5 July 2019

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

Subject: Industry Submission on Consultation Paper on the Proposed Payment Services Notices on Prevention of Money Laundering and Countering the Financing of Terrorism

On behalf of the Asia Internet Coalition (AIC) and its members, I am writing to express our sincere gratitude to the Monetary Authority of Singapore (MAS) for the opportunity to submit comments on the **Consultation Paper on the Proposed Payment Services Notices on Prevention of Money Laundering and Countering the Financing of Terrorism**. AIC is an industry association comprised of leading Internet and technology companies in the Asia Pacific region with an objective to promote the understanding and resolution of Internet and ICT policy issues. Our current members are Airbnb, Amazon, Apple, Expedia Group, Facebook, Google, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Oath), and Booking.com.

We commend this initiative by MAS on proposing to issue new notices to payment services providers on anti-money laundering and countering the financing of terrorism ("AML/CFT"), pursuant to the Monetary Authority of Singapore Act (Cap. 186) ("MAS Act"). With an expanding digital economy and integration of financial markets and payments ecosystem, the solutions to anti-money laundering and countering the financing of terrorism should not go unnoticed and should have a goal to guarantee an honest and safe financial system. Further, we also welcome the G20 support on the recently amended FATF Standards to virtual assets and related providers for anti-money laundering and countering the financing of terrorism.

As responsible stakeholders to shape the industry dialogue around the most pressing issues, we appreciate the ability to participate in this discussion and the opportunity to provide inputs into the policy-making process. As such, please find appended to this letter detailed comments and recommendations, which we would like to respectfully request MAS to consider, which could be a useful feedback for future consultations to determine an optimal approach to implementing an effective guideline in prevention of money laundering and countering the financing of terrorism.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490. Importantly, we would also be happy to offer our inputs and insights, directly through meetings and discussions and help shape the **AML/CFT** regulatory framework in Singapore.

Sincerely,

Jeff Paine
Managing Director, Asia Internet Coalition

RESPONSE TO CONSULTATION PAPER

Please note that all submissions received will be published and attributed to the respective respondents unless they expressly request MAS not to do so. As such, if respondents would like:

(i) their whole submission or part of it (but not their identity), or

(ii) their identity along with their whole submission,

to be kept confidential, please expressly state so in the submission to MAS. MAS will only publish non-anonymous submissions. In addition, MAS reserves the right not to publish any submission received where MAS considers it not in the public interest to do so, such as where the submission appears to be libellous or offensive.

Consultation topic:	Consultation Paper on the Proposed Payment Services Notices on Prevention of Money Laundering and Countering the Financing of Terrorism
Name[1]/Organisation: [1]if responding in a personal capacity	**Asia Internet Coalition (AIC)**
Contact number for any clarifications:	+65 8739 1490
Email address for any clarifications:	Secretariat@aicasia.org
Confidentiality	
I wish to keep the following confidential:	N/A *(Please indicate any parts of your submission you would like to be kept confidential, or if you would like your identity along with your whole submission to be kept confidential. Your contact information will not be published.)*

General comments:

1. We appreciate MAS' view that there are low risk activities that are properly exempt from many KYC/AML requirements. An "Exempted Products" category such as the one created by MAS is very valuable and allows licensees to offer lower risk products at lower costs because licensees will not need to incorporate the cost of out-sized compliance requirements on low value, low margin products. It also allows licensees to focus their AML efforts where they are more valuable – on high dollar transactions.
2. Nonetheless, in determining the threshold for low risk activities with respect to Activity A, we recommend that the amount be increased from S$1000 to S$2000. As support for this conclusion, we point to the Financial Crimes Enforcement Network ("FinCEN") in the United States, which conducted significant research and a similar comment period on the issue of what amount is reasonable to exclude from its AML regime, and determined that amounts below USD $2000 (~S$2700) were low risk and sufficiently insignificant indicators of money laundering activity to warrant reporting and customer due diligence.
3. We further request with respect to the Activity A low risk criteria that instead of e-wallet load limit, MAS consider articulating the threshold as a limit per single stored value device or a single transaction limit over a particular time period. The e-wallet capacity limit can be problematic in the event a customer received multiple stored value devices for a particular occasion, such as a birthday or wedding. The e-wallet function in such a case would be the redemption tool only, and it would not reflect the risk to restrain the e-wallet function rather than the device. For example, in the event of a wedding, consider that many guests could each purchase a single device under the limit, and they would all send the stored value cards to the couple on the same wedding date. Even though the cards are all legitimately received and it is not suspicious to redeem all those cards at the same time to a single e-wallet account since each card purchased was under the threshold, the bride and groom would not be able to redeem all their cards in a program attempting to operate within the low risk activities thresholds. This outcome is undesirable because the cards pose no more risk in the e-wallet than they do in the couple's physically possession and the only benefit of the e-wallet is to store the existing cards, all under the threshold, in an organized and cumulative fashion. Thus the e-wallet may be designed only to simplify the customer experience by making an online record of the multiple birthday or wedding gift cards a customer received and therefore should not be the place where the threshold is measured. Instead, to the extent a threshold is required,

that should be exercised on the purchase of the individual devices themselves. No individual stored value card or device should be above the threshold, but it should be acceptable that the total received by a single person in their e-wallet may exceed the threshold if multiple cards were received at a point in time for a special occasion.

Response to Key Questions

Question 3: AML/CFT Requirements for Offering of Exempted Products. MAS seeks comments on the proposed requirements applicable to payment services providers offering Exempted Products as set out in paragraphs 2.14 to 2.18. *(Please refer to paragraph 3.3 of the draft PS Notice 01)*

We agree that all licensees should be aware of their risk and conduct assessments to understand their risk and therefore understand why MAS has included Section 5 as applicable to even Exempted Products, however, we note that Section 5.3 could be read to imply that even where a company has Exempted Products and separately conducted a risk assessment to confirm that their products are low or very low risk, they may need to have processes and procedures in place to further mitigate the risk. There may be situations where risks may exist but are sufficiently low that mitigation processes and procedures do not outweigh the costs to customers are therefore are not desirable to implement.

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)*

While, we agree with MAS' view that third-party reliance is appropriate for the sector, particularly the ability to rely on another body regulated by another credible regulatory agency, even if outside Singapore. To ensure the objective is achieved, we request that MAS modify the language in Section 3.6 (a) of the Consultation Paper to indicate that the licensee may rely on a third party that "is subject to and supervised for compliance with AML/CFT requirements materially consistent with Standards set by FATF, and has adequate AML/CFT measures in place to comply with those requirements." This is because countries with strong compliance regimes may not follow FATF requirements exactly, and we do not want licensees to fail to use this method of efficiency for concerns

that the standard followed by a third party is not 100% the same as that provided by FATF, although it may be equally or more stringent. As long as the third party's supervising agency uses highly effective measures materially derived from FATF standards, the objective would be met.

Section 3.7 of the Consultation Paper states that, given the higher ML/TF risks posed by virtual assets and VASPs, MAS intends to preclude licensees from third-party-reliance on VASPs, whether local or foreign. We are concerned that this proposal will outright prevent VASPs from relying on other VASPs to perform CDD/KYC measures, even in situations where the VASP it intends to rely on is able to demonstrate a robust AML/CFT procedure that meets the standards set by FATF. For instance, when an order book is shared between two DPT exchanges, one DPT exchange should be allowed to rely on a third-party exchange to perform the appropriate CDD measures provided it is satisfied that the third-party exchange has in place a reliable AML/CFT framework.

We are of the view that if the to-be-relied-on VASP is able to satisfy the requirements under Section 11.2 of PS Notice 02, then that VASP should not be precluded by the Authority.

In addition, Section 11.1(c) of PS Notice 02 appears to exclude the parent entity, branches and subsidiaries, etc., from relying on each other when they are the holders of a payment services licence or equivalent licence. This will impose a significant CDD burden on entities within the same group providing payment services (i.e., DPT exchange and digital wallet services). We are of the view that third parties belonging to the same group should be able to rely on group-wide AML/CFT programmes without carving out holders of payment service licences or equivalent licences from Section 11.1(c) of PS Notice 02.

We have the following additional comments on the AML Requirements of Annex B1 generally, if you believe it is appropriate to submit these as well.

1. Section 7.8. We request narrowing of this requirement or clarification of what constitutes a "connected party". In the case of customers who may be large or multi-national companies, requiring information on all of their subsidiaries or affiliates may be sensitive and confidential information that is overly burdensome or risky to provide in light of the nature of the transaction. In the case of customers who are natural people, we suggest that there may be many cases where additional relations' information is not warranted in order to perform a single transaction on behalf of the individual, and the request for information on "connected parties" may prove unduly burdensome and onerous as it is undefined.

2. Section 7.14. In many cases there may be a number of beneficial owners that do not have a significant or controlling stake in the business. To prevent unnecessary burden to companies with numerous owners who do not have the power to individually control the company, we request revision of this section so that only beneficial owners with more than 50% control need to be verified.
3. Section 7.36. We note that in many cases there may be virtual fraud and identity verification techniques that are more effective than those that can be performed by a human face-to-face but may appear less stringent in terms of the information requested from the customers. For example, the efficacy of certain machine learning and algorithms may be much greater than a physical customer identification procedure of comparing the person's appearance to that of an identification photo. Particularly in light of ever-changing and improving technology, we request clarity or acknowledgement that virtual, AI-based or machine learning-based procedures may be used if they are reasonably considered as or more effective than traditional models of CDD, even if they appear less stringent in that they require less information gathering from the customer.
4. Section 18(a). We respectfully request that licensees not be required to have a "single" point of contact for referring suspicious transactions. In lieu of a single point of contact, a particular team or referral line may be better positioned to track referrals and take action. We encourage MAS to allow licensees flexibility to determine how best to structure their reporting team, and require instead only that licensees clearly document and make available the escalation/referral method to all pertinent employees.

Question 9. <u>Wire Transfer Requirements for DPT Services</u>. 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)*

Through a DPT provider's customer due diligence (CDD), it is possible to confirm a customer's identity, determine whether the user/customer resides in a FATF-sanctioned country, and create a customer profile concerning their likelihood to engage in money laundering or other improper behaviours. However, when a customer engages in a

transaction from one DPT service to another, the "beneficiary information" is limited to only their virtual currency address, transaction ID and the transaction amount. The digital address of a virtual currency is linked neither to a financial institution bank account nor to any other DPT accounts, but instead it is transferred to another DPT service in a digital form, whether on a PC or mobile phone. If, as proposed by the MAS, DPT services were only allowed to receive funds from or remit funds to beneficiaries with financial institution-level information (for example, their identity and address), a significant amount of funds would be locked in the service provider infrastructure, causing confusion in the global cryptocurrency market.

As an alternative, the relevant AML authority should require a payment service provider to engage an independent vendor that satisfies the FATF's global AML standards and is able to identify the risks associated with virtual currency addresses. The information collected by a reliable vendor can be used to determine whether any questionable transactions and/or customers are flowing to institutions that have a high potential for engaging in money laundering practices. Such a vendor would be able to share with the DPT service providers the information related to high-risk customers and DPT services that have been flagged on suspicion of money laundering. Accordingly, each DPT service can report suspicious transactions to STRO, and STRO will also be able to trace suspicious transactions based on the information provided by the vendor.

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 13 shall apply to a payment service provider when it effects the sending of one or more digital payment tokens by value transfer or when it receives one or more digital payment tokens by value transfer on the account of the value transfer originator or the value transfer beneficiary but shall not apply to a transfer and settlement between the payment service provider and another financial institution where the payment service provider and the other financial institutions are acting on their own behalf as the value transfer originator and the value transfer beneficiary."

We wish to clarify the meaning of the reference to "financial institution" in this paragraph, as it is unclear whether this definition would include transfers made to the account of another payment service provider which is licensed by MAS, or another unlicensed payment services provider in another jurisdiction which does not have any specific

regulations for digital payment token exchanges. We also wish to clarify whether the value transfer requirements would also apply in the case of pure crypto-crypto transfers (between different exchanges or within the same exchange), or whether they would be limited to fiat-crypto transfers.

Question 11. <u>CDD Information.</u> 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)*

Given the unique characteristics of DPT exchange services, we agree with MAS's intention to adopt alternative customer-specific information for CDD purposes that could potentially supplement or substitute for traditional customer-specific information. The proposed alternative CDD information listed in 5.7 of the Notice would provide relevant information to better understand customer transactions for anti-money-laundering purposes.

However, insisting upon receipts and documentation for original cryptocurrency purchases is not always the most effective way to verify fund sources. Unlike traditional financial transactions, where fiat currencies play the primary role, the majority of DPT transactions only involve cryptocurrencies. A cryptocurrency can be changed to different types of cryptocurrencies multiple times. Therefore, the original documentation of a purchase does not always match with a current asset being traded at the exchange. Recent transaction data from the blockchain could provide more effective information for certain transactions.

Thus, we encourage MAS to consider the characteristics of a transaction and the exchange of DPT when adopting alternative CDD information.