GLOBAL
DIGITAL
FINANCE

July 5, 2019

VIA EMAIL:

amlcft_consult@mas.gov.sg

PS AML/CFT Notices Consultation
Anti-Money Laundering Department
Monetary Authority of Singapore
10 Shenton Way, MAS Building
Singapore 079117

Re: Consultation regarding the Proposed Payment Services Notices on Prevention of Money Laundering and Countering the Financing of Terrorism

Dear MAS Team,

Global Digital Finance support efforts by global standard setters, national authorities and regulators to consult and work with the nascent global digital/virtual asset industry.

To that end, we are hereby providing input to the Consultation regarding the proposed payment services notices on prevention of money laundering and countering the financing of terrorism[1].

The input has been drafted and led by the GDF Anti-Money Laundering Working Group.

About GDF

Global Digital Finance ("GDF") is a not-for-profit industry body that promotes the adoption of best practices for crypto and digital assets and digital finance technologies through the

1 http://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Consultation%20Papers/2019%20PS%20AMLCFT%20Notices%20Consultation/Consultation%20Paper%20on%20Proposed%20Payment%20Services%20Notices%20on%20AMLCFT.pdf

development of conduct standards, in a shared engagement forum with market participants, policymakers and regulators.

Established in 2018, GDF has convened a broad range of industry participants, with 300+ global community members—including some of the most influential digital asset and token companies, academics and professional services firms supporting the industry. GDF is proud to include Circle, ConsenSys, DLA Piper, Diginex, Hogan Lovells, Huobi and R3 as patron members.

The GDF Code of Conduct is an industry-led initiative driving the creation of global best practices and sound governance policies, informed by close conversations with regulators and developed through open, inclusive working groups of industry participants, legal, regulatory and compliance experts, financial services incumbents and academia. Code principles undergo multiple stages of community peer review and open public consultation prior to ratification.

For consistency, we have used the terms 'virtual assets' and 'virtual asset service providers' in our response, in line with the FATF Glossary.

Given the remit of GDF, we have concentrated our responses on Activity F - Digital Payment Tokens that concern virtual assets and virtual asset service providers.

Consultation Inputs

Question 1: Scope. MAS seeks comments on the proposal in paragraph 2.3 to additionally impose AML/CFT requirements on payment service providers for such other business activity that is subject to AML/CFT requirements by another regulatory authority in Singapore but where payment service providers have been exempted from the application of such requirements under the regulatory authority.

Our answer is from the viewpoint of potential licensees and regulated entities under the Payment Services Act i.e. Point 1.8(b) of the consultation paper.

To build and ensure trust and integrity in the new digital payment ecosystem, in principle, we agree that MAS should impose a consistent standard of AML/CFT requirements on non-payment, non-financial trading activities ("trading activities") that are conducted by a

MAS-licensed payment service provider within the same legal entity. Such trading activities include, for example, dealing in precious stones, precious metals, antique collectibles or fine art that is a medium of value with global secondary markets, and which can be used as vehicles for money laundering. We are keen to learn of how MAS would regulate such an entity.

Where there are specific situations that the PS Act has not covered and other regulations are silent, we recommend that such situations be considered on a case-by-case basis by MAS. For example, the regulatory treatment of an issuer and/or dealer of an "asset-backed" digital token that can be based on cash-flow, a physical asset or an intangible asset; and if such a digital token has been programmed to automatically pay out digital payment tokens upon certain events or triggers.

Any eventual regulatory approach should be to strike a balance between financial safety and soundness standards, uphold Singapore's financial industry reputation as well as ensure the cost effectiveness of regulatory compliance on such an issuer who may be a start-up. This is to support innovation inclusiveness (i.e. innovation not just for those who are well-resourced), and to encourage the constant experiment and innovation in Singapore of virtual assets and digital assets that can eventually combine the nature of payments, securities and assets.

Question 2: Alignment with FATF Standards. MAS seeks comments on the proposed requirements in paragraph 2.8, in relation to transfer of DPT and custodian wallet services. MAS also welcomes suggestions on other types of DPT-related services that a DPTS provider could be involved in and which may pose ML/TF risk, necessitating application of AML/CFT measures as well.

In light of the 21 June FATF's adoption of the Interpretative Note to Recommendation 15 on New Technologies, MAS should apply AML/CFT measures that are in line with global FATF Standards – which would include custodian wallet services – as proposed by the Consultation's Paragraph 2.8.

In the 21st June press release, FATF has further mentioned that they will establish a Contact Group to engage the industry and there will be a FATF review after 1 year circa June 2020 of this implementation. We would also recommend for MAS to establish a Contact Group in Singapore to continuously engage the industry including virtual asset licensees and FIs to monitor for implementation experiences, challenges and any new approaches that can similarly meet AML/CFT objectives. This is also to recognise the dynamic nature of the virtual

asset ecosystem and technologies, and in which "crypto-AML/CFT" effectiveness and practical efficiency can be better realised when different stakeholders can come together to combine knowledge in technology, laws and regulations and financial service practices.

Question 4: Simplified Due Diligence. MAS seeks comments on whether SCDD should be permitted for the various payment services covered under the Notices. If so, comments are sought for the SCDD conditions set out in paragraph 3.1 and scenarios where SCDD is not permitted under paragraph 3.2. (Please refer to paragraph 8 of the draft PS Notice 01 and paragraph 7 of the draft PS Notice 02)

GDF is supportive to permit simplified CDD ("SCDD") measures for conditions set out in the Consultation paragraph 3.1 and apply to various payment services covered under the draft PS Notice 02. While paragraph 7.5 indicated payment service providers may perform SCDD for a customer defined as a financial institution in Appendix 2, the list only includes entities and persons regulated in Singapore or subject to exemption. The same as our response to Question 2, MAS should consider extending Appendix 2 to allow SCDD for entities with AML/CFT measures in line with FATF standards. This is consistent with the 21 June FATF VASP RBA guidance, and the draft PS Notice 02 paragraph

11. (b) for Third Party Reliance.

While GDF is also supportive of the scenarios where SCDD would not be permitted per paragraph 3.2. in the Consultation, we noted no definition nor examples of a person with "higher risk characteristics" is available in the Consultation and the draft PS Notice 02. Similar to our earlier response, we suggest MAS benchmark FATF Recommendations to provide examples of higher-risk factors in the guidance, for example, the nationality and/ or country of residence in a higher-risk jurisdiction, connection to Politically Exposed Person ("PEP") and sanctions exposure to prohibit SCDD. In those scenarios, Enhanced Due Diligence ("EDD") should be applied for proper risk assessment and mitigation.

Question 5. Third Party Reliance. MAS seeks comments on whether third party reliance is appropriate for the sector. (Please refer to paragraph 12 of the draft PS Notice 01 and paragraph 11 of the draft PS Notice 02)

Paragraph 3.7 indicates the intention to preclude licensees from third party reliance on VASPs, whether local or foreign, taking into account the higher perceived ML/TF risks posed

by virtual assets and VASPs. Also noted from the PS Notice drafts that "third party" is defined to exclude holders of a payment services licence or equivalent licence.

The GDF believes third party reliance on licensed Major Payment Institutions ("MPIs") should be permitted, even when the holder of the payment services licence is a VASP Provider.

The same as our response to Question 2 and 4, MAS should consider extending Appendix 2 to allow SCDD for entities with AML/CFT measures in line with FATF standards. This is consistent with the 21 June FATF VASP RBA guidance, and the draft PS Notice 02 paragraph 11. (b) for Third Party Reliance.

Lastly, we also suggest MAS updating paragraph 11.4(b) from "immediately" obtain CDD information from the third party to "within a reasonable time and prior to establishing a business relationship".

Fundamentally, the decision to place reliance should be a commercial decision, since the responsibility remains on the payment service licence holder.

Further elaboration as follows.

Risk

As mentioned in Q10.

Restrictive to efficiency

A local VASP may have centralised CDD arrangements with their parent company or its subsidiaries. It may not make sense to exclude such arrangements from reliance given the risks are mitigated within the same company.

Also, where it may be possible for there to be correspondent relationships between adequately licensed VASPs in different jurisdictions, it would not make sense to undergo KYC.

Restrictive to technology and innovation

Allowing reliance between MPIs will help to create effective customer flows between licenced entities, related or otherwise, which may specialise in the different activity types.

VASPs which are large enough to be licenced as MPIs would be better able to handle the stringent CDD requirements as compared to new start-ups looking to innovate.

Virtual asset MPIs may provide a familiar platform for new players and innovators in the blockchain space to rely on for CDD.

MPIs can look to set the standards in the virtual asset space and encourage virtual asset start-ups to work with them. If there is disproportionate regulatory friction, start-ups may choose to test innovations in areas that are more difficult to regulate.

Question 8. Cross-border Transfer. MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.

Although the FATF guidance[2] stipulates that all virtual asset transfers should be considered as cross border, the GDF believes that not all value transfer of virtual assets should be considered as cross-border in nature. If all value transfer of virtual assets is treated as cross-border, this approach will place unnecessary burden on virtual asset providers without considerations and which will not be commensurate with the obligations of other financial institutions.

Domestic value transfers of virtual assets can be identified via:

A. Where the Beneficiary holds its wallet or public address in the same Singapore-licensed virtual asset service provider as the Originator.
B. Where the Beneficiary holds its wallet or public address in another Singapore-licensed virtual asset service provider. Originator's VASP "A" should be aware of VASP "B" and should have established some direct commercial relationship with "B". In this case, "A" can offer an option for the Originator to transfer to the Beneficiary's address in "B".

In other words, we recommend that a value transfer of virtual assets be considered as domestic in nature if the Originator and the Beneficiary are customers of any MAS-licensed VASP ("equation").

[2] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html, note 113

Where a value transfer does not fulfil this equation, such a value transfer of virtual assets would be cross-border in nature, subject to the examination of detail in more complex situations.

This equation approach has an additional benefit of supporting continued innovation and adoption of virtual assets and applying safety and soundness standards consciously to avoid unnecessary costly "one-size-fits-all" application. Otherwise, if there is no recognition of domestic value of transfer, full cross-border AML/CFT/Sanctions and other international safeguards will have to be applied even in a simple repetitive scenario such as where a virtual asset-backed loyalty-card holding consumer in Singapore pays a cafe in Singapore for a coffee i.e. it is a face-to-face transaction, payment is from a known or identifiable human source, the boundaries of the transaction value are well established and the dual-use nature of the product for criminal purposes is negligible. Treating all DPT transactions as cross-border could potentially lead to a volume of false positive inhibiting faster identification of true criminal transactions.

Question 9. Wire Transfer Requirements for DPT Services. MAS seeks comments on whether the FATF's wire transfer requirements are applicable to DPT transactions. Specifically, what information would be relevant for law enforcement purposes, and what records should be kept and/or be attached to a DPT transaction? Please also provide examples of how this requirement could be operationalised in practice, including industry-wide initiatives. (Please refer to paragraph 13 of the draft PS Notice 02)

With regards to the Wire Transfer Requirements for DPT Services we refer MAS to the GDF Input to the FATF public statement (the "Public Statement"), dated 7 April[3]. In particular we draw MAS'

The Wire Transfer Requirements have now been adopted into the FATF Recommendations as of 21 June. To this end, the focus should now be on ensuring the most effective and efficient implementation. Currently, the crypto ecosystem's infrastructure does not exist to facilitate the full implementation of the wire transfer requirements and thus, any guidance response should be aligned. For context, it took over 2 years for SWIFT to be developed.

[3] https://www.gdf.io/wp-content/uploads/2018/01/GDF-Input-to-the-FATF-public-statement-of-22-Feb-2019-FINAL.pdf

Such infrastructure once created and agreed will likely be industry-led and global. In this regard, GDF is taking part in the V20 event[4] at the end of June 2019 alongside ACCESS where solutions and a roadmap will be discussed. The ultimate industry solution may, in part, be driven by the information sharing proposal presented by the GDF in the GDF Input mentioned in the opening paragraph to this question.

The GDF response therefore recommends:

1. Adoption of the information collection requirements highlighted in the FATF Guidance released on 21 June in note 114.[5]
2. A two-stage implementation. Initially, collection and screening of beneficiary information by obliged entities followed by transmission once such technical infrastructure is agreed and in place.
3. A review in line with the 12-month review that the FATF will conduct to consider efficiency, effectiveness, and implementation by obliged entities.

Question 10. Designated Threshold. MAS seeks comments on the proposal in paragraph 5.5 not to set a threshold for the application of CDD i.e. require CDD to be conducted from the first dollar for DPT transactions, even in the case of occasional transactions. (Please refer to paragraph 6.3(b) of the draft PS Notice 02)

Paragraph 5.5 proposes not to set a threshold for the application of CDD to virtual asset transactions. This means that customer due diligence ("CDD") will be conducted from the very first dollar of virtual asset transactions, even when dealing with occasional transactions.

We do not consider this deviation from the FATF Recommendations to be appropriate as:

- it is based on the premise that all virtual asset transactions present the same level of ML/TF risk whereas the risks can vary greatly;
- it could stifle the development of technology and innovation by deterring new investors or investment in new products;
- it is not in line with the amendment to FATF Recommendation 10 which provides for an occasional transactions designated threshold of USD/EUR 1 000 for virtual asset businesses and the deviation is not justified.

[4] https://www.v20.io

[5] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

We elaborate below.

Risk

We understand that the reason for adopting this approach is that all customers / virtual asset transactions are to be treated as "high risk". We consider this to be based on a fundamental but widely held misconception that all virtual asset business models and virtual asset transactions present the same level of ML/TF risk. The level of inherent risk for each business model / virtual asset may vary significantly and, as with all legal entities, the strength of the AML/CTF controls in place can significantly impact upon the residual risk.

For example, decentralised platforms and those virtual assets offering anonymity to customers may be considered to present an increased inherent ML/TF risk. Whilst it may be appropriate to apply CDD for all customers wishing to purchase privacy virtual assets, regardless of value, it does not follow that the same approach should be applied to other virtual assets with a lower risk profile.

In relation to controls, if a virtual asset business is licensed, and therefore supervised for compliance with AML/CTF laws by local authorities, this should offer significant comfort that a business has an AML/CTF programme in place. This should reduce the risk of abuse of an occasional transaction threshold, i.e. the controls in place should recognise a series of linked transaction as is expected of money service operators and banks.

Requiring CDD on all transactions therefore appears disproportionate to the ML/TF risks involved.

It is unlikely that transactions for less that USD/EUR 1,000 will attract criminality. Indeed, given the limited number of exchanges available, it would be very difficult to abuse this limit to criminal purposes through a series of transactions.

Restrictive to technology and innovation

Virtual asset service providers are still an "unknown" for the majority of the population. In addition, for those already investing / trading in virtual assets, new and innovative virtual assets are being developed that they may wish to trial.

New technology promotes innovation and competition. It allows the jurisdictions that embrace it to keep pace with advancements; particularly important for a competitive financial centre such as Singapore.

It is well known that the best way for new investors to understand virtual assets is to buy some and trade. Often, this will be in low value amounts. If customers are faced with CDD requirements when wishing to purchase a very low value virtual assets, this may prevent adoption of the new technology.

FATF recommended threshold

The FATF Recommended designated threshold for virtual asset occasional transactions above which CDD must be completed has been set at USD 1,000. This is already a stricter requirement than the USD 15,000 that applies under Recommendation 10 for fiat occasional transactions, yet it is still higher than MAS'

Question 11. CDD Information. MAS seeks comments on whether any other customer-specific information that is relevant in the context of DPT transactions could be made applicable to potentially supplement or substitute existing identifiers for CDD purposes, including those that are featured in Table 2. (Please refer to paragraph 6.6 of the draft PS Notice 02)

As an overarching comment, a risk-based approach ("RBA") should be adopted in determining the CDD information to be collected. As is the trend globally, taking a principle RBA to AML/CTF, rather than prescriptive measures, is more attuned to achieving the objectives of CDD, i.e. it allows KYC efforts and resources to be targeted where the risk of ML/TF is greatest. Requiring the information in table 2 to be collected on a mandatory basis does not appear to be appropriate as it is not in line with an RBA. We set out below specific feedback on each suggestion within table 2.

DPT sending/receiving addresses

The address could be collected for record-keeping purposes but the limitations of using it for CDD must be acknowledged. The address will not provide information regarding who owns the address.

The collection of metadata may provide a better source of CDD information, for example, the IP address or device ID involved in the transaction. We would suggest that collection of metadata information be an option where enhanced due diligence ("EDD") is necessary.

Receipts/documentation on original purchase of cryptocurrency from an exchange or similar intermediary

This does not appear to be a practical requirement, particularly if it is mandatory. Many customers, particularly those with long periods of trade, will not have a receipt from the original purchase.

For customers new to virtual asset transactions, this information will not be available. We recommend against this requirement.

Transaction details in relation to original purchase of DPT – i.e. number (hash) of transaction, value of transaction (e.g. 2 Bitcoins), timestamp, fee (cost of transaction), size of transaction (in bytes), funds balance history in the address, message recorded in transaction

In itself, this information should be available and could be provided.

It is assumed that the purpose of collecting this information is to verify source of funds and trace transactions through the ledger to the current transaction in order to conduct a risk assessment. Again, we suggest this is only required where EDD is necessary. Traditionally, source of funds information must only be verified where a customer is high risk. As previously explained, not all virtual asset transactions will be high risk. Tracing virtual asset trades from the original purchase is potentially manageable with analytic technology but it is not always practical or resource-effective to do so for every single transaction as the output required manual review. For start-ups this will simply not be possible for all transactions and could be prohibitive to technology and financial inclusion. Consequently, we advise that regulated entities should make use of transactional data using an RBA, which can enable a more effective allocation of systems and resources to scrutinizing transactions that present a higher risk of ML/TF.

For customers new to virtual asset transactions, this information will not be available.

Reasons for purchase of DPT

This should be caveated in similar terms to CDD traditionally, i.e. with “unless this is obvious”. In many cases there will not be a reason other than investment and this will be “obvious”. We suggest that an RBA is adopted such that this is only required where it is not already obvious and/or for customers/transactions that present a high risk of ML/TF. We do not recommend setting a value threshold above which this should be obtained, thresholds are easily circumvented by maintaining transaction just below the limit.

Reasons for current transaction, if applicable

The answer immediately above equally applies here.

We hope you may find our response helpful. Please do not hesitate to contact our Executive Director, Teana Baker-Taylor (Teana@gdf.io) or either of our AML working group co-leads, Benedicte Nolens (benedicte@gdf.io) or Malcolm Wright (malcolm.wright@diginex.com) for further questions or comment.