not one where Recommendation 13 applies, the VASP may still need to undertake a counterparty due diligence process similar to that set out in Recommendation 13"*

Paragraph 261 then goes on to provide further information on Recommendation 13 and counterparty VASP due diligence:

> *"Although a counterparty VASP relationship may not be a correspondent banking relationship, there are similarities in the approach to counterparty due diligence which can be of assistance to VASPs. Accordingl*y, the process set out in Recommendation 13 is referenced in this Guidance."

The two sentences highlighted from Paragraph 147, and the final sentence from Paragraph 147 and that of Paragraph 261 highlighted appear somewhat contradictory and could benefit with clarification. That is; the final sentence of Paragraph 147 states that the VASP may still "need", whereas Paragraph 261 simply says Recommendation 13 "may be of assistance".

Clarification on when Recommendation 13 would apply and under what circumstances would be assistive and this may be as simple as adjusting the language in the last sentence of Paragraph 147 to reflect Paragraph 261.

3.3 Data Privacy

Paragraph 162 provides clear direction that VASPs should transmit and store the required travel rule information securely, and the clarification of storage is also helpful in this regard.

However, there remains much debate within the industry of the overlay of national privacy regulations, and how these interplay with VASPs' legal ability to collect, store, and transmit the required information. There are several references to national data privacy legislation within the Guidance (e.g. Paragraph 259) but nothing that explicitly guides a clear direction for the industry.

By way of example, an originator VASP collects, screens, stores, and transmits (i.e. collects and processes) beneficiary required information based on the information provided by their customer (the originator). In this example the VASP would not have gained explicit consent (nor would be able to be able to

obtain such consent) to collect and process the beneficiary's information which may be subject to data privacy obligations in a third country.

This aspect is a preventative factor in implementation of the travel rule as firms remain uncertain as to how they should proceed in order to also meet both travel rule and data privacy legislative requirements.. This is particularly acute where VASPs operate across multiple borders, and data privacy obligations differ from country to country.

GDF would request the FATF provide direction in this regard. If this is beyond scope of the FATF, then the inclusion of wording as follows may suffice to guide competent authorities appropriately:

> "*Countries should provide clear guidance to VASPs, both domestic and foreign, on the data privacy implications on the collection, storage and transmission of the required information.*"

3.4 Legal Entity Identifiers (LEIs)

GDF welcomes the inclusion of LEIs in Paragraph 165, particularly given that LEIs were built into the IVMS101 message format now used by the industry sector for the transfer of required information. In this regard, a stronger stance that encourages, but stops short of mandating, LEI usage may support greater adoption by VASPs which will add further support and integration into the existing financial system, as well as potentially shortening the sunrise period. An LEI will also provide consistency of information where a VASP is registered or licensed with multiple supervisors, or operates across multiple borders.

3.5 Paragraph 177 and Regulatory Sandboxes

One of the adoption issues in respect of the travel rule is that licenses may not be issued by competent authorities until travel rule solutions are implemented by a VASP, or that limiting factors may be imposed as described in Paragraph 177.

The limiting factors suggested within this Paragraph may have serious consequences were a competent authority to restrict business activities in the ways suggested in the examples. By way of example, most VASP exchanges rely on liquidity from across the market for active trading and depth of the order book (i.e. liquidity from outside the VASP). Meanwhile, VASPs providing custody require deposits and withdrawals which by their very nature will come from sources outside the VASP. In this regard, the GDF would request

GDF GLOBAL DIGITAL FINANCE

that the FATF remove these examples so as not to lead competent authorities towards implementing such practices.

Rather, GDF considers there is a more proactive option that competent authorities could adopt which will also accomplish a greater collaboration and partnership between the industry and competent authorities. That is, whether VASPs could automatically be placed into a national sandbox or international network sandboxes (GFIN[16]) that would allow them to operate as licensed or registered for a fixed period of time without penalties in respect of their travel rule implementation.

The further benefits of this approach may be to accelerate licensing regimes whilst at the same time accelerate the testing and adoption of travel rule solutions.

3.6 Paragraph 179

The final word in Paragraph 179, "*limitations*" infers that countries should consider limiting unhosted wallet transactions, with the consequence that this may drive more business underground (that is, larger transactions may simply move peer-to-peer or be split into smaller transactions across multiple exchanges), or it may result in VASPs being unable to continue with operations. When considered as a risk-based approach, a more suitable wording may be "*appropriate risk mitigations*" that will allow for the size, nature, and complexity of the individual industry sector, national risk assessment, and other factors to be considered.

3.7 Paragraph 261

Paragraph 261 highlights:

> "*This underscores the importance of implementation and suggests that VASPs will have to consider additional control measures for countries with weak implementation*"

Two concerns arise from this wording; first that countries are not adopting the FATF Recommendations for VASPs in a consistent manner or at a similar pace. This makes for challenging adoption by an industry that typically operates across borders, and yet that remains committed to comply with required laws, regulations and guidance.

[16] https://www.thegfin.com/

More importantly, against this context how is a ‘weak implementation’ to be judged and who is making this assessment? The FATF may do so over an extended period of time through mutual evaluations but this does not solve for this point in the interim. How is the industry to assess both technical and effectiveness compliance to the FATF Recommendations sufficient to determine what is a “weak implementation”?

We duly request that the wording of this sentence be revisited towards more appropriate language or be removed altogether.

4. Does the revised Guidance provide clear instruction on how FATF Standards apply to so-called stablecoins and related entities (see Boxes 1 and 4 and paragraphs 72-73, 122 and 224)?

Is the revised Guidance sufficient to mitigate the potential risks of so-called stablecoins, including the risks relating to peer-to-peer transactions?

The revised FATF Guidance is generally helpful in confirming the applicability of VASP regulations to stablecoin issuers. However, when it comes to the specific details of comparing stablecoin issuers to other VASPs, particularly for the purpose of conducting an AML/CFT risk assessment, there are several aspects of the Guidance which appear to reflect a misunderstanding of how centrally administered stablecoins function.

The following five points will address our areas of concern:

4.1 Purpose of Stablecoins (Box 1, Page 14)

It is uncontroversial that the regulation of something should never happen independently of that thing's purpose. For example, many pharmaceutical drugs are illegal in all contexts outside the purpose of the provision of health care. Similarly, assaulting another person is illegal in all contexts outside the purpose of reasonably protecting one's own life. There are many other examples. Law and regulation has a long tradition of considering the purpose of the thing or behaviour that is being regulated. This is among the most important considerations. For this reason, it is important to get this purpose right.

In the very first sentence of "Box 1", a suggestion is made that

> "*stablecoins purport to overcome the price volatility issues associated with VAs by maintaining a stable value relative to some reference asset or assets.*"

This may be an accurate description of one of the features of stablecoins, but it is certainly not the purpose of stablecoins, nor the reason they exist. Stablecoins may be more accurately characterised as follows:

> *"Stablecoins were designed to overcome challenges with cross border banking, particularly the refusal of financial institutions to onboard VASPs. They have the cost and speed advantages associated with other VAs, but overcome price volatility issues by being designed to maintain a stable value relative to some reference asset or assets."*

Against this backdrop, stablecoins have been adopted primarily for the purpose of trading and investing of virtual assets, but they have also been adopted for the purpose of general cross-border trade, albeit to a lesser degree at this time.

Pharmaceutical drugs are regulated on the basis of the purpose to which they will be used, with the approval process involving a careful consideration of the possible negative consequences that could accompany the fulfilment of that purpose. This regulatory process basically weighs the pros and cons of the public availability of a given drug. This cannot sensibly be done without first knowing what the drug's purpose is. By suggesting that the purpose of stablecoins is to address a problem with virtual assets, when in reality they were explicitly created to overcome problems with cross-border banking, the Guidance then emphasises the risks without due reference to the benefits. Returning to the pharmaceutical analogy, this might be like adjudicating a pharmaceutical drug based only on the risks it poses, without any reference to its potential medical utility.

For the competent authorities who are responsible for interpreting and implementing the FATF recommendations, it would be helpful for the Guidance to reiterate the importance of understanding the purpose of stablecoins, through engagement with industry stakeholders.

4.2 Characterization Stablecoin Issuers (Para. 72-73)

Paragraph 72 of the Guidance suggests that multiple entities in any given "*stablecoin arrangement*" could be classified as a VASP and thus also have AML/CFT obligations:

> "*For so-called stablecoins, a range of entities involved in any so-called stablecoin arrangement will have AML/CFT obligations under the revised FATF Standards. So-called stablecoins may have a central developer or a governance body. A governance body consists of one or more natural or legal persons who establish or participate in the establishment of the rules governing the stablecoin arrangement… If one or more parties have decision making authority over structures that affect the inherent value of a VA, such as changing the reserve requirements or monetary supply for a so-called stablecoin, they are likely to be VASPs as well, depending on the extent of the influence.*"

It is not clear at all why related entities other than the customer-facing entity, which collects customer data to comply with AML/CFT regulations and

conducts transfers and services, should be considered a VASP for the purpose of this Guidance. The responsibilities of a VASP concern the AML/CFT risks and controls associated with customers and counterparties in relation to the products and services being offered, as well as where these parties reside, operate and transact to and from. It is unclear why entities that perform stablecoin functions such as treasury management should be classified as a VASP as:

1. There are no comparable AML/CFT risks related to this activity;
2. Most VASP responsibilities such as performing KYC, transaction monitoring, filing SARs, record keeping, and documenting these processes are not pertinent; and
3. Registration with a local competent authority would serve no purpose with respect to transferring any information respecting AML/CFT risks.

While corporate arrangements may vary, it is likely that the entity that issues stablecoins and/or redeems those stablecoins for fiat or some other asset is the entity that should be registered as a VASP. Related companies that do not issue stablecoins or redeem stablecoins for reserve assets are unlikely to have any AML/CFT responsibilities that are enforced by competent authorities.

Where a stablecoin arrangement is such that no legal-entity exists but rather a person or persons have created a programmatic automated stablecoin issuing and redeeming system, it may be that one of the persons responsible for the project should be registered as a VASP and ensure that the stablecoin project fulfills pertinent AML/CFT responsibilities, and that as part of such a project governance, a person from the project is nominated.

Like many businesses, especially within the traditional financial services sector, stablecoin issuers may use segregated corporate structures which break up the compliance, technological, and treasury functions. In our view, it should only be necessary for the legal entity which performs compliance functions to be classified as a VASP and be registered with a competent authority. This would allow:

1. For all customers to be verified;
2. For all customers, transfers and counterparties to be risk rated;
3. For SARs to be filed when appropriate and by the appropriately proscribed entity;

4. For these processes to be documented; and
5. For relevant information to be transferred between VASPs or competent authorities and for all other relevant FATF Recommendations to be observed.

Requiring other persons or entities to register as VASPs may then lead to a consequential impact on competent authorities' resources having to process such registrations, as well for the stablecoin project participants having to fulfil registration requirements but not having AML/CFT commitments beyond registration.

Relatedly, in Paragraph 46, the revised Guidance appears to suggest that stablecoins could be classified as securities for the purpose of applying the FATF Standards:

> "*The FATF reaffirms previous statements that a so-called stablecoin is covered by the Standards as a VA or as a traditional financial asset (e.g., a security).*"

This text may have the consequence that the Guidance may lead countries towards viewing stablecoins as a security which may not necessarily be accurate without appropriate assessment. We respectfully request that the FATF remove "*(e.g, a security)*" from the text to allow for countries to assess and qualify each stablecoin project on its own merits.

4.3 "Stabilization Mechanism" (Para. 122)

The revised Guidance distinguishes stablecoins from other virtual assets based on the existence of a "*stabilization mechanism*", and makes reference to the ML/TF risks associated with this mechanism:

> "*As previously noted, the distinguishing technical feature of so-called stablecoins is a stabilization mechanism. An assessment of the ML/TF risks and mitigation of the risks associated with this mechanism should form part of the licensing and registration process.*"

While we certainly agree that the distinguishing feature of stablecoins can be accurately described as a "*stabilization mechanism*", the revised Guidance uses language that appears to reflect a misinterpretation of how this process works in the context of currently operational and prominent centrally-administered stablecoins. Since the Guidance requires that the "*stabilization mechanism*" be considered when performing an assessment of

the risks associated with stablecoins, we believe it is important that this mechanism is adequately explained and understood. The following points will resolve the apparent confusion surrounding this concept:

1. The Guidance describes the stabilization mechanism as a "*technical feature*" of stablecoins. This might be an accurate way to describe the "*stabilization mechanism*" of "*algorithm-backed*" stablecoins, but the stabilization mechanism of currently operational and prominent centrally-administered stablecoins should be viewed as a non-technical feature. This is not a matter of semantics: the stabilization mechanism of currently operational and prominent centrally-administered stablecoins is the product's only meaningful non-technical feature. Technology is undoubtedly involved, but the "*stabilization mechanism*" itself is not a mechanical process or set of rules, but rather a system of market-driven incentives that is generally known as "*market-based price discovery*". This is not a mechanical or technological process, but rather a combination of business design and knowledge of how humans respond to incentives.

   The "*stabilization mechanism*" of currently operational and prominent centrally administered stablecoins is best described by considering its two parts:

   A. the ability to be issued and to redeem tokens from the issuer (Primary Market), and

   B. a decentralized, market-based system of incentives (Secondary Market).

   Strictly speaking, it is interactions between Primary and Secondary markets that keep prices stable in these latter markets, with the issuer's peg being what keeps prices stable in the Primary Market. The Secondary Markets are where most trading occurs, but what keeps prices stable in these markets is the independent participation by Primary Market participants, who are incentivised to seek arbitrage profits. This feature, a system of market-based incentives that is indifferent to who interprets and acts upon them, cannot be considered "*technical*". It is the only important non-technical feature.

   In this regard, we request that FATF considers amending Paragraph 122 to read,

> *"As previously noted, a distinguishing feature of stablecoins can be a technical stabilization mechanism. Supervisors should be especially cautious of claims that so-called stablecoins involve no entity that qualifies as a VASP. As discussed in the FATF report to the G20, so-called stablecoins may also be more likely to reach mass adoption by the public as compared to some VAs in jurisdictions where financial services are less sophisticated, which could potentially greatly increase the risks they pose if realized. Therefore, where mass adoption is evident, mass adoption should be included as a factor meriting consideration in assessing the AML/CFT risks of a stablecoin issuer when a stablecoin issuer undergoes its regulatory testing. As a general matter, however, the AML/CFT aspects of licensing or registration procedure for VASPs and obliged entities launching, or involved in, so-called stablecoins should be similar to that for VAs ."*

2. The Guidance uses language to describe the stabilization mechanism that reflects a misunderstanding of its decentralized nature: (Para 72)

   > "*A governance body [for so-called stablecoins] consists of one or more natural or legal persons who establish or participate in the establishment of the rules governing the stablecoin arrangement… They may also carry out the basic functions of the stablecoin arrangement (such as managing the stabilization function) or this may be delegated to other entities*."

   Only prices in the Primary Market can be said to be "*managed*" by the stablecoin issuer (by processing issuances and redemptions at the pegged rate). But most trading occurs in Secondary Markets, where prices are kept stable by the arbitrage activity of Primary Market participants. This is neither a "*managed*" nor "*delegated*" process. It is a decentralized process that can be carried out by anyone who can participate in both markets (users who are KYC-verified with the issuer and thus can participate in the Primary, as well as Secondary markets). Importantly, there is neither coercion nor contractual reliance on any single Primary Market participant. To illustrate, if the largest Primary Market participants of a currently operational and prominent centrally-administered stablecoin issuer suddenly disappeared, the "*stabilization mechanism*" would only be temporarily affected: new

entrants would be incentivised to quickly enter the market based on the prospect of available arbitrage profits.

The Guidance describes the "*stabilization mechanism*" as though it were a technology or a centralised administrative procedure, but only the Primary Market can be described in this way. In Secondary Markets, which are several orders of magnitude more active, the "*stabilization mechanism*" is a decentralized process that is carried out exclusively by KYC-verified Primary Market participants. But since the issuer is indifferent to which verified Primary Market participant works to stabilize prices in Secondary Markets, this process cannot be said to be "*delegated*" or "*managed*".

We dutifully request that the FATF amend Paragraph 72 to read:

> *"For so-called stablecoins, a range of the entities involved in any so-called stablecoin arrangement may have AML/CFT obligations under the revised FATF Standards. So-called stablecoins may have a central developer or governance body. A governance body consists of one or more natural or legal persons who establish or participate in the establishment of the rules governing the stablecoin arrangement (e.g., determine the functions of the so-called stablecoin, who can access the arrangement and whether AML/CFT preventive measures are built into the arrangement). They may also carry out the basic functions of the stablecoin arrangement (such as managing the stabilization function) or this may be delegated to other entities. They may also manage the integration of the so-called stablecoin into telecommunications platforms or promote adherence to common rules across the stablecoin arrangement. A legal person who constitutes the governance body could also be a VASP if it is also the legal entity that issues stablecoins and redeems those stablecoins for reserve assets. Where no legal entity is established and a natural or natural persons manage the stabilization and issuance of stablecoins and the redemption of stablecoins for reserve assets, a legal person must become responsible for registering as a VASP and executing the responsibilities of a VASP."*

3. The Guidance again references the need to consider the "*stabilisation mechanism*" in Paragraph 122:

> *"As a general matter, however, the AML/CFT aspects of licensing or registration procedure for VASPs and obligated entities launching, or involved in, so-called stablecoins should be similar to that for VAs, except for the need to consider the stabilization mechanism."*

As mentioned, the "*stabilization mechanism*" in the context of currently operational and prominent centrally administered stablecoins is best captured by the market activity of Primary Market participants. Since these users must all be KYC verified by the stablecoin issuer, this aspect of centralized stablecoins is already fully covered by existing AML/CFT laws. As such, the "*stabilization mechanism*" of centrally administered stablecoins does not require any special attention or additional consideration by competent authorities who are working to address AML/CFT concerns. The reserve assets held by stablecoin issuers are analogous to those held by other VASPs. If anything they would be safer, due to the lower proportion of virtual assets, and higher proportion of fiat assets, being held by the stablecoin issuer. As well, many stablecoin issuers offer varying examples of transparency of their reserves that no other VASP or financial institution offers.

In this regard, we request that the FATF amend the last sentence of Paragraph 122 to read:

> *"As a general matter, however, the AML/CFT aspects of licensing or registration procedure for VASPs and obligated entities launching, or involved in, so-called stablecoins should be similar to that for VAs."*

4.4 Risk Assessment of Stablecoins (Para. 224 & Box 4)

The Guidance suggests that stablecoins may pose a higher risk than other virtual assets, but it is unclear as to why this might be the case:

> "*Like other VAs, assessment of their risks should form part of this process, and so-called stablecoins may tend to pose higher risks, according to the judgement of supervisors, with attendant consequences for the type and intensity of supervision*."

The only explanation offered for this heightened risk is the prospect of widespread adoption. While we agree with the general concept that should risk exist, it would be greater with more widespread adoption, this reasoning cannot substitute for an analysis and description of the risk itself. In the

context of AML/CFT, there is insufficient data regarding stablecoins that would cause them to pose any greater risk than other virtual assets. The Guidance acknowledges that the stabilisation mechanism is the distinguishing feature of stablecoins but, as explained above, there are no additional AML/CFT concerns associated with this characteristic.

If FATF meant that stablecoins, like other VAs, pose higher risks than other financial instruments such as cash, then it is recommended that the point is clarified. In this regard, we recommended that FATF amend Paragraph 224 to read,

> *"VASPs or FIs involved in so-called stablecoins, should be supervised in the same manner as VAs or traditional financial assets as appropriate. Like other VAs, assessment of their risks should form part of this process, and so-called stablecoins may tend to the same risks as other VAs, according to the judgement of supervisors, with attendant consequences for the type and intensity of supervision. If a given so-called stablecoin qualifies as a traditional financial asset, it should be supervised according to that determination in the same manner as all other similarly categorized assets. Given the cross-border nature of VA transfers, international cooperation of VASP supervisors is very important."*

Stablecoin issuer risks respecting AML/CFT are best mitigated by individual jurisdictions using a risk based approach: creating more controls only when warranted by the risks posed by stablecoin issuers. We believe that proposing regulations for all stablecoins based on the hypothetical business model in box 4 is an incomplete approach, and that more consideration should be given to stablecoin business models as they exist today. It is recommended that FATF amend the last Paragraph in Box 4 to include the last sentence in the following:

> *"It is important to note that the exact details of any arrangement must receive prior adequate and independent scrutiny to make these determinations and the exact application of AML/CFT measures will depend on each individual country. It is also recognized that not all stablecoin projects are organized as this example and may have different use cases ..."*

4.5 "Is the revised Guidance sufficient to mitigate the potential risks of so-called stablecoins, including the risks relating to peer-to-peer transactions?"

Our position is that the risks of stablecoins and their issuers are analogous to the risks of VAs and other VASPs, and that prior guidance was already sufficient to mitigate these potential risks. New recommendations by FATF necessitate an updated risk assessment of this sector. As for the risks related to per-to-peer transactions, please refer to our response to Question 2 above.

5. Are there any further comments and specific proposals to make the revised Guidance more useful to promote the effective implementation of FATF Standards?

5.1 Self Regulatory Bodies

Paragraphs 5 and 125 state that:

> "*VASPs should be supervised or monitored by a competent authority, not a self-regulatory body (SRB)*"

Whilst we agree with this statement in principle, we also believe SRBs have demonstrated that they have an important role to play in both the traditional and virtual asset ecosystem; two examples being the JVCEA in Japan, and FINRA in the United States. It would be helpful for the FATF to provide examples of the way in which SRBs *can* support competent authorities. Examples may include:

- Reinforcing the establishment and growth of regulatory sandboxes for the innovation, testing and deployment of regulatory technologies alongside regulatory oversight.
- Providing rapid technical input to the competent authority to augment the authority's own internal knowledge with emerging technologies and AML/CFT risk.
- Providing initial screening of VASP licensing applications for completeness and accuracy ahead of filing with the competent authority.
- Ensuring firms adhere to standards set by competent authorities (e.g. marketing standards, certified training for staff, etc.), and report failures to the competent authority.
- Providing input to the competent authority where important industry or individual VASP information comes to light that the authority is unaware of.
- Providing an initial point of contact for customer complaints

5.2 Level Playing Field

In Paragraph 22(c), the level playing field principle appears to be at odds with the discussion on initial risk assessments discussed in Paragraph 28. Paragraph 22(c) suggests:

> "*Countries and their competent authorities should treat all VASPs, regardless of business model, on an equal footing from a regulatory*

> *and supervisory perspective when they provide fundamentally similar services.*"

Therefore, countries should "*subject VASPs to AML/CFT requirements that are functionally equivalent to other entities when they offer similar products and services with similar risks and based on the activities in which the entities engage*." Meanwhile, Paragraph 28 states that

> "*the overall risk at a national level should be determined by individual jurisdictions through an assessment of the … VASP sector. 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*."

Paragraph 28 appears to be in line with FATF Guidance on Risk-Based Supervision which states that

> *"Supervisors should ensure that their supervisory strategies are kept under regular review."* [17]

In attempting to level the playing field in Paragraph 22(c) and similarly in Paragraph 112, this creates a policy approach that may lead to regulatory overreach and unnecessary / unintended compliance burden for centralised VASPs which may operate more akin to MVTS providers and should be treated to a similar regulatory regime.

Further, within the Guidance different recommendations and risk ratings are provided for stablecoins, despite the fact that centralised stablecoins employ business models that are, from a risk perspective, essentially equivalent to other centralised VASPs, particularly exchanges. Both businesses hold reserve assets that are continually being deposited and withdrawn by users. Both businesses keep fiat reserves available for customer withdrawals or trading, and the customers trust both types of businesses to execute their transactions.

We respectfully urge the FATF to separate out guidance, and provide a direction for countries to appropriately differentiate and assess the risks between centralised and decentralised VASPs on the basis of functional *and* operational equivalency, and that countries should make determinations and regulation in regards to each as separate operating models and the risks that each pose.

[17] Paragraph 76, http://www.fatf-gafi.org/media/fatf/documents/Risk-Based-Approach-Supervisors.pdf

5.3 Cross Border Service Provision

Paragraph 26 in the Guidance on the Risk Based Approach to MTVS [18] states:

> *"Some MVTS providers provide services across national borders through establishments, including through a network of agents operating in another country. Competent authorities of the MVTS provider, acting across national borders with a physical presence through one or several agents established in another country (home country licensing/registration competent authorities), should liaise with the MVTS's host authorities to ensure any ML/TF concerns are adequately addressed [Through applicable passport mechanisms]."*

and further states:

> *"This is without prejudice to supranational rules that would enable MVTS providers to supply services throughout the supranational jurisdiction on the basis of the legislation prevailing in the countries in which they are situated, without requiring from the host country to impose licensing or registration obligations on entities situated in another country and providing cross-border services."*

The above text provides policy support for a regulatory regime where an MVTS can rely upon VASP licensing in the country in which it is created, and be subject to supervision by a primary supervisor. Centralised VASPs in particular are not dissimilar to MVTS in terms of organisational structure and cross-border reach, with domestic customer bases in host countries often not sufficient to warrant a full licensing regime across every host country. This would currently result in some countries being isolated from such innovative technology, particularly in developing countries where such technology may broadly assist with financial inclusion and other economic benefits.

We therefore urge the FATF to consider providing such text within the guidance that would enable countries to take a similar approach as those found in Paragraph 26 of the MTVS guidance. Mention is briefly made of a Primary Supervisor concept (Page 94, Paragraph 17) with regards to information exchange and it would be beneficial to see this concept extended to licensing and registration regimes as well. We believe that such an option would see a faster adoption of compliance requirements, and in particular acceleration of travel rule adoption.

[18] https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf

Further, in Paragraph 119, the Guidance lists a number of suggested requirements that could be imposed on VASPs seeking licensing or registration, "*on the basis of risk*":

> "*Such conditions could potentially include, depending on the size and nature of the VASP activities, requiring a resident executive director, substantive management presence, specific financial requirements and/or requirements for VASPs to disclose the registration(s)/license(s) which they hold in marketing materials, website and mobile applications.*"

We believe that there is a potential unintended consequence within this text; that countries may rush to implement such controls without fully undertaking a thorough and informed risk assessment that would then warrant such risk mitigations. This may lead to over-regulation, stifling the industry, and potentially preventing positive developments that may result.

As highlighted above, many VASPs may not be able to generate sufficient customer numbers or liquidity in a single country to support substantial substance and financial requirements, and therefore the risks they pose within a country may be low.

Therefore, we urge the FATF to either withdraw the text highlighted above, or as a minimum to provide a stronger emphasis that such conditions should be imposed only after a thorough and informed risk assessment has taken place. Further, that such conditions should be considered on the basis of thresholds (e.g. turnover, customer numbers in a country, etc.).

5.4 Classification of VAs

Paragraph 44 states

> "*There may however be instances where the same asset will be classified differently under different national frameworks or the same asset might be regulated under multiple different categorizations*"

It is recognised that a complete cross-jurisdictional approach to VA classification is impossible; however countries should give consideration to how a VA is classified in other countries in order to make a fully informed choice on their categorisation. This is particularly important in the context of potential regulatory arbitrage, mentioned a few places elsewhere in the Guidance and has recently become apparent with comparison of proposed

asset categorization between the European Commission's Regulation of Markets in Crypto-assets (MiCA) and the UK proposed approach.

5.5 Training

Although Training is covered in Paragraphs 229-231 of the Guidance, we believe that the Guidance should also explicitly mention that appropriately trained and qualified staff should provide input to the National Risk Assessment to ensure that VASP regulatory frameworks are proportionate to the identified risks at a country level. That is to say, experts with deep domain knowledge in the different virtual asset business models, and how they might be exploited by bad actors.

5.6 Prohibition

Paragraphs 94 and 95 provide guidance to countries that may seek to prohibit virtual assets. We believe that with the fast growth and maturity of VAs, any risk assessment that leads to prohibition may become outdated rapidly at the disadvantage of residents of such a country. We would therefore welcome such language that guides such countries towards performing risk assessments more frequently based on latest available data in order to reaffirm any decisions in relation to prohibition of virtual assets.

5.7 Iterative Revision

As the FATF and policy makers appreciate, the industry continues to evolve rapidly, with new business models, technologies, and data becoming available on a continuous basis. As such, it is unlikely that this Guidance will stand the test of time, as it may do in the traditional financial sector which is transforming at a slower pace.

We would urge the FATF membership to continue ongoing engagement with the industry through bodies such as GDF, and in particular to consider an iterative update to the Guidance as deemed necessary when the content appears to no longer be relevant, or has been superseded by industry developments, technological developments, or data / evidence upon which the Guidance is based.

5.8 Supervisors' Network

With regards to the concept of a primary supervisor raised in Paragraph 5.3 as well comments on interactive revision and ongoing engagement with the industry highlighted in Paragraph 5.7, GDF is mindful that the FATF has

numerous projects and cannot solely focus on VAs to the detriment of other financial service sectors that require attention.

However, and as highlighted earlier, VAs and VASPs require more than a point-in-time Guidance, as their constant evolution, the evolution of the regulatory landscape, and the level of technical knowledge and expertise needed in order to effectively legislate for and supervise the sector requires an ongoing dialogue; both public-public and public-private.

If the FATF is, for whatever reasons, unable to continue to actively lead such ongoing dialogues, or would like to extend its capacity into the global VASP community, GDF would welcome the opportunity to provide support and as an independent global convener. GDF currently runs a regulatory ONLY forum with more than 25 jurisdictional regulators and global agencies. This "stewardship platform" between the global industry and regulators is designed as an "observation deck" for regulator-only purviews of codes and standards, and to enable the GDF community to respond to specific emerging regulatory priorities (e.g. DeFi, Stablecoins, etc.) through education, deeper dives, multi-bilaterals, or further consultative work with industry players.

GDF offers access at the community membership level at no cost to individuals of firms in the global VASP community to participate in open working groups and community events. Attesting to GDF Codes requires a minimum registration fee and only paying members can lead working groups.

The proposed GDF role as convener could take the form of closed-door AML/CFT supervisor discussions (similar to regulatory forums that GDF already convenes) as well as public-private forums to bring supervisors and the industry together. In this construct, FATF could continue to act as an observer, and where necessary then feed back to the membership on updates, challenges, and so forth.

We believe that the establishment of a "supervisors' network" in the context of the Travel Rule implementation as well as other VASP AML obligations is essential to ensure a harmonised approach that can accelerate adoption and understanding, and also remove the risks of regulatory arbitrage, through providing regular engagement dialogues, shared knowledge and tools and support.