

**Annex A**

**LIST OF RESPONDENTS TO THE CONSULTATION PAPER ON NEW PAYMENT SERVICES NOTICES ON  
PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM**

1. Alibaba.com Singapore E-Commerce Private Limited, Alipay Singapore E-Commerce Private Limited (for and on behalf of Ant Financial Services Group) and WorldFirst Asia, who requested for their comments to be kept confidential
2. The Association of Banks in Singapore
3. Accuity
4. Asia Internet Coalition, on behalf of Airbnb, Amazon, Apple, Expedia Group, Facebook, Google, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Oath), and Booking.com
5. Baibhav Bajpai
6. Baker McKenzie.Wong & Leow
7. CardUp Pte. Ltd.
8. Coda Payments Pte. Ltd.
9. Collyer Law LLC
10. Cynopsis Solutions Pte. Ltd.
11. Deloitte & Touche, together with Grab Financial, PayPal and Revolut, who requested for their comments to be kept confidential
12. Ebuy Coin Pte. Ltd.
13. ECXX Global Pte. Ltd., who requested for their comments to be kept confidential
14. Global Digital Finance
15. Linklaters Singapore Pte. Ltd. on behalf of the Singapore Fintech Association and the Association of Cryptocurrency Enterprises and Startups, Singapore, who requested their comments to be kept confidential
16. Luno Pte. Ltd., who requested for their comments to be kept confidential
17. Naboo Ltd.
18. OKCoin Pte. Ltd. (OKCoin Singapore)
19. PayPal Pte. Ltd., who requested for their comments to be kept confidential
20. RazerPay Pte. Ltd.
21. Refinitiv
22. RHTLaw Taylor Wessing LLP, RHT Compliance Solutions, InvestaCrowd and Tilde Pte. Ltd.
23. SingCash Pte Ltd, Telecom Equipment Pte Ltd and Singtel Mobile Pte Ltd (collectively known as "Singtel")
24. TransferWise Singapore Pte. Ltd.
25. Wirecard Asia Holding Pte Ltd
26. Xfers Pte. Ltd.
27. Respondent A, who requested for their identity to be kept confidential
28. Respondent B, who requested full confidentiality of identity and comments
29. Respondent C, who requested full confidentiality of identity and comments
30. Respondent D, who requested full confidentiality of identity and comments
31. Respondent E, who requested full confidentiality of identity and comments
32. Respondent F, who requested full confidentiality of identity and comments

- 33. Respondent G, who requested full confidentiality of identity and comments
- 34. Respondent H, who requested full confidentiality of identity and comments
- 35. Respondent I, who requested full confidentiality of identity and comments
- 36. Respondent J, who requested full confidentiality of identity and comments
- 37. Respondent K, who requested full confidentiality of identity and comments
- 38. Respondent L, who requested full confidentiality of identity and comments
- 39. Respondent M, who requested full confidentiality of identity and comments
- 40. Respondent N, who requested full confidentiality of identity and comments

Please refer to Annex B for the full submissions.

Annex B

**FULL SUBMISSIONS FROM RESPONDENTS TO THE  
CONSULTATION PAPER ON NEW PAYMENT SERVICES NOTICES ON PREVENTION OF MONEY  
LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM**

S/N	Respondent	Full Responses from Respondent
1.	The Association of Banks in Singapore	<p><b>General comments:</b></p> <p><b>Question 1: <u>Scope</u>.</b> 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.</p> <p>Bank A: We concur with MAS' proposal for AML/CFT requirements to be based on a holistic review of the payment service providers ("PSP") business activities.</p> <p>Bank B: We agree. Just as banks have to ensure that customer due diligence is performed on their customers, payment service providers should also ensure that the relevant due diligence is performed on their other business activity that is subject to AML/CFT requirements by another regulatory authority in Singapore.</p> <p>Bank C: We would like MAS to clarify whether payment service providers that provide non payment services activities which carry ML/TF risks (for example dealing in precious stones and metals) would be regulated under the Precious Stones and Precious Metals (Prevention of Money Laundering and Terrorism Financing) Act 2019 or the Payment Services Act (if the MAS does impose AML/CFT requirements on payment service providers for such business activity).</p> <p><b>Question 2: <u>Alignment with FATF Standards</u>.</b> 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.</p> <p>Bank A: We propose to consider the movement of DPT between 2 DPTS providers.</p>

S/N	Respondent	Full Responses from Respondent
		<p>Bank B: We agree. Such activities should have AML/CFT measures in place to ensure that there is a level of client due diligence, traceability and accountability. This is in view of the ML/TF risk associated with digital payment tokens. The question is whether a DPTS provider has to be “Singapore based” for such requirements to apply. For a non-Singapore based DPTS provider where DPT-related services are accessible from within Singapore, would these requirements apply?</p> <p>We would like MAS to clarify whether entities that are not incorporated in Singapore but offer DPT services in Singapore will require a license under the PS Act.</p> <p><b>Question 3: <u>AML/CFT Requirements for Offering of Exempted Products.</u> 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)</b></p> <p>Bank A: We concur with MAS’ proposal.</p> <p>Bank B: We propose to stipulate the specific identifiable source refers as being an account with FI regulated for AML/CFT. Alternatively, to apply similar threshold as domestic money transfer services</p> <p>Bank C: One of the low risk criteria for Activity A Account Issuance Services is “issuing payment accounts that do not have an e-wallet capacity that exceeds S\$1,000”. We would like MAS to clarify whether this limit is on a daily/monthly/yearly basis. In addition, would it make a difference where the e-wallet is topped up e.g. outside of Singapore?</p> <p><b>Question 4: <u>Simplified Due Diligence.</u> 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)</b></p> <p>Bank A: Licensees carrying out Activity F should not be allowed to perform SCDD. Additionally, is there a requirement for PSP to report on the annual cumulative transactions undertaken for its customer under 3.2(i)?</p> <p>Bank B: A risk-based approach can be permitted as this would allow DPTS to apply due diligence according to the risk profile. The risk profile approach</p>

S/N	Respondent	Full Responses from Respondent
		<p>should be structured/assessed in the same manner as how an FI would approach such risk classification for measurability.</p> <p><b>Question 5. <u>Third Party Reliance</u>. 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)</b></p> <p>Bank A: The bank opines that third party reliance is not appropriate for the sector.</p> <p>Bank B: We feel that the full scope of third party reliance may not be appropriate for the sector currently as they should be the primary point for their customer acquisition and the due diligence to be conducted. The sector's due diligence standards may not be as mature at this point as compared to financial institutions like banks, to have third party arrangements for key customer due diligence processes. Otherwise, it may also increase the ML/TF risk to the whole network involved in the chain of the financial transaction flow.</p> <p>The concept of Third Party Reliance benefits non-banks, as banks are one of the parties that can be relied on. To level the playing field, this section should be expanded to include reliance on other sources of data (credit bureau, alternate bureaus and other FinTechs that triangulate data) instead of just the third party listed.</p> <p>Bank C: Where the Payment Service Provider relies on a Financial Institution as set out in Appendix 2 to perform CDD measures, the Financial Institution must provide information on the "shared" client to the Payment Service Provider. We would like MAS to clarify whether the Financial Institution could satisfy this requirement without breaching Banking Secrecy laws.</p> <p><b>Question 6. <u>Correspondent Account Services</u>. MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 3.9 would be applicable to the Activity performed by your institution. (Please refer to paragraph 13 of the draft PS Notice 01 and paragraph 12 of the draft PS Notice 02)</b></p> <p>Bank A: We propose MAS to consider exempting the requirements where a PSP engages the services of a financial institution that is operating in Singapore.</p> <p><b>Question 7. <u>Bearer Instruments and Cash Payouts</u>. MAS seeks comments on the proposal in paragraph 3.10 to apply the prohibition on issuance of bearer negotiable instruments and restriction of cash payout requirements to licensees which perform Activities A, B, C, F and G. (Please refer to</b></p>

S/N	Respondent	Full Responses from Respondent
		<p><b><i>paragraph 11 of the draft PS Notice 01 and paragraph 10 of the draft PS Notice 02)</i></b></p> <p>Bank A: We would like clarify if exemption can be applied for cash cheques issued for the PSP's operational needs.</p> <p>Bank B: We agree. This is a useful control to maintain traceability of funds movement.</p> <p><b>Question 8. <u>Cross-border Transfer</u>. MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.</b></p> <p>Bank A: Cross-border transfers should exclude transfers via FIs in Singapore.</p> <p>Bank B: Fundamentally, the risk associated with cross-border transfers is the counterparty's information and the background on the purpose of transaction that is available in the wire-transfer message. If the DPT's business model is primary serving the domestic market where identity information of the customers is readily available and traceable, the risk level is different from the transfers which involved other countries/jurisdictions out of Singapore. However, due to the nature of DPT, there is no physical address to the location of the asset. A cross border classification would be more appropriate. The parties within these transactions may not always be based in the same location while the asset may also not sit in the same location as the transactors.</p> <p><b>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)</b></p> <p>Bank A: The following information should be obtained at a minimum: (1) Wire transfer originator and beneficiary information; and (2) Payment reference number. Where required, the DPTS provider must produce a record of the related transaction aligned to the payment reference number which should include the source and destination of funds.</p> <p>Bank B: FATF's wire transfer requirements should be applicable to DPT transactions where it involves cross-border value transfers. The requirements stated in paragraph of draft PS Notice 02 is largely similar to wire transfer requirements for banks in Singapore.</p>

S/N	Respondent	Full Responses from Respondent
		<p><b>Question 10. <u>Designated Threshold.</u></b> 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. <i>(Please refer to paragraph 6.3(b) of the draft PS Notice 02)</i></p> <p>Bank A: Transactions from an identifiable source can be considered for exemption, e.g. to or from an account established in Singapore and the DPTs are sold through ATM machines in Singapore.</p> <p>Bank B: We agree that CDD should be conducted on all customers of DPTS that transact from the first dollar. With reference to paragraph 5.5 of the consultation paper, we feel that the nature of the DPT service should not allow for occasional transactions (i.e. non-customers). Unlike physical financial institutions serving walk-in occasional transactions, the Internet-based (non face-to-face) nature of DPT service providers should be subject to due diligence to address the inherent risk associated with DPT.</p> <p><b>Question 11. <u>CDD Information.</u></b> 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. <i>(Please refer to paragraph 6.6 of the draft PS Notice 02)</i></p> <p>Bank B: Other customer-specific information to consider include:</p> <ul style="list-style-type: none"> <li>• Address of the sender/beneficiary as these could change with each transaction</li> <li>• Customer's unique ID number</li> <li>• Whether transaction is carried out on behalf of a third party</li> </ul> <p>Bank C: The proposed alternative CDD information to be collected could supplement (but not substitute) the customer specific information highlighted in paragraph 5.6.</p>
2.	Accuity	<p><b>General comments:</b></p> <p><b>Question 1: <u>Scope.</u></b> 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</p>

S/N	Respondent	Full Responses from Respondent
		<p><b>payment service providers have been exempted from the application of such requirements under the regulatory authority.</b></p> <p>We view that payment service providers conducting activities supportive of their primary business model but are similar to the nature of DNFBPs (e.g. real estate agents, dealers in precious metals and stones, lawyers and notaries, trust and company service providers) be imposed with AML/CFT requirements through inter-agency collaboration, with due responsibility to inform MAS of any STR filed to the STRO. This increases the oversight of the nature of business that the payment service providers conduct which facilitates MAS or another regulatory authority with ongoing monitoring and provision of guidelines for sub-sector risk mitigation on emerging typologies.</p> <p><b>Question 2: <u>Alignment with FATF Standards.</u> 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.</b></p> <p>Some DPT-related services such as mixers / tumblers should be particularly scrutinized as they undermine the traceability of DPT transactions. We would argue that such services should be considered to carry a higher ML/TF risk and should be either restricted or backed by enhanced due diligence – justification for the recourse to the mixing / tumbler service may include proof of origin and destination of funds.</p> <p>This is also consistent with the recent FATF Guidance on Virtual Assets (Paragraph 110):</p> <p>“Countries should ensure that VASPs licensed by or operating in their jurisdiction consider whether the VASP can manage and mitigate the risks of engaging in activities that involve the use of anonymity-enhancing technologies or mechanisms, including but not limited to AECs, mixers, tumblers, and other technologies that obfuscate the identity of the sender, recipient, holder, or beneficial owner of a VA. If the VASP cannot manage and mitigate the risks posed by engaging in such activities, then the VASP should not be permitted to engage in such activities.”</p> <p>We would be in the view to require DPTS providers to classify the inherent ML/TF risks posed by the various DPT they offer services in.</p> <p>a) Some DPT labelled as “privacy coins” (i.e. Monero, Zcash etc.), should be classified as high ML/TF risks. The DPTS providers should be</p>



S/N	Respondent	Full Responses from Respondent
		<p>required to establish a risk classification of the various set of tokens, based on their features (technology, convertibility, geographical reach etc.)</p> <p>b) The emergence of stablecoins (particularly private stablecoins issued by financial institutions e.g. MUFG, Goldman Sachs) and its likeliness for global use requires measured consideration from the perspective of regulatory structuring as it may constitute a deposit, debt or security. The challenge lies within how the regulator and court will share the same interpretation that can be reconciled with policy goals.</p> <p>c) Extending the regulatory reach to platforms that facilitate peer-to-peer exchange of virtual assets (DApp) which could enable anonymous transfers of funds between individuals, contributing to “layering” of funds to mask their origin. Non custodian wallet providers that function similarly to custodian wallet providers may require increased scrutiny.</p> <p><b>Question 3: <u>AML/CFT Requirements for Offering of Exempted Products.</u></b>  <b>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)</b></p> <p><b>With reference to paragraph 5 of PS Notice 01 – Assessing the Risks and applying a risk-based approach</b></p> <p>We view that the AML/CFT Compliance Officer (as referred to, in PS Notice 01 paragraph 19.3) should be required to oversee the accuracy and maintenance of the risk management activities described in paragraph 5. There should be a requirement to provide regular information on these ML/TF risks to the board of directors.</p> <p><b>With reference to paragraph 6 of PS Notice 01 - New products, practices and technologies</b></p> <p>We view that the AML/CFT Compliance officer (as referred to, in PS Notice 01 paragraph 19.3) should be accountable for the identification and assessment required under paragraph 6.1. That assessment should include the formal classification of the project under the “exempted products”, if applicable. We suggest adding the requirement for the AML/CFT Compliance Officer to sign-off these assessments.</p>

S/N	Respondent	Full Responses from Respondent
		<p>The reason for these requirements is that the classification of a payment activity under the exempted activity should be:</p> <ul style="list-style-type: none"> <li>a) Backed formally by the designated AML/CFT Compliance officer</li> <li>b) Reconsidered and confirmed in the event of any change</li> </ul> <p><b>With reference to paragraph 19 of PS Notice 01 – Internal Policies, Compliance, Audit and Training</b></p> <p>Regarding paragraph 19.3, we see in other jurisdictions a requirement for the institutions to provide their regulatory authority with the name of their AML/CFT Compliance Officer / MLRO.</p> <p>Regarding paragraph 19.7(c), we suggest to also require training on the compliance <b>tools</b> deployed within the organization, notably for performing sanctions screening and transaction monitoring. This is important to ensure tools are being properly deployed, configured and their outputs correctly interpreted and processed.</p> <p><b>Question 4: <u>Simplified Due Diligence</u>.</b> 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. <i>(Please refer to paragraph 8 of the draft PS Notice 01 and paragraph 7 of the draft PS Notice 02)</i></p> <p><b>With reference to PS Notice 01 Paragraph 8 / PS Notice 02 Paragraph 7</b></p> <p>In line with PS Notices 01's paragraphs 8.2 and 8.3 as well as PS Notice 02's paragraphs 7.2 and 7.3, we would suggest that payment service providers should be required to carry out sufficient monitoring of both transactions and customers, in order to ensure that the SCDD continue to be commensurate with the customer's risk level.</p> <p>Overall, regarding the application of SCDD, it would be useful to provide further substance to situations potentially corresponding to lower AML/CFT risks (similarly to what the EU 4<sup>th</sup> AML Directive has specified in its Annex II). This would favor a level playing field in the AML/CFT risk assessment and in the application of SCDD measures.</p> <p><b>Question 5. <u>Third Party Reliance</u>.</b> MAS seeks comments on whether third party reliance is appropriate for the sector. <i>(Please refer to paragraph 12 of the draft PS Notice 01 and paragraph 11 of the draft PS Notice 02)</i></p>

S/N	Respondent	Full Responses from Respondent
		<p>We would like to highlight to MAS on licensees' reliance on vendors that is not covered in the Notices. We propose MAS to consider the inclusion of specific provisions for governing outsourcing arrangement related to the performance of AML/CFT measures outlined in paragraphs 7, 8 and 9 of PS Notice 01 and paragraphs 6, 7 and 8 of PS Notice 02.</p> <p>The suggested provision could include a reference to MAS' Guidelines on Outsourcing last revised on 5<sup>th</sup> October 2018, reminding institutions that any outsourcing arrangement with an entity not covered by the definition of a "third party" (as per paragraphs 12.1 of PS Notice 01 and 11.1 of PS Notice 02) should be consistent with MAS Guidelines on Outsourcing, especially for the purpose of managing the risks referenced in paragraph 5.2 of PS Notice 01. These provisions on outsourcing could also reaffirm the following in relation to outsourcing arrangements:</p> <p><i>For the avoidance of doubt, notwithstanding [any outsourcing arrangement], the payment service provider shall remain responsible for its AML/CFT obligations in this Notice.</i></p> <p>With the varying scale of business across payment service providers, reliance on vendors for certain elements of CDD measures is often assessed as a cost-effective option as opposed to developing an in-house infrastructure solely for the purpose. We view that Question 5 is appropriate and applicable for the sector.</p> <p><b>Question 6. <u>Correspondent Account Services.</u> MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 3.9 would be applicable to the Activity performed by your institution. (Please refer to paragraph 13 of the draft PS Notice 01 and paragraph 12 of the draft PS Notice 02)</b></p> <p>These requirements would not be applicable to our activities.</p> <p><b>Question 7. <u>Bearer Instruments and Cash Payouts.</u> MAS seeks comments on the proposal in paragraph 3.10 to apply the prohibition on issuance of bearer negotiable instruments and restriction of cash payout requirements to licensees which perform Activities A, B, C, F and G. (Please refer to paragraph 11 of the draft PS Notice 01 and paragraph 10 of the draft PS Notice 02)</b></p> <p>We have no comment for this question.</p> <p><b>Question 8. <u>Cross-border Transfer.</u> MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.</b></p>

S/N	Respondent	Full Responses from Respondent
		<p>Yes, we do think this is a mandatory assumption to make. This is consistent with the recent FATF guidance which considers DPT as cross-border by nature. DPT's global reach was a key ML/TF risk identified as early as in FATF 2015 Guidance and further emphasized in the Financial Stability Board's (October 2018) paper outlining the inherent cross-border elements of DPT necessitates international coordination for initiatives within standard-setting bodies.</p> <p>Since no country indication accompanies DPT transactions, it is difficult to account for country risk of a specific DPT transaction. Also, considering the technical possibility to conduct global and cash-based transactions through DPTS providers (e.g. depositing cash into a DPT address or redeeming of fiat equivalent of a DPT address through ATM), it is indeed safer to assume that any DPT transaction is cross-border.</p> <p><b>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)</b></p> <p>In the "Guidance for a risk-based approach to virtual assets and virtual asset service providers" by FATF, paragraph 112 confirm that Recommendation 16 defining "wire transfers" apply to all DPTS providers (or VASPs) that are functionally analogous to wire transfers.</p> <p>Considering the possibility offered by DPTs to transfer funds globally and rapidly, we would expect DPTS providers to be subjected to the same requirements as other providers of Money or Value Transfer Services.</p> <p>On-top of the information already listed in paragraph 13 of PS Notice 02 (notably paragraph 13.6), we would suggest that law enforcement could use additional information to better assess the ML/TF risks related to the transactions:</p> <ul style="list-style-type: none"> <li>a) In addition to the paragraphs 6.21 and 6.23, the requirement to inquire about the "background and purpose" of "complex, unusually large or unusual patterns of transactions", we would argue that the "background and purpose" should be collected by the originator's DPTS provider for any transaction exceeding the S\$1500 threshold.</li> <li>b) Technical information about the originator's and beneficiary's locations (i.e. IP addresses with associated time stamps), and device</li> </ul>

S/N	Respondent	Full Responses from Respondent
		<p>identifiers could be useful information for suspicious activity monitoring (e.g. the use of IP-obfuscating techniques, inconsistency of IPs with declared street address etc.).</p> <p>c) Technical information about the source of funds (e.g. deposit from bank transfer, cash deposit, or previous DPT transfer) and about the known use of privacy enhancing coins or services.</p> <p>About the operational process for sharing this information, we would argue that blockchain platforms are the best solution for conditional and secure information sharing processes.</p> <p>The originating DPTS provider should be in charge of loading a transaction's underlying required information within a blockchain where all registered DPTS providers would be connected. Access to a transaction's underlying information would be limited to the other DPTS acting as intermediary or beneficiary's DPTS provider. Law enforcement agencies should have a global access on all transactions processed/facilitated by Singapore-licensed DPTS providers.</p> <p>Such a system would also enable efficient and traceable workflows for implementing other requirements set out in paragraph 13 of PS Notice 02:</p> <ul style="list-style-type: none"> <li>a) beneficiary Institution's requests to originating institutions for sharing identifying information for transactions below the S\$1500 threshold, as per paragraph 13.5 (b);</li> <li>b) beneficiary institution's decision to reject or block transfers lacking the required information and associated follow-up)</li> </ul> <p><b>Question 10. <u>Designated Threshold</u>. 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)</b></p> <p>We agree with MAS proposition here. We assess it as consistent with MAS's conditions for defining exempt payment activities. This is also consistent with FATF guidance that makes clear that considering the global reach allowed by DPT, every transaction should be considered cross-border.</p>

S/N	Respondent	Full Responses from Respondent
3.	Asia Internet Coalition (AIC), on behalf of Airbnb, Amazon, Apple, Expedia Group, Facebook, Google, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Oath), and Booking.com	<p><b>General comments:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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</li> </ol>

S/N	Respondent	Full Responses from Respondent
		<p>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.</p> <p><b>Response to Key Questions</b></p> <p><b>Question 3: <u>AML/CFT Requirements for Offering of Exempted Products.</u> 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)</b></p> <p>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.</p> <p><b>Question 5. <u>Third Party Reliance.</u> 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)</b></p> <p>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</p>

S/N	Respondent	Full Responses from Respondent
		<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <ol style="list-style-type: none"> <li>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.</li> </ol>



S/N	Respondent	Full Responses from Respondent
		<p>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.</p> <p>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.</p> <p>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.</p> <p><b>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)</b></p> <p>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</p>

S/N	Respondent	Full Responses from Respondent
		<p>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.</p> <p>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.</p> <p><b>Question 10. <u>Designated Threshold</u>. 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)</b></p> <p>"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."</p> <p>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</p>

S/N	Respondent	Full Responses from Respondent
		<p>(between different exchanges or within the same exchange), or whether they would be limited to fiat-crypto transfers.</p> <p><b>Question 11. CDD Information.</b> 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. <i>(Please refer to paragraph 6.6 of the draft PS Notice 02)</i></p> <p>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.</p> <p>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.</p> <p>Thus, we encourage MAS to consider the characteristics of a transaction and the exchange of DPT when adopting alternative CDD information.</p>
4.	Baibhav Bajpai	<p><b>General comments:</b></p> <p><b>Question 1: Scope.</b> 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.</p> <p>[BB,01/July/2019]</p> <ol style="list-style-type: none"> <li><b>Reward Systems:</b> Most businesses use the #Token# system to woo customers. The token system could be as simple as Points accrued on Credit Card to as complex as Crypto-Currency pegged by another Crypto-Asset with an international element (different jurisdiction) to it. These #Points# or #Tokens# may be used for payments in</li> </ol>

S/N	Respondent	Full Responses from Respondent
		<p>formal/informal networks under the influence of such businesses. All businesses offering such schemes to their customers or potential customers should be under the scope.</p> <p><b>2. Vulnerable Businesses:</b> Consistent loss-making firms creates potential risk, exposure, and vulnerability in the system. Business streams which are loss-making, whose focus is expansion should be marked for a higher level of disclosures while using payment systems. In point 1, if not all, but at least vulnerable businesses should be brought in-scope.</p> <p><b>Question 2: Alignment with FATF Standards.</b> MAS seeks comments on the proposed requirements in paragraph 2.8, about 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.</p> <p>[BB,01/July/2019]</p> <p><b>Assumption:</b> One set of rules for all may not provide intended insights to regulators and may even be counterproductive to innovation.</p> <p><b>Suggestion:</b> Categorize DPTS providers in two classes:</p> <ol style="list-style-type: none"> <li><b>1. Privacy-oriented</b> – Stringent thresholds, Stringent CDD while account issuance (causing more formality for customers), not per transaction but regular (may start with weekly, reduce to monthly) overall transaction summary (to keep threshold check). Most important is regulator should be made aware of Customers (Individuals) opting in for Privacy. The continuous feedback loop from Customers to Regulators is must in this case.</li> <li><b>2. Convenience-oriented (non-privacy oriented)</b> – Lenient threshold and less formality for end-customer. The regulator should be able to get Data Analytics for transaction patterns and any other details relevant.</li> </ol> <p><b>Question 3: AML/CFT Requirements for Offering of Exempted Products.</b> 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. <i>(Please refer to paragraph 3.3 of the draft PS Notice 01)</i></p>

S/N	Respondent	Full Responses from Respondent
		<p>[BB,01/July/2019] &lt;No comments&gt;</p> <p><b>Question 4: <u>Simplified Due Diligence</u>.</b> 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. <i>(Please refer to paragraph 8 of the draft PS Notice 01 and paragraph 7 of the draft PS Notice 02)</i></p> <p>[BB,01/July/2019]</p> <p>Considering the response to Question 2 and Question 11 as a base.</p> <p>SCDD should not be allowed for 'Privacy Lovers' but should be for 'Convenience Lovers.'</p> <p><b>Question 5. <u>Third Party Reliance</u>.</b> MAS seeks comments on whether third party reliance is appropriate for the sector. <i>(Please refer to paragraph 12 of the draft PS Notice 01 and paragraph 11 of the draft PS Notice 02)</i></p> <p>[BB,01/July/2019]</p> <p>&lt;No comments&gt;</p> <p><b>Question 6. <u>Correspondent Account Services</u>.</b> MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 3.9 would be applicable to the Activity performed by your institution. <i>(Please refer to paragraph 13 of the draft PS Notice 01 and paragraph 12 of the draft PS Notice 02)</i></p> <p>[BB,01/July/2019] &lt;No comments&gt;</p> <p><b>Question 7. <u>Bearer Instruments and Cash Payouts</u>.</b> MAS seeks comments on the proposal in paragraph 3.10 to apply the prohibition on issuance of bearer negotiable instruments and restriction of cash payout requirements to licensees which perform Activities A, B, C, F and G. <i>(Please refer to paragraph 11 of the draft PS Notice 01 and paragraph 10 of the draft PS Notice 02)</i></p> <p>[BB,01/July/2019]</p> <p>&lt;No comments&gt;</p> <p><b>Question 8. <u>Cross-border Transfer</u>.</b> MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.</p>

S/N	Respondent	Full Responses from Respondent
		<p>[BB,01/July/2019]</p> <p>Considering response for Question 2 and Question 11 as a base. For DPT, “one-stick-fit-all” approach would be counter-productive. <b>Bespoke Regulation</b> is a solution to this. Many DPT may be considered cross-border in nature but keep flexibility. Dynamic Rules implementation services would be very critical. Refer to Question 11’s response for “How?”.</p> <p><b>Question 9. <u>Wire Transfer Requirements for DPT Services.</u> MAS seeks comments on whether the FATF’s wire transfer requirements apply 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)</b></p> <p>[BB,01/July/2019]</p> <p>&lt;No comments&gt;</p> <p><b>Question 10. <u>Designated Threshold.</u> 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)</b></p> <p>[BB,01/July/2019]</p> <ol style="list-style-type: none"> <li><b>1. Threshold:</b> ML/FT does not need a threshold. Every single cent counts. There are numerous examples where consistent cent-level frauds at large scale have caused Businesses/Customers to lose a fortune. However, Thresholds levels could be given as rewards for choices made by end-users. I suggest Threshold should be categorized into three categories: Privacy lovers (lower threshold); Convenience lovers (higher thresholds); Yet to be known (zero threshold).</li> <li><b>2. Privacy vs. Convenience:</b> For customers willing to opt for Privacy, enhanced CDD should be done, and in return, Privacy in transactions, limited to threshold should be granted. For Customers willing to opt for Convenience, ready to share all information with Regulator, regular CDD should be done and rewarded with a higher threshold. For customers, whose CDD is not up-to-the-mark for genuine reason</li> </ol>

S/N	Respondent	Full Responses from Respondent
		<p>(refugees, weakest sections, not part of mainstream) zero threshold should be considered.</p> <p><b>Question 11. CDD Information.</b> 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. <i>(Please refer to paragraph 6.6 of the draft PS Notice 02)</i></p> <p>[BB,01/July/2019]</p> <p>The traditional way of regulation may not serve the purpose. Here it is essential to <i>monitor “Customers (Humans)” more than “Numbers.”</i> Parameters to help <u>Human Nature (Response) Analytics</u> is a critical key.</p> <p>Challenge is that even with Tech Support, the resources with Regulators to analyze are limited. Also, there is a limit to scenarios one can imagine. How about getting frequent feedbacks from end-users of the DPT services?</p> <p>Feedbacks are worth when, it is non-diluted, as soon as possible, and as much as possible.</p> <p>Challenge with getting feedback from a separate system (other than payment system itself) is a burden on end-user. Very few would give feedback, and among those who will give feedback, most will give diluted information due to time decay.</p> <p>The solution, I propose, is to create <u>a Feedback Form integrated into Payment Systems</u>. Given the Digital nature of transactions, the first time in history, it should be possible to <u>integrate an Optional Feedback (rating + text box) Form after every transaction</u>. To create an analogy, something similar found in DBS Net banking after end-user clicks log out or WhatsApp call, after disconnecting the call a feedback form appears.</p> <p>The regulator should be able to employ Human Behaviouralists to draft rules and AI/Machine Learning to identify patterns as per rules.</p> <p>Most important, Regulator <u>should be able to create Dynamic rules/sanctions</u> (based on feedback reviews) which should be able to implement as quickly as upgrading an app on Android phone from Play Store. In other words, the sanctions/rules should be <b>deployable program codes</b>. If traditional ways are followed, I’m afraid; it would be too easy to exploit loopholes in the regulations given the dynamic nature of DPTS.</p>

S/N	Respondent	Full Responses from Respondent
5.	Baker McKenzie. Wong & Leow	<p><b>General comments:</b></p> <p><u>Application of MAS defined low risk activities</u></p> <p>1. We refer to paragraph 2.2 of the Consultation Paper on the Proposed Payment Services Notices on Prevention of Money Laundering and Countering the Financing of Terrorism ("<b>Consultation Paper</b>"), where certain low risk criteria for money-laundering/terrorism financing ("<b>ML/TF</b>") are defined. We make the following submissions here.</p> <p>(a) <u>Definition of "payment for goods and services"</u>. "Payment for goods and services" is defined in the Draft Notice to Payment Services Providers (Specified Payment Services) on Prevention of Money Laundering and Countering the Financing of Terrorism ("<b>Draft PS Notice 01</b>") as "<i>payment or part payment of goods or services to a merchant</i>" (emphasis ours). "Merchant" is in turn defined as:</p> <p style="padding-left: 40px;"><i>"a person (other than an individual who is not required to be registered under the Business Names Registration Act 2014 (Act 29 of 2014)) who, in the course of the person's business —</i></p> <p style="padding-left: 40px;">(a) <i>provides goods or services;</i></p> <p style="padding-left: 40px;">(b) <i>promotes the use or purchase of goods or services; or</i></p> <p style="padding-left: 40px;">(c) <i>receives, or is entitled to receive, any money or other consideration for providing goods or services,</i></p> <p style="padding-left: 40px;"><i>and includes any employee or agent of the person"</i> (emphasis ours).</p> <p>Currently, the definition of "merchant" excludes an individual who is not required to be registered under the Business Names Registration Act 2014 (Act 29 of 2014), e.g. individuals who do not carry on business in Singapore and individual proprietors carrying on business under only the individual proprietor's full name. This would also mean that foreign individuals carrying on business outside Singapore would also fall outside the definition of "merchant".</p>



S/N	Respondent	Full Responses from Respondent
		<p>In this regard, we submit that the low risk criteria for Activities B and C should extend to transactions where the goods or services are provided/supplied by individuals who do not technically fall within the definition of "merchant" under the Payment Services Act ("<b>PSA</b>"). This is because:</p> <p>(i) many businesses in the payments industry cater to both corporate entities and individuals who provide/supply the goods and services that are being transacted. This is so particularly in the case of businesses operating as an online platform or marketplace for sale and purchase in goods and services to be transacted on the platform/marketplace. The buyers and sellers of these goods and services may be corporate merchants but are often also individuals (e.g., individual sellers selling hand-made items). If the strict definition of "merchant" is intended to apply such that only payment service providers facilitating payments of goods or services to such merchants only will be able to avail themselves of the low risk exemption for purposes of the AML/CFT requirements, this would mean that online platforms/marketplaces who facilitate payments will effectively not be able to rely on the fact that the payment are indeed meant for goods or services, as persons utilising services on the platforms/marketplaces will often not fall within the technical definition of a "merchant". This appears to us to render nugatory the regulatory purpose of treating payment for goods or services as a relevant factor in assessing whether a payment service is low risk;</p> <p>(ii) it would be incongruous for persons carrying on merchant acquisition activities in respect of individual merchants to be exempt from licensing under the PSA, and for merchant acquisition service to be broadly exempt from regulation for ML/TF risks, but for payment service providers in respect of money transfer services to be subject to AML/CFT requirements where the goods and services being</p>

S/N	Respondent	Full Responses from Respondent
		<p>paid for are not technically supplied by or paid to a corporate merchant; and</p> <p>(iii) read literally, such a definition would mean that in respect of cross border money transfer service, a payment transaction would not be regarded to be payment for goods and services where foreign individuals are involved in the provision of goods or services. Again, this does not seem to us to accord with the regulatory intent to treat payment for goods or services as a relevant factor in assessing whether a payment service is low risk, in respect of cross border transactions.</p> <p>As such, we submit that the definition of "payment for goods or services" should be deleted from the Draft PS Notice 01.</p> <p>(b) <u>Application of low risk criteria to payers and payees.</u> We seek clarification on whether any distinction would need to be made between payers and payees when applying the low risk criteria for Activities B and C.</p> <p>For ease of reference, we reproduce the low risk criteria for Activity B as follows:</p> <p><i>"Services that only allow the user to perform the following transactions:</i></p> <p><i>(a) <b>Payment for goods or services</b> <u>and</u> where <b>payment is funded</b> from an identifiable source (being an account with a FI regulated for AML/CFT);</i></p> <p><i>(b) <b>Payment for goods or services</b> <u>and</u> where the transaction is under S\$20,000; <u>or</u></i></p> <p><i>(c) <b>Payment is funded</b> from an identifiable source <u>and</u> where the transaction is under S\$20,000."</i> (emphasis in bold added)</p> <p>Similarly, we reproduce the low risk criteria for Activity C as follows:</p> <p><i>"Services where the user is only allowed to <b>pay for goods or services</b> and where that <b>payment is</b></i></p>

S/N	Respondent	Full Responses from Respondent
		<p><i><b>funded</b> from an identifiable source.”</i> (emphasis in bold added)</p> <p>We note that the descriptions used under Activities B and C refer primarily to the <i>payer</i> (rather than the payee). For example, the descriptions refer to “payment for goods or services” (which implies payment by a payer), and the source from which “payment is funded” (which implies payment funding by a payer). The criteria makes no reference to the profile, actions or identification of the payee.</p> <p>As provided by paragraph 2.2 to the Consultation, a licensee is not required to comply with the AM/CFT requirements under the MAS’ Proposed Payment Services Notices on Prevention of Money Laundering and Countering the Financing of Terrorism (“<b>Notices</b>”) if it provides services that meet these prescribed low risk criteria for ML/TF. We seek MAS’ confirmation that there is <u>no need</u> for the licensee to apply the AML/CFT requirements on <i>both</i> the payers and payees once the prescribed low risk criteria for ML/TF is met (notwithstanding that the low risk criteria does not make reference to the profile, actions or identification of the payee).</p> <p>(c) <u>Provision of services beyond MAS defined low risk activities.</u> We refer to footnote 2 in paragraph 2.2 of the Consultation. It is stated that where a licensee provides services beyond MAS defined low risk activities, the licensee would have to ensure that all its activities (including those are MAS defined low risk activities) comply with the requirements in the AML/CFT Notices. We submit that this goes against the risk-based approach advocated by the MAS towards managing ML/TF risks and that it would impose a significant compliance burden on licensed payment service providers that are predominantly involved in low-risk activities.</p> <p>Where licensed entities provide services that do not constitute a “product” under the Notices (and thereby unable to meet the “Exempted Product” definition) and are engaged in activities beyond the MAS defined low risk activities, such entities should be allowed to take a risk based approach and comply with the AML/CFT Notices in respect</p>

S/N	Respondent	Full Responses from Respondent
		<p>of activities that fall outside the MAS defined low risk activities.</p> <p><u>When CDD is to be performed</u></p> <p>2. We submit that unlike financial institutions which require CDD to be conducted at the point of account opening, the nature of the business models of payment service providers, particularly those operating online (such as online platforms and marketplaces) are such that CDD should only be carried out at the point in time where the customer seeks to utilise the payment service by way of the initiation of a transaction (which would be a later point of time, subsequent to account opening). We elaborate below.</p> <p>Paragraph 7.3 of the Draft PS Notice 01 provides that a payment services provider shall perform CDD measures when, amongst others, the payment service provider establishes business relations with any customer. “<b>Business relations</b>” is in this regard defined as:</p> <p><i>“the <u>opening or maintenance of an account</u> (whether a payment account or otherwise) by the payment service provider for the purposes of accepting, processing or executing any transaction in the name of a person (whether a natural person, legal person or legal arrangement)”</i> (emphasis ours).</p> <p>The above proviso and definition are similarly contained in the Draft Notice to Payment Services Providers (Digital Payment Token Service) on Prevention of Money Laundering and Countering the Financing of Terrorism (“<b>Draft PS Notice 02</b>”).</p> <p>A plain reading of the Draft PS Notice 01 and Draft PS Notice 02 suggests that CDD is to be conducted when the payment services provider opens or maintains a customer’s account, whether or not such an account is a payment account or merely a user login account. We understand that this follows the approach of when financial institutions regulated by the MAS are required to perform CDD measures, which is reasonable given the nature of how financial institutions operate and where their primary business activity is to provide financial services.</p> <p>However, in the context of payment service providers, <u>and particularly for those whose primary business does not involve providing payment services (such as online platforms and</u></p>

S/N	Respondent	Full Responses from Respondent
		<p><u>marketplaces that provide a payment services only on a secondary basis</u>), it is submitted that requiring CDD measures to be performed at the outset of establishing business relations will be onerous and cause significant friction. To elaborate, online businesses commonly allow customers to set up an account (such as a user login account) quickly and would like to reduce friction in the customer experience. Customers signing up for an account on these online platforms/marketplaces may hold the accounts for an extended period of time without initiating any payment transaction. The online platform/marketplace provides other forms of services that may not necessarily involve payment services (e.g. aggregating posts from other users / recommending relevant news and articles). The payment services provided to initiate any payment transaction would only be required when there is an actual transaction for the goods and services on the online marketplace. If CDD is required to be performed on the customer even before the customer undertakes the first transaction, this may result in lost business opportunities and business costs to the online business, as customers may be reluctant to provide CDD information at the outset for what is ostensibly not a financial transaction in the eyes of the customer.</p> <p>We therefore submit that CDD measures should not always be required at the point of opening an account, but rather, may be performed only at the point where the customer seeks to initiate a payment transaction. The point in time at which CDD measures are to be undertaken should be determined based on an assessment of when actual payment services will be provided.</p> <p><u>Measures for non-account holder</u></p> <p>3. We refer to paragraph 7.42 of Draft PS Notice 01 and the definition of "customer", i.e. a person with whom the payment service provider establishes or intends to establish business relations, or for whom the payment service provider undertakes or intends to undertake any transaction without an account being opened.</p> <p>In the context of money transfer services where a payment service provider acts on behalf of a payee, it may facilitate the receipt of moneys by the payee from multiple payors and in that regard, will not establish any business relations with the payors. In such context, we wish to clarify with the MAS that the payment service provider <u>will not</u> be regarded as undertaking a transaction for the payors (without an account being opened), as to be required to either treat</p>

S/N	Respondent	Full Responses from Respondent
		<p>the payors as its customers or to apply the measures for non-account holder set out in paragraph 7.42 of Draft PS Notice 01 on the payors. In other words, we submit that a payment service provider should only be required to treat persons with whom it contracts with to provide services (whether or not an account is opened) as its customer for purposes of the AML/CFT requirements.</p> <p><b>Question 1: <u>Scope</u>. 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.</b></p> <p>4. We submit that where a payment service provider carries on non-payment service business activities which are separately subject to AML/CFT requirements by another regulatory authority in Singapore, there should be no need to impose additional AML/CFT requirements on such non-payment service business activities from an MAS regulatory perspective. The non-payment service business activities should continue to be subject to the AML/CFT requirements applicable under the relevant laws and regulations, and there is no need for an overlay of additional AML/CFT requirements by the MAS.</p> <p><b>Question 2: <u>Alignment with FATF Standards</u>. 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.</b></p> <p>N.A.</p> <p><b>Question 3: <u>AML/CFT Requirements for Offering of Exempted Products</u>. 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)</b></p> <p>5. It is not clear when a licensed payment service provider would be regarded as providing services/activities that meet the MAS defined low risk criteria as opposed to an “Exempted Product”.</p>

S/N	Respondent	Full Responses from Respondent
		<p>A "product", for purposes of the definition of "exempted product", is defined to mean a facility which is offered by a payment service provider to its customers in relation to one or more specified payment services under the same terms and conditions. We would like to clarify with the MAS whether the touchstone for whether a payment service provider may regard its service offering as a "product" (for the purposes of determining whether it may then be an exempted product) to be whether or not there is room for negotiation by a customer of the payment service provider's terms for the offering of the service, and if there is none, that the service offering may be regarded as being a "product" for purposes of the definition.</p> <p>Further, assuming that a payment service provider offers a different pricing model for its services to different customers, but that apart from pricing all other terms and conditions for the offering of the service remains the same, would the MAS consider such an offering to fall within the definition of "product"?</p> <p><b>Question 4: <u>Simplified Due Diligence</u>. 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)</b></p> <p>6. We agree with the approach to allowing licensees a risk-based approach to perform CDD, and to adopt simplified due diligence measures based on their risk assessment.</p> <p>A number of payment service providers have however communicated concern over the requirement for a payment service provider, in respect of there being no face-to-face contact, to perform CDD measures that are at least as stringent as those that would be required to be performed if there was face-to-face contact.</p> <p>In this regard, we would request for clarification from the MAS on:</p> <p>(a) whether a licensee would be permitted to rely on its risk assessment to carry out simplified CDD and thereby avoid performing any additional non-face-to-face measures (e.g.</p>

S/N	Respondent	Full Responses from Respondent
		<p>holding real-time video conference that is comparable to face-to-face communication); and</p> <p>(b) whether, given the MAS Circular on the Use of MyInfo and CDD Measures for Non Face-To-Face Business Relations, payment services providers relying on MyInfo would still be required to undertake any additional non-face-to-face measures.</p> <p>7. We note that licensees will not be permitted to perform simplified CDD measures where the annual cumulative transactions undertaken for a customer exceeds SGD 20,000. In this regard, given that licensees who provide payment services solely for the payment of goods and services to merchants, and the transactions are funded from an identifiable source, are wholly exempt from the application of Draft PS Notice 01, we would submit that there should not be a SGD 20,000 cap for which simplified CDD measures are disallowed, if the underlying transaction remains as one for the payment of goods and services, and is funded from an identifiable source.</p> <p><b>Question 5. <u>Third Party Reliance</u>.</b> MAS seeks comments on whether third party reliance is appropriate for the sector. <i>(Please refer to paragraph 12 of the draft PS Notice 01 and paragraph 11 of the draft PS Notice 02)</i></p> <p>N.A.</p> <p><b>Question 6. <u>Correspondent Account Services</u>.</b> MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 3.9 would be applicable to the Activity performed by your institution. <i>(Please refer to paragraph 13 of the draft PS Notice 01 and paragraph 12 of the draft PS Notice 02)</i></p> <p>N.A.</p> <p><b>Question 7. <u>Bearer Instruments and Cash Payouts</u>.</b> MAS seeks comments on the proposal in paragraph 3.10 to apply the prohibition on issuance of bearer negotiable instruments and restriction of cash payout requirements to licensees which perform Activities A, B, C, F and G. <i>(Please refer to paragraph 11 of the draft PS Notice 01 and paragraph 10 of the draft PS Notice 02)</i></p> <p>N.A.</p>



S/N	Respondent	Full Responses from Respondent
		<p><b>Question 8. <u>Cross-border Transfer</u>.</b> MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.</p> <p>N.A.</p> <p><b>Question 9. <u>Wire Transfer Requirements for DPT Services</u>.</b> 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. <i>(Please refer to paragraph 13 of the draft PS Notice 02)</i></p> <p>N.A.</p> <p><b>Question 10. <u>Designated Threshold</u>.</b> 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. <i>(Please refer to paragraph 6.3(b) of the draft PS Notice 02)</i></p> <p>N.A.</p> <p><b>Question 11. <u>CDD Information</u>.</b> 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. <i>(Please refer to paragraph 6.6 of the draft PS Notice 02)</i></p> <p>N.A.</p>

S/N	Respondent	Full Responses from Respondent
6.	CardUp Pte. Ltd.	<p><b>General comments:</b></p> <p><u>Regarding PS Notice 01</u></p> <p>Paragraph 7.11: we would like to request clarifications regarding the rationale behind collecting a specimen signature for every natural person appointed to act on behalf of a customer. As an online payment service provider, we do not verify transactions with a signature but with an OTP and other digital means. Therefore, collecting specimen signatures, which might be relevant for some businesses, wouldn't increase our risk management controls and would overly burden our customers.</p> <p><b>Question 4: <u>Simplified Due Diligence</u>.</b> 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. <i>(Please refer to paragraph 8 of the draft PS Notice 01 and paragraph 7 of the draft PS Notice 02)</i></p> <p>(Confidentiality requested)</p> <p><b>Question 5. <u>Third Party Reliance</u>.</b> MAS seeks comments on whether third party reliance is appropriate for the sector. <i>(Please refer to paragraph 12 of the draft PS Notice 01 and paragraph 11 of the draft PS Notice 02)</i></p> <p>Yes</p> <p><b>Question 6. <u>Correspondent Account Services</u>.</b> MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 3.9 would be applicable to the Activity performed by your institution. <i>(Please refer to paragraph 13 of the draft PS Notice 01 and paragraph 12 of the draft PS Notice 02)</i></p> <p>It wouldn't be applicable to CardUp.</p> <p><b>Question 7. <u>Bearer Instruments and Cash Payouts</u>.</b> MAS seeks comments on the proposal in paragraph 3.10 to apply the prohibition on issuance of bearer negotiable instruments and restriction of cash payout requirements to licensees which perform Activities A, B, C, F and G. <i>(Please refer to paragraph 11 of the draft PS Notice 01 and paragraph 10 of the draft PS Notice 02)</i></p> <p>CardUp is not involved in any cash transactions.</p>

S/N	Respondent	Full Responses from Respondent
7.	Coda Payments Pte. Ltd.	<p><b>General comments:</b></p> <p>As background information, we provide a payment service which facilitates payments solely to online merchants from the merchants' customers ("<b>end users</b>") who would like to pay for digital content using payment channels or methods available in their country. We specialize in supporting alternative payment channels that end users without a credit or debit card can use, such as direct carrier billing (paying with a purchase using prepaid mobile credit, or by having the charge posted to the end user's postpaid mobile phone bill), bank transfers, over-the-counter payments, voucher redemptions, and e-wallets (stored value accounts). We do not ourselves operate any of these payment channels; instead, we contract with payment channel operators to collect payments on behalf of our merchants. End users are individuals who are subscribers, account holders or users of these payment channels.</p> <p>Our merchants are typically prominent technology companies – eight of China's top ten game publishers are Coda clients – who use our services to collect payments for digital content, goods or services online, such as in-game credits. We receive funds settled to us from payment channel operators (less a fee taken by them for their provision of the payment service) and channel such said funds (less a fee taken by us for our provision of the payment service) to the merchant for payment.</p> <p>The bulk of the payments that we process, by both transaction value and volume of transactions, are made by end users outside Singapore (mostly in the emerging markets of Southeast Asia) to merchants outside Singapore (mostly in Hong Kong).</p> <p>We consider the risk of money laundering or terrorism financing ("<b>ML/TF</b>") in our business to be low, for the following reasons:</p> <ol style="list-style-type: none"> <li>1. Using our services to launder money or finance terrorism would be inefficient, both because the per-transaction value made by an end user to the merchant is very low (S\$2-3 on average) and because the fees paid by us to the payment channels and those paid by merchants to us are very high (18% on average). Direct carrier billing, which is the most popular payment channel in our business, would be an expensive, cumbersome and slow way to move meaningful amounts of money.</li> <li>2. The transactions processed are in relation to the purchase of digital content supplied by our merchants who are reputable game publishers</li> </ol>

S/N	Respondent	Full Responses from Respondent
		<p>and other digital content providers. All of them are regulated, and many of them are publicly listed.</p> <p>3. We provide local language customer support to end users, so there is a channel for end users to provide us direct feedback regarding our merchants, thereby mitigating the risk of merchants utilising our service in any way other than for the payment of goods or services.</p> <p>4. Settlement of funds to our merchants is only carried out by way of bank transfer, and where the beneficiary name of the bank account matches the name of the contracting party.</p> <p>5. We work with reputable third-party payment channels in the local jurisdictions (e.g. mobile network operators and convenience store chains) that collect payments directly from end users, and they are responsible for fulfilling any CDD requirements set forth by the relevant regulatory bodies in their jurisdictions.</p> <p>6. We have implemented certain measures, such as a maximum per-transaction limit which varies across our payment channels, and automated blocking and alerts of transaction volumes exceeding certain established thresholds for our merchants.</p> <p>7. We do not collect in or settle to countries subject to sanctions and/or jurisdictions deemed high-risk or non-cooperative by the Financial Action Task Force ("FATF").</p> <p>8. We have a high-touch point sales process whereby we carry out face-to-face meetings with employees of most of our merchants and all payment channels.</p> <p>9. We carry out daily manual review of transaction volumes to identify suspicious patterns, and practise suspicious transaction reporting where necessary in compliance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A of the Republic of Singapore).</p> <p>10. Outward money transfers from Singapore end users to foreign merchants compared against the payments processed by us on the whole represent a very small portion of our business.</p> <p>11. Inward money transfers to Singapore merchants from foreign end users compared against the payments processed by us on the whole also represent a small portion of our business.</p>

S/N	Respondent	Full Responses from Respondent
		<p>Given the nature of our business, we would like to request MAS to clarify the definition of “customer” in the draft Notices to provide that such term is meant to include only our clients to whom we provide transaction processing services (i.e. our merchants), and does not include their customers. We wish to highlight that it would not only be commercially impractical and detrimental to the business to require money transfer service providers (“<b>MVTS Providers</b>”) who (i) predominantly conduct cross-border transactions for payment of online goods (especially in-game credits), (ii) handle transactions which have very low per-transaction value; and (iii) do not collect payments or funds directly from the end users (i.e. ultimate payers), to carry out CDD on end users, but it would also appear to be disproportionate to the ML/TF risks that these transactions are exposed to and inconsistent with the risk-based approach taken by the FATF for such services.<sup>1</sup></p> <p>If AML/CFT measures are indeed applicable to the end users being the ultimate payers, this will significantly impact the way we carry on our business. Millions of users in sixteen countries use our services each month. It would be impossible for us to carry out CDD (or even simplified CDD) on them, and we will very likely have to consider terminating or restricting certain aspects of our business where we will not able to conduct CDD, particularly on direct carrier billing and over-the-counter payment users, or re-domiciling our company in a jurisdiction where no such requirement exists.</p> <p><b>Question 1: <u>Scope</u>.</b> 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.</p> <p>NIL</p> <p><b>Question 2: <u>Alignment with FATF Standards</u>.</b> 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.</p>

<sup>1</sup> FATF (2016), *Guidance for a Risk-Based Approach for Money or Value Transfer Services*, FATF, Paris <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-money-or-value-transfer.html>

S/N	Respondent	Full Responses from Respondent
		<p>NIL</p> <p><b>Question 3: <u>AML/CFT Requirements for Offering of Exempted Products.</u></b>  <b>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)</b></p> <p>In respect of the low-risk exemption for cross-border money transfer services, we note from paragraph 3.2(c) of the draft PS Notice 01 that the exemption criteria are more limited as compared to domestic transfer services. Based on the proposed, MVTs Providers who process transactions via certain means, especially direct carrier billing, over-the-counter payments, and voucher redemptions in our case, will not qualify for the exemption and will be subject to the Notice even when the transaction values are very small.</p> <p>While cross-border money transfer services may be more vulnerable to the ML/TF risks than domestic transfers, in view of the type of goods or services offered and the conditions of our transactions as set out above under “general comments”, we consider these transactions and money transfers in this connection to carry inherently low ML/TF risks.</p> <p>Therefore, we respectfully submit that MAS consider expanding the exemption criteria for cross-border money transfer services by applying the same or similar exemption criteria as proposed for the domestic service, except with a lower transaction-value threshold limit for services performed for the payment of goods or services where it cannot be established that the payment is funded from an identifiable source.</p> <p>Currently, cross-border transfers are only considered Exempted Products if the product is “<i>to be used only as a means of payment for goods or services and is funded with monies from an identifiable source</i>” (see draft PS Notice 01 paragraph 2.1). We would propose that MAS revise the definition of “Exempted Product” for cross-border transfers as follows to closely mirror the language for domestic transfers, except with a much lower limit:</p> <p style="padding-left: 40px;"><i>“exempted product” means ---</i></p> <p style="padding-left: 40px;">...</p> <p style="padding-left: 40px;">(c) “where the product involves a cross-border money transfer service, the product satisfies at least two of the following requirements: (i) is to be used only as a means of payment for goods or services; (ii) is funded</p>

S/N	Respondent	Full Responses from Respondent
		<p><i>with monies from an identifiable source; (iii) the payment transaction does not exceed S\$1,000.”</i></p> <p>This would enable us to continue with our business model while also mitigating the risk presented by cross-border transfers from unidentifiable sources. We note that the proposed S\$1,000 limit is lower than the <i>de minimus</i> limit permitted by the FATF Recommendations,<sup>2</sup> and the relevant excerpt is set out below:</p> <p><i>5. Countries may adopt a de minimis threshold for cross-border wire transfers (no higher than USD/EUR 1,000), below which the following requirements should apply: (a) Countries should ensure that financial institutions include with such transfers: (i) the name of the originator; (ii) the name of the beneficiary; and (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer. (b) Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information.</i></p> <p>It should also be highlighted that the FATF Recommendation referred to above (i) relates to wire transfers, which are of higher risks than payments to merchants for goods and services; and (ii) requires only non-verified identification of the payment sender to be provided.</p> <p>It is also worth noting that MAS already exempts banks from conducting CDD with respect to domestic and cross-border transfers below S\$1,500 that are sent or received by customers who lack an existing account with that bank.<sup>3</sup> The relevant excerpt is set out below.</p> <p><b><i>When CDD is to be Performed</i></b></p> <p><i>6.3 A bank shall perform the measures as required by paragraphs 6, 7 and 8 when –</i></p> <p>...</p>

<sup>2</sup> FATF (2012-2018), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FATF, Paris, France, <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>, Interpretive note to Recommendation 16 (Wire Transfers).

<sup>3</sup> MAS (2015), *MAS Notice 626 – Prevention of Money Laundering and Countering the Financing of Terrorism – Banks*, Paragraph 6.3.

S/N	Respondent	Full Responses from Respondent
		<p><i>(c) the bank effects or receives any funds by domestic wire transfer, or by cross-border wire transfer that exceeds S\$1,500, for any customer who has not otherwise established business relations with the bank;</i></p> <p><b>Question 4: <u>Simplified Due Diligence</u>.</b> 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. <i>(Please refer to paragraph 8 of the draft PS Notice 01 and paragraph 7 of the draft PS Notice 02)</i></p> <p>We agree that SCDD should be permitted for licensed activities covered under the Notices. However, the suitability of the proposed conditions under which SCDD is permitted will depend on whether the CDD would only apply to the customers of MVTs Providers' direct merchants as queried above. This can affect our risk assessment and application of AML/CFT measures, especially where funds cannot be definitively ascertained to be from an "identifiable source".</p> <p>Regarding the proposed annual cumulative transaction threshold of S\$20,000 under Paragraph 8.4(a) of Notice 01, we respectfully request that MAS consider increasing the annual cumulative transaction amount to an amount which is appropriate in light of the nature of transactions undertaken by us and MVTs Providers who carry on similar activities. Due to the volume of transactions that may be processed for our merchants, and that fund settlements are received from the various payment channels and are paid to our merchants on agreed settlement cycle basis (which can range from weekly, monthly or otherwise), the cumulative transaction amount received or sent (despite the low per-transaction value) by MVTs Providers annually could easily be in excess of the threshold limit of S\$20,000. We are of the view that S\$200,000 would be a more appropriate amount.</p> <p><b>Question 5. <u>Third Party Reliance</u>.</b> MAS seeks comments on whether third party reliance is appropriate for the sector. <i>(Please refer to paragraph 12 of the draft PS Notice 01 and paragraph 11 of the draft PS Notice 02)</i></p> <p>Our payment channel partners (most of whom are located overseas) are generally regulated in their local jurisdictions in light of the tightening of the payments industry regulations globally. They are therefore obliged under their various regulatory frameworks to apply AML/CFT measures on their customers i.e. end users, as well as merchants i.e. us. Therefore, reliance on these partners to perform the requisite CDD in our business sector is applicable and would be appropriate, in the event that AML/CFT measures</p>



S/N	Respondent	Full Responses from Respondent
		<p>are to be applied to customers of our direct merchants and payment channel partners.</p> <p>On this note, it appears that definition of “third party” under Paragraph 12.1(b) of the draft Notice 01 excludes “holders of payment services licence or equivalent licence”. We wish to clarify whether we can rely on the CDD conducted by our foreign payment channels, most of whom are foreign licensed payment gateway providers and e-money issuers.</p> <p><b>Question 6. <u>Correspondent Account Services</u>.</b> MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 3.9 would be applicable to the Activity performed by your institution. <i>(Please refer to paragraph 13 of the draft PS Notice 01 and paragraph 12 of the draft PS Notice 02)</i></p> <p>NIL</p> <p><b>Question 7. <u>Bearer Instruments and Cash Payouts</u>.</b> MAS seeks comments on the proposal in paragraph 3.10 to apply the prohibition on issuance of bearer negotiable instruments and restriction of cash payout requirements to licensees which perform Activities A, B, C, F and G. <i>(Please refer to paragraph 11 of the draft PS Notice 01 and paragraph 10 of the draft PS Notice 02)</i></p> <p>NIL</p> <p><b>Question 8. <u>Cross-border Transfer</u>.</b> MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.</p> <p>NIL</p> <p><b>Question 9. <u>Wire Transfer Requirements for DPT Services</u>.</b> 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. <i>(Please refer to paragraph 13 of the draft PS Notice 02)</i></p> <p>NIL</p> <p><b>Question 10. <u>Designated Threshold</u>.</b> 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</p>

S/N	Respondent	Full Responses from Respondent
		<p>case of occasional transactions. <i>(Please refer to paragraph 6.3(b) of the draft PS Notice 02)</i></p> <p>NIL</p> <p><b>Question 11. <u>CDD Information.</u></b> 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. <i>(Please refer to paragraph 6.6 of the draft PS Notice 02)</i></p> <p>NIL</p>

S/N	Respondent	Full Responses from Respondent
8.	Collyer Law LLC	<p><b>General comments:</b></p> <p><b>Question 1: <u>Scope</u>.</b> 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.</p> <p>Collyer Law: Insofar as there are gaps that would allow regulatory arbitrage, we agree that the additional AML/CFT requirements should be imposed.</p> <p><b>Question 2: <u>Alignment with FATF Standards</u>.</b> 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.</p> <p>Collyer Law: We agree with this recommendation. In fact, while we accept that the PS Act is taking an incremental approach to regulation of activities related to DPTs, we think it will lead to clarity if custodial services for DPTs are included in the First Schedule to the PS Act. We expect that DPTS providers are likely to outsource custodial services to either streamline their operations or to mitigate their risk. Having DPTS providers such as crypto-exchanges manage both hot (exchange) wallets and cold storage may be perceived as less secure as an independent custodian.</p> <p>The regulatory arbitrage we foresee is that in order to avoid being regulated, DPTS providers who want to provide custodial services will outsource the services to third parties not licensed under the PS Act. MAS would not have regulatory oversight over those third parties.</p> <p><b>Question 8. <u>Cross-border Transfer</u>.</b> MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.</p> <p>Collyer Law: We expect OTC brokers to be making markets within Singapore itself, and it does not make sense to characterise such value transfers as cross-border.</p>

S/N	Respondent	Full Responses from Respondent
		<p>Qualifying wire transfers means a cross-border wire transfer above any applicable threshold as described in paragraph 5 of the Interpretive Note to Recommendation 16.</p> <p>The net effect of this FATF recommendation is to completely exclude certain DPTs, such as Monero, ZCash and Dash, which provide for anonymous signatures. This means that certain popular DPTs will not be permitted to list and trade on DPT exchanges regulated under the PS Act. While laudable from an AML/CFT perspective, this may render Singapore as an unattractive destination as a crypto-currency hub if commonly-used tokens like these cannot be traded here. We should highlight that ZCash's zk-SNARK is seen as an cutting-edge innovative breakthrough, so in the interests of AML/CFT measures, there may be a dampening effect on innovation in this respect.</p> <p>Even public addresses and wallets on a public blockchain are pseudonymous, so this requirement also effectively removes the pseudonymous nature of such addresses, since the names of the originator and beneficiary must be included.</p> <p><b>Question 10. Designated Threshold.</b> 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. <i>(Please refer to paragraph 6.3(b) of the draft PS Notice 02)</i></p> <p>Collyer Law: We believe the FATF proposal on establishing a threshold is adequate and reasonable. DPT transactions are largely internet based and occasional transactions may be rare, but the threshold proposed by FATF makes more sense as it allows the DPTS provider to focus on customers and recurrent transactions as opposed to spending time to perform CDD on each and every transaction, including "occasional" transactions which by definition will not likely to be repeated. Moreover, it does not seem that occasional transactions with the amount less than USD/EUR1,000 represent high ML risk or financial crime risk due to the low amount in question, unless they are batched together and submitted in a series to "fly under the radar"</p> <p><b>Question 11. CDD Information.</b> 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. <i>(Please refer to paragraph 6.6 of the draft PS Notice 02)</i></p> <p>Collyer Law: Given that crypto-wallets are not tied to national identification documents or names, but public addresses / private keys, owners of VA</p>

S/N	Respondent	Full Responses from Respondent
		<p>should have maintained their receipts and other documentation since there would be no other way of verifying that those wallets belong to them.</p> <p>While we understand that the identification of the customer for the DPTS provider may be based on the different sources of information in comparison with the traditional customer identification for the other financial institutions, the proposed alternative types of the information to be obtained to identify a customer in our view do not fully fit to the "identification" information about the customer during the standard CDD process. The items 1 and 2 refer to the "source of funds/source of wealth" usually collected if the customer falls into high-risk category of customers, which are usually PEPs or other categories of customers, considered being high-risk by the DPTS provider. this may be the case with the pseudonymous accounts and transactions.</p> <p>item 3 is usually the information already available to the DPTS provider when the blockchain transaction is being performed via the provider, and would be used by the DPTS provider to identify the customer and its ownership to the assets being subject to the transaction.</p> <p>As for items 4 and 5 - this information seems to be very similar to the one collected by the banks as a part of their AML/CFT controls in trade finance and correspondent banking, where the bank should consider obtaining additional information "<i>to assess financial crime risk specific to a trade finance transaction.</i>" (emphasis added, "AML/CFT CONTROLS IN TRADE FINANCE AND CORRESPONDENT BANKING").</p> <p>It makes sense to request additional information due to the fact that DPT transactions are rightly or wrongly, seen as high-risk profile transactions, as compared with other payment services and payments transactions, which is similar to trade finance to a certain extent.</p> <p>Accordingly, we are of the view that proposed alternative CDD information to be collected to identify a customer by the DPTS provider should be requested either in case of ECDD or when the transaction is identified by the provider as being high-risk transaction, but not necessarily as a standard operating procedure.</p>

S/N	Respondent	Full Responses from Respondent
9.	Cynopsis Solutions Pte. Ltd.	<p><b>General comments:</b></p> <p><b>Question 1: <u>Scope</u>.</b> 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.</p> <p>What if they are registered with other authority like MinLaw? Should MAS impose AML standard to all business type they do.</p> <p><b>Question 2: <u>Alignment with FATF Standards</u>.</b> 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.</p> <p>Perhaps MAS can consider the number of bank account a person is associated with and the number of wallets a person can hold.</p> <p>We realise that there is a conflicting of words in footnote 2 of the (Page 5) of the consultation paper against point 2.17a (Page 9) of the consultation paper.</p> <p>Footnote 2 mentioned that low risk activity (aka “exempted product”) would <u>not</u> need to comply with certain sections of PS Notice 01 while point 2.17a indicated that exempted product are to be subjected to all AML/CFT requirement. Perhaps MAS may want clarify further on this.</p> <p><b>Question 3: <u>AML/CFT Requirements for Offering of Exempted Products</u>.</b> 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. <i>(Please refer to paragraph 3.3 of the draft PS Notice 01)</i></p> <p>Under PS Notice 01, paragraph 3.3 - we noted that CDD would not be required. Perhaps MAS would like to clarify on this part.</p> <p>We also noted that there were no comments on cross border transfer, will there be any threshold on that?</p> <p><b>Question 4: <u>Simplified Due Diligence</u>.</b> MAS seeks comments on whether SCDD should be permitted for the various payment services covered under</p>

S/N	Respondent	Full Responses from Respondent
		<p><b>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)</b></p> <p>In referral to para 2.5 &amp; 2.18, it mentioned that MAS consider Activity F as “higher” risk. Thus, we are not sure how this is applicable for SCDD.</p> <p><b>Question 5. <u>Third Party Reliance</u>. 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)</b></p> <p>Personal view is that, there is no right or wrong in appointing 3rd party reliance. The payment service provider might not have the knowledge or expertise in KYC area. However, agreed on the point of 12.3 and 12.5 of the Notice 1.</p> <p><b>Question 6. <u>Correspondent Account Services</u>. MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 3.9 would be applicable to the Activity performed by your institution. (Please refer to paragraph 13 of the draft PS Notice 01 and paragraph 12 of the draft PS Notice 02)</b></p> <p>In referral to PS Notice 01 13.3a (iii) - other than the country of operation &amp; incorporation mentioned, I’m not sure how does the licensee can ensure that the respondent financial institution’s AML/CFT controls and ascertain that they are adequate and effective.</p> <p><b>Question 7. <u>Bearer Instruments and Cash Payouts</u>. MAS seeks comments on the proposal in paragraph 3.10 to apply the prohibition on issuance of bearer negotiable instruments and restriction of cash payout requirements to licensees which perform Activities A, B, C, F and G. (Please refer to paragraph 11 of the draft PS Notice 01 and paragraph 10 of the draft PS Notice 02)</b></p> <p>No comment, we leave it to MAS decisions</p> <p><b>Question 8. <u>Cross-border Transfer</u>. MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.</b></p> <p>No comment, we leave it to MAS decisions</p>

S/N	Respondent	Full Responses from Respondent
		<p><b>Question 9. <u>Wire Transfer Requirements for DPT Services.</u></b> 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. <i>(Please refer to paragraph 13 of the draft PS Notice 02)</i></p> <p>No comment, we leave it to MAS decisions</p> <p><b>Question 10. <u>Designated Threshold.</u></b> 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. <i>(Please refer to paragraph 6.3(b) of the draft PS Notice 02)</i></p> <p>From our company point of view, we think that conducting of CDD from the very first dollar is too much to ask for. If FATF is following USD 1,000 as a standard, not sure why are we not following it.</p> <p><b>Question 11. <u>CDD Information.</u></b> 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. <i>(Please refer to paragraph 6.6 of the draft PS Notice 02)</i></p> <p>It might be hard to track back to the initial source of fund</p>
10.	Ebuy Coin Pte. Ltd.	<p><b>Question 5. <u>Third Party Reliance.</u></b> MAS seeks comments on whether third party reliance is appropriate for the sector. <i>(Please refer to paragraph 12 of the draft PS Notice 01 and paragraph 11 of the draft PS Notice 02)</i></p> <p>Much of the business in this sector is conducted online, so there is a prevalent need for online non-face-to-face KYC.</p> <p>The risk of impersonation is the main risk inherent in knowing a customer online as opposed to face-to-face, as there is a lack of social cues and physical clues that come naturally with interacting with someone in person and being able to physically examine their ID documents.</p> <p>Mitigating the risk of impersonation brings us to the realm of digital forensics, which payment service companies may not have expertise in. As such I think it makes sense for payment service companies to have the option of engaging third party vendors, or other institutions that have refined their own online</p>



S/N	Respondent	Full Responses from Respondent
		<p>KYC processes, to help with some portion of the customer on-boarding process.</p> <p>On a related note – the current methods for online KYC employed by several digital asset institutions as well as eKYC vendors involve customers taking pictures or videos of themselves. Given the prevalence of publicly accessible counterfeiting technology, such as Deepfake technology, will MAS be providing any further specific guidelines on what constitutes adequate non-face-to-face KYC measures?</p> <p><b>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)</b></p> <p>For completeness, all sources of coins at one address or wallet may perhaps need to be identified.</p> <p>For example, Person A obtains 10 coins from Source B. Person A then obtains another 10 coins illicitly from Source C.</p> <p>Person A then spends 7 coins at Payment Institution 1, citing Source B as their originator, and spends another 7 coins at another Payment Institution 2, citing Source B again as their originator.</p> <p>Person A would then have been able to spend illicitly-obtained coins without links or checks being made on Source C.</p> <p>Also, as with other CDD information collected, the information will need to be verified in order for the check to be effective. A customer could potentially produce transaction information (transaction hash, timestamp, etc) that came from a fork, or a transaction that was never mined. The transaction information will need to be verified against the ledger on the main net.</p>
11.	Global Digital Finance	<p>Consultation Inputs</p> <p><b>Question 1: <u>Scope</u>. 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.</b></p>

S/N	Respondent	Full Responses from Respondent
		<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p><b>Question 2: <u>Alignment with FATF Standards.</u> 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.</b></p> <p>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.</p> <p>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</p>

S/N	Respondent	Full Responses from Respondent
		<p>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.</p> <p><b>Question 4: <u>Simplified Due Diligence.</u> 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)</b></p> <p>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.</p> <p>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.</p> <p><b>Question 5. <u>Third Party Reliance.</u> 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)</b></p> <p>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.</p> <p>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.</p>

S/N	Respondent	Full Responses from Respondent
		<p>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.</p> <p>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”.</p> <p>Fundamentally, the decision to place reliance should be a commercial decision, since the responsibility remains on the payment service licence holder.</p> <p>Further elaboration as follows.</p> <p><b>Risk</b> As mentioned in Q10.</p> <p><b>Restrictive to efficiency</b> 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.</p> <p>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.</p> <p><b>Restrictive to technology and innovation</b> 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.</p> <p>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.</p> <p>Virtual asset MPIs may provide a familiar platform for new players and innovators in the blockchain space to rely on for CDD.</p> <p>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.</p>

S/N	Respondent	Full Responses from Respondent
		<p><b>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.</b></p> <p>Although the FATF guidance<sup>4</sup> 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.</p> <p>Domestic value transfers of virtual assets can be identified via:</p> <ol style="list-style-type: none"> <li>Where the Beneficiary holds its wallet or public address in the same Singapore-licensed virtual asset service provider as the Originator.</li> <li>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".</li> </ol> <p>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").</p> <p>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.</p> <p>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.</p>

<sup>4</sup> <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>, note 113

S/N	Respondent	Full Responses from Respondent
		<p><b>Question 9. Wire Transfer Requirements for DPT Services.</b> 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)</p> <p>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<sup>5</sup>. In particular we draw MAS'</p> <p>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.</p> <p>Such infrastructure once created and agreed will likely be industry-led and global. In this regard, GDF is taking part in the V20 event<sup>6</sup> 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.</p> <p>The GDF response therefore recommends:</p> <ol style="list-style-type: none"> <li>1. Adoption of the information collection requirements highlighted in the FATF Guidance released on 21 June in note 114.<sup>7</sup></li> <li>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.</li> <li>3. A review in line with the 12-month review that the FATF will conduct to consider efficiency, effectiveness, and implementation by obliged entities.</li> </ol> <p><b>Question 10. Designated Threshold.</b> 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)</p> <p>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")</p>

<sup>5</sup> <https://www.gdf.io/wp-content/uploads/2018/01/GDF-Input-to-the-FATF-public-statement-of-22-Feb-2019-FINAL.pdf>

<sup>6</sup> <https://www.v20.io>

<sup>7</sup> <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>

S/N	Respondent	Full Responses from Respondent
		<p>will be conducted from the very first dollar of virtual asset transactions, even when dealing with occasional transactions.</p> <p>We do not consider this deviation from the FATF Recommendations to be appropriate as:</p> <ul style="list-style-type: none"> <li>• 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;</li> <li>• it could stifle the development of technology and innovation by deterring new investors or investment in new products;</li> <li>• 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.</li> </ul> <p>We elaborate below.</p> <p><b>Risk</b></p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Requiring CDD on all transactions therefore appears disproportionate to the ML/TF risks involved.</p> <p>It is unlikely that transactions for less than 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.</p>

S/N	Respondent	Full Responses from Respondent
		<p><b>Restrictive to technology and innovation</b></p> <p>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.</p> <p>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.</p> <p>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.</p> <p><b>FATF recommended threshold</b></p> <p>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’</p> <p><b>Question 11. CDD Information.</b> 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)</p> <p>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.</p> <p><b>DPT sending/receiving addresses</b></p> <p>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.</p> <p>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.</p>



S/N	Respondent	Full Responses from Respondent
		<p><b>Receipts/documentation on original purchase of cryptocurrency from an exchange or similar intermediary</b></p> <p>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.</p> <p>For customers new to virtual asset transactions, this information will not be available. We recommend against this requirement.</p> <p><b>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</b></p> <p>In itself, this information should be available and could be provided.</p> <p>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.</p> <p>For customers new to virtual asset transactions, this information will not be available.</p> <p><b>Reasons for purchase of DPT</b></p> <p>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.</p> <p><b>Reasons for current transaction, if applicable</b></p> <p>The answer immediately above equally applies here.</p>

S/N	Respondent	Full Responses from Respondent
12.	Naboo Ltd.	<p><b>General comments:</b></p> <p>Naboo proposes a new paragraph to be added to Annex B2 (“PS Notice 02”) in order to provide guidelines for the assertion of “source of funds” in transactions where the funds are in the form of DPT.</p> <p>Today’s industry standard to verify the source of funds procedure, is to track the DPTs up to the closest exchange, and if that exchange is regulated or has good international reputation, clear the DPTs presented in the transaction from any suspicion of ML/TF. This is, as we believe, performing AML/CTF test based on the meta and not based on the content.</p> <p>We propose to add this paragraph to Annex B2:</p> <p><b>Question 1: <u>Scope</u>. 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.</b></p> <p>We suggest that AML/CFT regulation be applied to all non-payment services when DPT is involved, for instance, the sell or brokerage of goods or real-estate. For example if a licensed FI (that performs activity F) is offering a service to hold funds as a trustee or custodian to its clients, for the purpose of a real-estate transaction with DPT, that transaction should be subject to AML/CFT scrutiny as if it was a pure financial transaction.</p> <p><b>Question 2: <u>Alignment with FATF Standards</u>. 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.</b></p> <p>With regards to decentralized VASPs, we propose to require AML/CFT checks from FIs (performing activity F) even if they are not the custodians of the funds (i.e. the FI is acting as a marketplace for clients to trade DPTs, peer-to-peer, with their own private wallets). Every DPT transactions performed under a licensed FI should be subject to ML/TF risk mitigation, without limitation on wallet custody.</p>

S/N	Respondent	Full Responses from Respondent
		<p>Another DPT related service that poses ML/TF risk is DPT trustees, that hold DPTs and potentially perform due-diligence for a pending transaction performed “off-chain” (i.e. outside the DPT domain, for example an exchange of goods).</p> <p><b>Question 3: <u>AML/CTF Requirements for Offering of Exempted Products.</u></b> 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. <i>(Please refer to paragraph 3.3 of the draft PS Notice 01)</i></p> <p>No Comments</p> <p><b>Question 4: <u>Simplified Due Diligence.</u></b> 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. <i>(Please refer to paragraph 8 of the draft PS Notice 01 and paragraph 7 of the draft PS Notice 02)</i></p> <p>Regarding SCDD on payment in DPTs for goods and services, in paragraph 3.1, item (ii) it is written that the transactions are funded from an “identifiable source”. “identifiable source” is defined in Annex B2 as an account which is maintained by a FI regulated by MAS or by another international authority which complies with FATF standards.</p> <p>This is, in our view, performing AML/CTF test based on the meta and not based on the content, in other words if the DPT in this said transaction are traced back to a regulated FI, all of the funds are cleared from ML/TF risk.</p> <p>We propose a different method for ML/TF risk mitigation, we propose that the source of funds (in case of DPT) be traced up to where the tokens were mined or issued (in the genesis block) by performing deep forensics on all blockchains (all kind of DPT) to mitigate the ML/TF risk that stems from coin mixers and exchange token pools.</p> <p><b>Question 5. <u>Third Party Reliance.</u></b> MAS seeks comments on whether third party reliance is appropriate for the sector. <i>(Please refer to paragraph 12 of the draft PS Notice 01 and paragraph 11 of the draft PS Notice 02)</i></p> <p>No Comments</p> <p><b>Question 6. <u>Correspondent Account Services.</u></b> MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 3.9 would be applicable to the Activity performed by</p>

S/N	Respondent	Full Responses from Respondent
		<p><b>your institution. (Please refer to paragraph 13 of the draft PS Notice 01 and paragraph 12 of the draft PS Notice 02)</b></p> <p>No Comments</p> <p><b>Question 7. <u>Bearer Instruments and Cash Payouts</u>. MAS seeks comments on the proposal in paragraph 3.10 to apply the prohibition on issuance of bearer negotiable instruments and restriction of cash payout requirements to licensees which perform Activities A, B, C, F and G. (Please refer to paragraph 11 of the draft PS Notice 01 and paragraph 10 of the draft PS Notice 02)</b></p> <p>No comments</p> <p><b>Question 8. <u>Cross-border Transfer</u>. MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.</b></p> <p>In our view, since DPT exists in multiple jurisdictions at the same time, cross-border should be judged based on the nationality and geographical location of the parties involved in the DPT transaction. In other words, if all parties of the DPT transaction are of the same nationality (SG) and reside within the same country (SG), then the transaction should be considered local, if one or more members of the involved parties are from another nationality or geographical location, then the transfer should be considered cross-border.</p> <p>Geographical location can be asserted by either CDD or Geo-IP positioning (in case of a client connecting online).</p> <p><b>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)</b></p> <p>With regards to DPT FATF's wire transfer requirements, in our view these requirements are applicable to DPT with some modifications. We propose the following modifications to the requirements:</p> <ol style="list-style-type: none"> <li>1. when the DPT transaction is peer-to-peer, FATF's requirements can be met.</li> <li>2. If the originator of an DPT transaction is a wallet in the custody of an exchange (FI performing activity F), then a source of funds check (in</li> </ol>

S/N	Respondent	Full Responses from Respondent
		<p>line with our comments to question 4) needs to be performed and added to the requirements. This is in order to uncover the “true” originator of the transaction masked by the FI’s token pools.</p> <p>3. If the originator or the beneficiary are a wallet attributed to a coin mixer (a wallet that performs many-to-many transactions in order to limit the traceability of DPT). A source of funds check (in line with our comments to question 4) needs to be performed and added to the requirements. This is in order to uncover the “true” originator or beneficiary of the transaction.</p> <p>With regards to Law Enforcement, in our view, the DPT wallet addresses involved in the transaction along with the KYC data attributed to each wallet and the “source of funds” report going back to the minting of the DPT for each wallet involved in the transaction.</p> <p><b>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)</b></p> <p>We agree (no comments), since DPT is a fertile ground for ML and TF, MAS should enforce strict regulation on the trade and use of DPT until such a time where the risk of ML and TF is reduced to a lower more acceptable level.</p> <p><b>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)</b></p> <p>In order not to reiterate, we propose that the “Source of funds” check be expanded beyond sending and receiving address and beyond the first “identifiable source” to include the complete history back to the minting of the DPT. This since that today’s system has inherent ML/DF risks since the source of funds check relies on the existence of regulation and not on the content of it. Our proposed method for “source of funds” check can be found in this document under our comments to question 4.</p>

S/N	Respondent	Full Responses from Respondent
13.	OKCoin Singapore	<p>Thank you for your continuous efforts in combating financial crimes and mitigating money laundering and terrorist financial risks. In light of the New Payment Services Bill, please see the following as our comments.</p> <p><b>1)</b> With reference to Section 3 Simplified Customer Due Diligence, paragraph 3.1 (as quoted below), we appreciate the implementation of a simplified customer due diligence on a risk-based approach.</p> <p><i>“3.1 Licensees should adopt a risk-based approach to performing CDD. Consequently, MAS intends to permit licensees carrying out Activities A, B, C, and F to perform simplified customer due diligence (“SCDD”) measures where:</i></p> <p><i>(i) the licensee is satisfied, upon the overall analysis of risks, that the ML/TF risks are low; or</i></p> <p><i>(ii) the services provided to such customer are cross border wire transfers conducted solely for the payment of goods and services to merchants, and the transactions are funded from an identifiable source. “</i></p> <p><b>Our comment:</b></p> <p>Our current business offers services to our customers with the fiat-to-token trading services. May I clarify if our services will fall into the consideration of 3 (ii) “payment of goods and services to merchants” when our customers deposit and withdraw their fiat currency and digital payment tokens into and out from our exchange trading platform?</p> <p><b>2)</b> With reference to paragraph 3.6 and 3.7 Third Party Reliance, it was stated that MAS is seeking for advice whether it is appropriate to have a third party to conduct the CDD/ onboarding function for the licensees.</p> <p><b>Our comment:</b></p> <p>We welcome MAS to allow licensees to have the CDD/ onboarding functions to be conducted by a third party who meet the AML KYC requirement set by the MAS and other international standards such as FATF. As our business is expanding globally, our company has our back office already set-up in one operating site to support all the operating branches from all over the world. We continue to ensure that our AML KYC policy and procedures are up to the local and international regulatory standards.</p>

S/N	Respondent	Full Responses from Respondent
		<p><b>3)</b> With reference to paragraph 5.6 and 5.7 Collection of CDD Information, it was mentioned that there are a few alternative Customer-specific information for CDD (as quoted below).</p> <p><i>“1. DPT Sending/ Receiving Addresses (“Source of funds”)</i></p> <p><i>2. Receipts/documentation on original purchase of cryptocurrency from an exchange or similar intermediary</i></p> <p><i>3. Transaction details in relation to original purchase of DPT – i.e. number (hash) of transactions, 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</i></p> <p><i>4. Reasons for purchase of DPT.</i></p> <p><i>5. Reasons for current transaction, if applicable.”</i></p> <p><b>Our comment:</b></p> <p>1. Each customer may have more than 1 wallet addresses. We think it is not practical to request the wallet address(es) from the customers during the CDD process. Besides that, according to the PS Notice 02 as stated in paragraph 5.2 (as quoted below), the originator information will be required to obtain and this information will be available upon request from the law enforcement agencies.</p> <p><i>“The cross-border value transfer requirements in PS Notice 02 will oblige licensees that facilitate the sending of DPTs to obtain and hold required and accurate originator information and required beneficiary information on DPT transfers, immediately and securely submit the above information to beneficiary DPTS providers and counterparts (if any), and make the information available on request to appropriate authorities. “</i></p> <p>We think that collection of the wallet address(es) of the customer as a mean of CDD shall be deemed unnecessary. In fact, every time when the customers deposit digital payment tokens to our platform, the wallet address(es) are recorded in the back-end system, according to the transaction behaviour. We think storing the transaction records would be a more practical approach to identify the actual source of fund of the customers.</p> <p>2. We think it is a good idea to generate a reference letter (as in the receipt/documentation) to show that the tokens are withdrawal (and previously</p>

S/N	Respondent	Full Responses from Respondent
		<p>traded, if applicable) on our exchange platform. So it is easier for regulators and law enforcement agencies to seek further assistance from us.</p> <p>3. When it was mentioned that the transaction details in relation to original purchase of DPT are required, may I clarify if it is referring to all the first-time deposit tokens to our exchange platform? For example, if the customer obtained 10 bitcoins from 10 different sources (one bitcoin from each source), does it mean that during the onboarding process, the customer needs to provide all the transaction details with regard to these 10 sources?</p> <p>We think a more practical way to do this is that, we could use the wallet address(es) which the customers have used in the token deposit as a unique identifier, in order to trace back all the transaction records of the customers on the blockchain upon request by the regulators or law enforcement agencies. All the transaction records should be available 24/7 on the blockchain and this information cannot be removed/ edited. The collection of the transaction records during the onboarding process shall be deemed unnecessary.</p> <p>4/ 5. Please clarify if the reasons of purchase/ current transaction only need to be obtained from the customers, or any verification would be required. We think that only collection is necessary during the onboarding process. When the customers are deemed suspicious, we shall pull out the entire KYC profiles and transaction history to assess the risk level of the customer and determine whether or not the reasons provided commensurate with the trading behaviour.</p> <p><b>4)</b> Apart from the above comments based on the Consultation Paper, we also have two more questions for your kind clarification</p> <p><b>Question 1:</b></p> <p>Our company operates an exchange platform to offer our customers with fiat-to-token trading services. During the onboarding/ CDD/ EDD process, it is difficult for us to conduct the review face-to-face with the customers. One way to enhance the verification part is that we ask our customers to take selfies with the passport and text on the top to show that they indeed intend to apply for an account at our platform, and/ or we request our customers to conduct a video verification with us. In the video verification, this will be conducted via the online software tools, such as Skype, and our customers will be required to read some statements or perform certain actions according to the instruction of our onboarding specialists</p>



S/N	Respondent	Full Responses from Respondent
		<p>We would like to confirm that the above process is acceptable by the MAS and whether the MAS has any requirement over the video recording tool to be used. So far, our company is using the publicly-available tools, such as Skype, instead of any in-house tools.</p> <p><b>Question 2:</b></p> <p>As part of the onboarding/ CDD/ EDD requirement, we require our corporate customers to provide the corporate structure and shareholder information if the shareholder is having 25% of shares or above. We have heard (but unofficially) from other sources that there may be requirement over the corporate voting structure as well, in addition to the shareholding structure. That means the people who have the voting right of 25% or above should provide their CDD information as part of the review. However, our current practice only considers the shareholding structures (25% or above rule), and we did/ do not require our corporate customers to provide the voting structure.</p> <p>We would like to seek clarification from the MAS whether or not we could follow our existing procedures regarding the collection of information on the corporate shareholding structure (25% or above rule) will suffice, and no collection of information on the corporate voting structure.</p> <p>Kindly consider the comments and suggestions made above. We are keen to apply for the license once the MAS has published the detailed guidance and requirements.</p> <p>We always support the efforts of the global standard setters, national authorities and regulators to continuously work with the industry to enhance the regulations. This industry keeps evolving and we are still in the early stage to see how it will emerge into. We are committed to embrace the change with our regulators to ensure that we continue to combat financial crime effectively.</p> <p>Should you have any questions, please feel free to reach out to me at <a href="mailto:christy.ho@okcoin.com">christy.ho@okcoin.com</a> or +852 9264-1912.</p>
14.	RazerPay Pte. Ltd.	<p><b>General comments:</b></p> <p><b>Question 1: <u>Scope</u>.</b> 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</p>

S/N	Respondent	Full Responses from Respondent
		<p><b>payment service providers have been exempted from the application of such requirements under the regulatory authority.</b></p> <p><i>With regards to imposing AML/CFT requirements for other non-payment services activities, Razer Pay is suggesting that the requirements should subject to the licensee's internal risk assessment and holistic monitoring of ML/TF risks across the business activities. There should not be any prescriptive AML/CFT requirements that licensees need to adhere to as the non-payment service business activity is already subject to exemption by other regulatory authorities on the basis of its low ML/TF risks.</i></p> <p><i>Razer Pay would like to suggest MAS to provide guidance on the list of business activities that might fall within the above exemption. This will be helpful to payment service provider to be guided should the licensee is required to notify MAS on the exempted business activity.</i></p> <p><b>Question 2: <u>Alignment with FATF Standards.</u> 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.</b></p> <p><i>Razer Pay has no comments with regards to this question as we do not offer DPT business activity currently.</i></p> <p><b>Question 3: <u>AML/CFT Requirements for Offering of Exempted Products.</u> 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)</b></p> <p><i>Razer Pay is in support of the exemption provided in paragraph 3.3. of the draft Notice.</i></p> <p><b>Question 4: <u>Simplified Due Diligence.</u> 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)</b></p> <p><i>Suggest MAS to include what are the acceptable measures to be included as SCDD process. Measures suggested include:</i></p>

S/N	Respondent	Full Responses from Respondent
		<ul style="list-style-type: none"> <li>• <i>Identify and verify the customer identity by collecting customer information;</i></li> <li>• <i>funding e-money account from a bank account, payment card or from identifiable resources</i></li> <li>• <i>Verifying the customers name or identity card with a banking institution or an issuer of payment card.</i></li> </ul> <p><b>Question 5. <u>Third Party Reliance.</u> 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)</b></p> <p><i>Razer Pay is supporting third-party reliance as it affords greater flexibility to perform measures required by para 7, 8 and 9 of the draft Notice. Less infrastructure is required to complete the required AML measures and it enhances customer experience as users need not go through the AML/CFT-required process when they have undergone the same with the “third party”.</i></p> <p><i>For clarity, suggest to include definition/clarification third party reliance does not apply to outsourcing or agency relationships as per FATF Interpretive Note.</i></p> <p><b>Question 6. <u>Correspondent Account Services.</u> MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 3.9 would be applicable to the Activity performed by your institution. (Please refer to paragraph 13 of the draft PS Notice 01 and paragraph 12 of the draft PS Notice 02)</b></p> <p><i>Currently Razer Pay does not provide any correspondent banking service or intend to engage any FIs for correspondent account services.</i></p> <p><b>Question 7. <u>Bearer Instruments and Cash Payouts.</u> MAS seeks comments on the proposal in paragraph 3.10 to apply the prohibition on issuance of bearer negotiable instruments and restriction of cash payout requirements to licensees which perform Activities A, B, C, F and G. (Please refer to paragraph 11 of the draft PS Notice 01 and paragraph 10 of the draft PS Notice 02)</b></p> <p><i>Razer Pay is in support of the restriction on issuance of bearer negotiable instruments and restriction of cash payouts. However, with regards to cash payouts the threshold might need to be increased as there are still demands for cash payouts from customers. This is to address the need from travellers, workers who are paid in cash and payments for transactions which needs to be made in cash.</i></p>

S/N	Respondent	Full Responses from Respondent
		<p><b>Question 8. <u>Cross-border Transfer</u>.</b> MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.</p> <p><i>Razer Pay has no comments with regards to this question as we do not provide DPT activities as defined by the draft PSA.</i></p> <p><b>Question 9. <u>Wire Transfer Requirements for DPT Services</u>.</b> 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. <i>(Please refer to paragraph 13 of the draft PS Notice 02)</i></p> <p><i>Razer Pay has no comments with regards to this question as we do not provide DPT activities as defined by the draft PSA.</i></p> <p><b>Question 10. <u>Designated Threshold</u>.</b> 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. <i>(Please refer to paragraph 6.3(b) of the draft PS Notice 02)</i></p> <p><i>Razer Pay has no comments with regards to this question as we do not provide DPT activities as defined by the draft PSA.</i></p> <p><b>Question 11. <u>CDD Information</u>.</b> 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. <i>(Please refer to paragraph 6.6 of the draft PS Notice 02)</i></p> <p><i>Razer Pay has no comments with regards to this question as we do not provide DPT activities as defined by the draft PSA.</i></p>
15.	Refinitiv	<p style="text-align: center;"><b><u>Consultation Responses</u></b></p> <p><b>Question 1: <u>Scope</u>.</b></p> <p>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.</p>

S/N	Respondent	Full Responses from Respondent
		<p><b>Response:</b> We agree with the proposed changes.</p> <p><b>Question 2: <u>Alignment with FATF Standards.</u></b></p> <p><b>MAS seeks comments on the proposed requirements in paragraph 2.8, in relation to transfer of digital payment transfer (DPT) and custodian wallet services. MAS also welcomes suggestions on other types of DPT-related services that a digital payment token service providers (“DPTS providers”) provider could be involved in and which may pose ML/TF risk, necessitating application of AML/CFT measures as well.</b></p> <p><b>Response:</b> We agree activities that fall under category F by DPTS are of higher risk and welcome MAS efforts to bring Virtual Asset Service Providers (VASPs) in line with FATF standards. Refinitiv would encourage the MAS to note in its guidance that Designated Non-Financial Business or Professions (DNFBPs) should also carry out CDD when providing services to DPTS, which is also recommended by FATF. For example, legal firms providing advice on initial coin offerings (ICOs) or other fund raising activities should be carrying out CDD on their customers as that activity has been shown to be at high risk for fraud.</p> <p><b>Question 3: <u>AML/CFT Requirements for Offering of Exempted Products –</u></b></p> <p><b>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).</b></p> <p><b>Response:</b> No comment.</p> <p><b>Question 4: <u>Simplified Due Diligence.</u></b></p> <p><b>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).</b></p> <p><b>Response:</b> While we recognize that there are scenarios where an activity is low risk we would encourage the MAS to consider adding in a requirement that firms that conduct SCDD be wary of multiple transactions by interlinked clients that aim to avoid the threshold in 3.2 (i). Trade based money laundering and financial crime more generally can only be identified in certain circumstances through transaction surveillance that would show when smaller transactions by multiple accounts are being used to avoid compliance. Firms should be aware that there are risks even if the specific transaction is low. In certain cases transaction monitoring may be necessary to ensure that payment firms can determine when customers are potentially</p>

S/N	Respondent	Full Responses from Respondent
		<p>transacting in a way that evades CDD. One example could be breaking down one transaction into multiple transactions to ensure they are within the SCDD limit.</p> <p><b>Question 5: <u>Third Party Reliance.</u></b></p> <p><b>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)</b></p> <p><b>Response:</b> We are supportive of the MAS' clarifications on third party reliance and the changes recommended regarding VASPs. The criteria closely follow what is already practiced in the industry and ensures that innovative companies have access to compliance systems that can help them effectively mitigate financial crime risk.</p> <p>We would encourage the MAS to provide clarification on whether 3<sup>rd</sup> country equivalence decisions would be allowed for certification of 3<sup>rd</sup> party systems. This would reduce the chance that certification of verification is duplicative.</p> <p><b>Question 6: <u>Correspondent Account Services</u></b></p> <p><b>MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 3.9 would be applicable to the Activity performed by your institution. (Please refer to paragraph 13 of the draft PS Notice 01 and paragraph 12 of the draft PS Notice 02)</b></p> <p><b>Response:</b> No comment.</p> <p><b>Question 7: <u>Bearer Instruments and Cash Payouts</u></b></p> <p><b>MAS seeks comments on the proposal in paragraph 3.10 to apply the prohibition on issuance of bearer negotiable instruments and restriction of cash payout requirements to licensees which perform Activities A, B, C, F and G. (Please refer to paragraph 11 of the draft PS Notice 01 and paragraph 10 of the draft PS Notice 02).</b></p> <p><b>Response:</b> We agree with this proposal.</p> <p><b>Question 8: <u>Cross-border Transfer</u></b></p> <p><b>MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.</b></p> <p><b>Response:</b> We agree with the proposal that DPT transactions should be considered cross border in nature as it is of higher risk and aligns with FATF</p>

S/N	Respondent	Full Responses from Respondent
		<p>requirements. An example we would highlight are the technological challenges in identifying sender, recipient and financial value when privacy coin transactions are initiated. We believe privacy coins should be flagged or treated with a higher risk profile and encourage MAS to specify guidelines around these.</p> <p><b>Question 9: <u>Wire Transfer Requirements for DPT Services</u></b></p> <p><b>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)</b></p> <p><b>Response:</b> Refinitiv believe that DPT service providers should adhere to the FATF wire transfer requirements and at a minimum collect</p> <ul style="list-style-type: none"> <li>• The full name of the originator</li> <li>• The originators account number or Public Key</li> <li>• The originators address</li> <li>• National Identity Number</li> <li>• Beneficiary account number or Public Key</li> <li>• Unique transaction reference number for batch transactions</li> </ul> <p>The information collected above should be transmitted as part of all wire transfers pertaining to DPT and stored by the sending and receiving institutions. The information collected can be fed into existing transactional monitoring systems that are designed to detect and flag suspicious transactions in line with existing practices and systems (e.g. the process followed by banks using the SWIFT network for wire transfers).</p> <p><b>Question 10: <u>Designated Threshold</u></b></p> <p><b>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).</b></p> <p><b>Response:</b> We believe that MAS should follow FATF guidelines regarding designated thresholds for CDD when conducting DPT transactions. This will prevent fragmentation between jurisdictions regarding the implementation of these DPT CDD requirements helping to reduce compliance and technology costs. It also helps to ensure that firms mitigate risks regarding “smurfing” or “structuring” of payments to avoid compliance thresholds where these transactions would be flagged as high risk.</p> <p><b>Question 11: <u>CDD Information</u></b></p>



S/N	Respondent	Full Responses from Respondent
		<p><b>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).</b></p> <p><b>Response:</b> We agree with the proposed recommendation.</p>
16.	<p>RHTLaw Taylor Wessing LLP</p> <p>RHT Compliance Solutions</p> <p>InvestaCrowd</p> <p>Tilde Pte. Ltd.</p>	<p><b>General comments:</b></p> <p>We are generally supportive of the proposals. However, MAS (and the financial industry) could reconsider the concept of “identity”, and consider new forms of data identifiers for AML/KYC purposes. Technological innovation is making it much easier and de rigueur for online non-face-to-face transactions and interactions to take place. However, much of AML/KYC processes are still reflective of an “offline” world and face-to-face transactions. In this regard, we urge and welcome MAS to engage industry and businesses in roundtable discussions and/or issue guidelines on acceptable AML/KYC standards for banks in on-boarding companies involved in crypto-assets, crypto-currencies, and similar types of digital businesses.</p> <p><b>Question 1: Scope.</b> 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.</p> <p>We are generally supportive of the proposal to impose such requirements. However, MAS could consider whether this proposal may result in an unlevel playing field between payment service providers (“PSPs”) who are required to comply with the MAS notices and unlicensed entities conducting the same activities but exempted out of the applicable AML requirements for unregulated activities. MAS could also clarify whether PSPs whose business concern asset-backed tokens are subject to both the regulations under the PS Act such as PS Notice 02, and the Precious Stones and Precious Metals Prevention of Money Laundering and Terrorism Financing Act 2019 (“PSPM”).</p> <p><b>Question 2: Alignment with FATF Standards.</b> 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</p>



S/N	Respondent	Full Responses from Respondent
		<p>may pose ML/TF risk, necessitating application of AML/CFT measures as well.</p> <p>We are generally supportive of the proposed requirements that align with FATF Standards. However, under the FATF standards, virtual asset services providers (“VASPs”), VASPs include entities who participate in and provide financial services related to an issuer’s offer and/or sale of a virtual asset (“ICO services”). MAS could clarify whether ICO services, and advisory services for non-securities token issuances will require licensing and be subject to the AML/CFT measures.</p> <p><b>Question 3: <u>AML/CFT Requirements for Offering of Exempted Products.</u> 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)</b></p> <p>We have no comments on this.</p> <p><b>Question 4: <u>Simplified Due Diligence.</u> 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)</b></p> <p>Generally, SCDD should be permitted. However, clarifications could be made with regard to SCDD conditions and scenarios listed above. Currently, customers who have higher risk characteristics include (i) domestic or international organisation politically exposed persons, or (ii) a family member or close associate of a politically exposed person, (iii) customers from a high risk third country identified by the Financial Action Task Force (“FATF”), (iv) customers from or in a country or jurisdiction known to have inadequate AML/CFT measure.</p> <p>Further clarifications could also be made about whether PSPs may conduct SCDD when dealing with another licensed financial institution or entity. For illustration purposes, could a PSP conduct SCDD when dealing with a licensed broker, dealer or fund manager (with a Capital Markets Services) Licence?</p> <p>MAS may wish consider to impose other conditions, wherein PSPs will apply SCDD when they ensure (i) the customer is seen face to face, (ii) the source of funds or wealth are transparent and understood by the PSPs, (iii) where</p>

S/N	Respondent	Full Responses from Respondent
		<p>the customer is not an individual, that there is no beneficial ownership beyond that legal entity.</p> <p>Instead of capping the annual cumulative transactions at S\$20,000, MAS could also broaden this condition and allow PSPs to conduct SCDD when transactions are not complex or unusually large, over \$1million, although PSPs' own risk assessment may indicate that a lower sum would be considered large.</p> <p>Currently, MAS defines "politically exposed person[s]" ("PEP") as "natural person[s] who [have] been entrusted with prominent public functions in a foreign country. MAS could also consider listing traits of a lower risk PEP who do not require Enhanced CDD. According to the UK's Money Service Business Guidance for Money Laundering Supervision, lower risk politically exposed persons possess traits such as, "low levels of corruption", "political stability and free and fair elections", "strong state institutions where accountability is normal", "credible anti-money laundering measures", "a free press with a track record for probing official misconduct", "an independent judiciary and a criminal justice system free from political interference", "a track record for investigating political corruption and taking action against wrongdoers", "strong traditions of audit within the public sector", "legal protections for whistle blowers", "well-developed registries for ownership of land, companies and equities". In other words, unlike the current proposed approach, the UK does not predetermine all PEPs as higher risk, there is a category of PEPs who are lower risk PEPs. MAS could consider this tiered approach.</p> <p>MAS could consider issuing guidelines on conditions and scenarios where SCDD should not continue. E.g. when doubts/suspicion is raised about whether documents obtained for identification are genuine.</p> <p><b>Question 5. <u>Third Party Reliance.</u> 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)</b></p> <p>We are generally supportive of the view that third party reliance is appropriate for the sector.</p>

S/N	Respondent	Full Responses from Respondent
		<p>Currently, third parties include “(a) a financial institution set out in Appendix 2;<sup>8</sup> (b) a financial institution which is subject to and supervised by a foreign authority for compliance with AML/CFT requirements consistent with standards set by the FATF (other than a holder of a payment services licence or equivalent licence); (c) the parent entity, the branches and subsidiaries of the parent entity, and other related corporations, of a payment service provider (other than a holder of a payment services licence or equivalent licence).” See para 12, PS Notice 01; see also para 11, PS Notice 02.</p> <p>However, it is unclear whether PSPs are able to rely on third parties, whose branch or subsidiary established in a high risk country, or is not supervised a foreign authority, but fully complies with an European Economic Area (EEA) or FATF low risk parent’s procedures and policies. For illustration purposes, if a third party’s branch is established in Philippines, and is not subject to supervision by the Philippines authorities for compliance with AML/CFT requirements consistent with standards set by the FATF, but it fully complies with an Economic Area (EEA) or FATF low risk parent’s procedures, could PSPs rely on this third party’s subsidiary in Philippines to perform certain elements of CDD? Such clarifications could also be issued through additional guidelines by MAS.</p> <p>While third party reliance is appropriate, MAS could consider allowing licensees to rely on a branch or subsidiary established in a high risk country who fully complies a low risk parent’s (e.g. regulated by an European Economic Area / US authority / authority who implements FATF standards) procedures and policies.</p> <p>MAS could also consider clarifying whether third party reliance may be permitted for licence holders who: (i) engage in proprietary trading for hedging or speculative purposes in payment tokens on exchanges in other jurisdiction (e.g. Binance, Huobi), or (ii) engage in principal trades for client accounts to provide liquidity through an electronic platform to a bank (on behalf of its customers), and (iii) have no control over who the counter-party is or what Know-Your-Customer (KYC) checks have been performed. These licence holders will be unable to conduct KYC checks and MAS could consider clarifying whether PSPs may rely on exchanges’ KYC/AML protocols.</p>

<sup>8</sup> Appendix 2 includes licensed banks, merchant banks approved under section 28 of the Monetary Authority of Singapore Act, licensed finance companies under the Finance Companies Act, licensed financial advisers under Financial Advisers Act, holders of a capital markets services licence, fund management companies, persons exempted under s 23(1)(f) of the Financial Advisers Act, exempted persons under s 99(1)(h) of the SFA, approved trustees under s 289 of the SFA, trust companies licensed under s 5 of the Trust Companies Act, direct life insurers licensed under s 8 of the Insurance Act, and insurance brokers registered under the Insurance Act.

S/N	Respondent	Full Responses from Respondent
		<p>Third party reliance is especially appropriate for licensees including DPT service providers, and MAS could consider including other third party providers in the digital payment token (or virtual assets) space which are dedicated to tracking the source of funds of digital payment tokens and fraud detection.</p> <p><b>Question 6. <u>Correspondent Account Services</u>.</b> MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 3.9 would be applicable to the Activity performed by your institution. <i>(Please refer to paragraph 13 of the draft PS Notice 01 and paragraph 12 of the draft PS Notice 02)</i></p> <p>We have no comments on this.</p> <p><b>Question 7. <u>Bearer Instruments and Cash Payouts</u>.</b> MAS seeks comments on the proposal in paragraph 3.10 to apply the prohibition on issuance of bearer negotiable instruments and restriction of cash payout requirements to licensees which perform Activities A, B, C, F and G. <i>(Please refer to paragraph 11 of the draft PS Notice 01 and paragraph 10 of the draft PS Notice 02)</i></p> <p>We have no comments on this.</p> <p><b>Question 8. <u>Cross-border Transfer</u>.</b> MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.</p> <p>We are of the view that not all DPT value transfers should be considered cross-border transfers.</p> <p>On one hand, a case can be made for having all value transfers of DPT to be considered cross-border. The FATF's Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers supports this view. As value transfers of DPT essentially involve the transfer of virtual assets, with PSPs hosting their servers on various countries, the transfer of DPT goes beyond the physical jurisdiction of Singapore and should be considered cross-border nature.</p> <p>However, if a natural person (A), who is presently residing in Singapore, makes a value transfer of DPT to another natural person (B), who is also presently residing in Singapore, should this transfer be considered cross-border in nature? Perhaps, MAS could consider exception and find that certain value transfer of DPT within Singapore between two natural persons residing in Singapore are not considered cross-border.</p>

S/N	Respondent	Full Responses from Respondent
		<p><b>Question 9. <u>Wire Transfer Requirements for DPT Services.</u></b> 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. <i>(Please refer to paragraph 13 of the draft PS Notice 02)</i></p> <p>We have no comments on this.</p> <p><b>Question 10. <u>Designated Threshold.</u></b> 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. <i>(Please refer to paragraph 6.3(b) of the draft PS Notice 02)</i></p> <p>MAS may wish to consider defining occasional transactions by setting a designated threshold for DPT transactions. According to the FATF Recommendation 10, “The occasional transactions designated threshold above which VASPs [or DPT payment] are required to conduct CDD is USD/EUR 1 000”.<sup>910</sup></p> <p>Instead of requiring CDD to be conducted from the first dollar, MAS could consider setting a threshold, finding that a person to be engaging in occasional transaction of DPT if the total amount of value transfers of DPT does not exceed US\$1,000 or its equivalent in Singapore currency, below which CDD need not apply.</p> <p><b>Question 11. <u>CDD Information.</u></b> 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. <i>(Please refer to paragraph 6.6 of the draft PS Notice 02)</i></p> <p>MAS proposed alternative CDD information to be collected, including (i) DPT Sending/ Receiving Addresses (“Source of funds”), (ii) Receipts/ documentation on original purchase of cryptocurrency from an exchange or similar intermediary, (iii) Transaction details in relation to original purchase of DPT – i.e. number (hash) of transaction, value of transaction (e.g. 2</p>

<sup>9</sup> See FATF’s Public Statement – Mitigating Risks from Virtual Assets [<https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html>]

<sup>10</sup> See also Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, [www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html](http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html)

S/N	Respondent	Full Responses from Respondent
		<p>Bitcoins), timestamp, fee (cost of transaction), size of transaction (in bytes), funds balance history in the address, message recorded in transaction, (iv) Reasons for purchase of DPT, and (v) Reasons for current transaction, if applicable. We believe that the above-mentioned information could supplement or replace existing identifiers for CDD purposes.</p> <p>However, MAS could consider the practicability of collecting the proposed alternative CDD information. For illustration purposes, if 1 bitcoin is made up of many different input transactions,<sup>11</sup> and such inputs are determined differently by different exchanges, it might be practically impossible to merely indicate a transaction hash or “receipt” for any single given transaction.</p>
17.	<p>SingCash Pte Ltd</p> <p>Telecom Equipment Pte Ltd</p> <p>Singtel Mobile Pte Ltd</p> <p>[collectively known as ‘Singtel’]</p>	<p><b>General General comments:</b></p> <p>Singtel welcomes the MAS’ consultation and effort to obtain and solicit feedback on the combined AML/CFT obligations that would apply to Payment Institutions (<b>PIs</b>) under the Payment Services Act (<b>PSA</b>).</p> <p>Singtel has comments on the following issues:</p> <ul style="list-style-type: none"> <li>• lack of clarity over payments for goods and services;</li> <li>• need for guidelines and clarity on enforcement of the PSA to ensure that parties do not avoid licensing ;</li> <li>• need for clarity over offer of multiple products;</li> <li>• application of AML/CFT approach across enterprise;</li> <li>• reviewing criteria ;</li> <li>• applying Simplified CDD as a default;</li> <li>• reliance on third parties; and</li> <li>• other comments including screening, wire transfers and agents</li> </ul> <p><b>Question 1: <u>Scope</u>. MAS seeks comments on the proposal in paragraph 2.3 to additionally impose Anti-Money Laundering and Countering the</b></p>

<sup>11</sup> Suppose the transaction of 1 bitcoin is made up of 0.1 bitcoin from mining, 0.1 bitcoin from small payment, 0.25 bitcoin from exchange A, 0.25 bitcoin from exchange B, and 0.3 bitcoin from a completely undocumented source.

S/N	Respondent	Full Responses from Respondent
		<p><b>Financing of Terrorism (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.</b></p> <p><u>Response</u></p> <p>Singtel agrees with the proposal in the Draft Notice to Payment Service Providers on Prevention of Money Laundering and Countering the Financing of Terrorism (<b>PS Notice 01</b>) that parties who offer low risk services or products be exempted from the AML/CFT requirements. That said, Singtel has concerns, which are:</p> <ul style="list-style-type: none"> <li>(a) There is a lack of clarity regarding enforcement in particular over payments for goods and services <ul style="list-style-type: none"> <li>(i) Services, products and commercial offerings in the digital payments world are dynamic and fluid. As such, whilst the MAS has proposed objective criteria, eg in the form of wallet limits, ensuring that payments are for goods and services or capped at certain amounts, it is not clear to us how these can be enforced. For example, there is no guidance on how a company should substantiate that a payment is for goods and services. This is in particular of interest to us given that there are payments in Singapore facilitated through market places [eg Carousell] where the payments are made directly to individuals.</li> <li>(ii) Consequently, Sections 7.51 – 7.54 and Section 15 of the Draft PS Notice 01 may in fact be unenforceable given that it is not possible for a Payment Service Provider (<b>PSP</b>) or a Payment Institution (<b>PI</b>) to know in advance the merchants involved in a payment for goods and services in order to perform screening of merchants. It is also not practical to acquire and then supply the recipient information in relation to these wire transfers. We elaborate on this further in the section on AML/CFT for Exempted Products and the section on Wire Transfers below.</li> </ul> </li> <li>(b) Need for guidelines and clarity on enforcement of the PSA</li> </ul>

S/N	Respondent	Full Responses from Respondent
		<p>(i) The MAS has already proposed that parties can obtain exemptions from being a Standard Payment Institution<sup>12</sup>; coupled with the MAS proposal to exempt PSPs from AML/CFT obligations for low-risk [also known as ‘Exempted Products’], this may result in a situation where there are providers who are not licensed and /or purport to offer low risk products and therefore are not subject to any oversight. In short, there is a risk that companies could simply hover under the thresholds of a Major PI and never be subject to any regulatory requirements. We believe that this defeats the purpose of the PSA. Whilst we see the logic in calibrating regulation according to size and operations, it has always been a matter of concern that licensees may be operating in such a way as to avoid / escape scrutiny over their operations. We ask that the MAS considers how this can be reviewed, eg where a licensee is exempted from AML/CFT obligations, they should not then be subject to the class exemption from obtaining an SPI licence. We also ask for guidelines or clarity on how the MAS will enforce the PSA to ensure that parties do not purport to qualify for exemption and therefore escape regulatory scrutiny.</p> <p>(ii) Furthermore, the MAS may also wish to publish a list of PSPs that are exempted and allow for the exemptions to expire every six (6) months unless the PSP can provide proof or substantiation that its operations still comply with the regulations or requirements set in place by the MAS.</p> <p><b>Question 2: <u>Alignment with FATF Standards</u>. 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.</b></p> <p><u>Response:</u></p>

<sup>12</sup> MAS proposes to grant class exemptions from licensing to entities that would otherwise have been required to hold a standard payment institution licence but do not pose sufficient ML/TF risks in its Proposed Payment Services Regulations.



S/N	Respondent	Full Responses from Respondent
		<p>NA</p> <p><b>Question 3: <u>AML/CFT Requirements for Offering of Exempted Products.</u></b>  <b>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)</b></p> <p><u>Response</u></p> <p>Whilst Singtel is supportive of an environment where less onerous obligations apply in relation to exempted products, we are concerned that the MAS' consultation and /or proposal leave some grey areas:</p> <p>(a) We seek clarity as to how the MAS looks at products. For example, a company offers multiple products to ONE customer.</p> <p>(i) Product A allows the customer to have cross border transfer of funds using an identifiable source of funds but the wallet is capped at S\$1000;</p> <p>(ii) Product B allows the customer to engage in domestic transfer of funds using an identifiable source of funds and the wallet is also capped at S\$1000; and</p> <p>(iii) Product C caps the customer's wallet at S\$3000 and allows the customer to engage in domestic money transfer for payments of goods and services using <i>any</i> source of funds.</p> <ul style="list-style-type: none"> <li>• Under S24 of the PSA, the MAS expects a Major PI to aggregate all the values of any payment account [an e-wallet also functions as a payment account] to one customer [identified using a unique identifier] such that the total value does not exceed the S\$5000.</li> <li>• This means that even if a Major PI intends to mitigate all the risks involved such that the customer can only engage in limited non-low risk activities, it is expected to aggregate all the wallet values and subject that to a hard cap of S\$5000. Furthermore, the annual value of transactions by the same customer is limited to S\$30,000.</li> <li>• This also means that when the MAS exempts all Standard PIs who offer low risk products, it could encourage construction</li> </ul>

S/N	Respondent	Full Responses from Respondent
		<p>of products that escape scrutiny – eg if the Standard PI is not capped at total wallet or account limit of S\$5000, they could in effect simply offer multiple low risk products and then only subject one high risk product (in this case Product C) to the CDD obligations. The same Standard PI is still not required to cap the total amount spent by the customer to S\$5000 or the annual spend to S\$30,000.</p> <p>(b) Limiting annual transactional values of a customer to S\$30,000</p> <ul style="list-style-type: none"> <li>Major PIs are limited to providing e-wallets of no more than S\$5,000 and not allowing their consumers to transact more than S\$30,000 on a per annum basis.</li> <li>Given that the scale of a Major PI is clearly larger than that of a standard PI and given that a customer who wishes to transact at more than S\$30,000 may in turn be using a product that is not exempted [ie not a low-risk for AML/CFT purposes], it is not reasonable to cap the Major PI at an annual transactional value of S\$30,000 per annum per customer. We ask the MAS to consider removing this annual limit to provide a more level playing field to facilitate the Major PIs. Alternatively, MAS may consider guidelines to allow Major PIs to continue to provide payment services to such customers after further prescribed checks, or to allow Major PIs to continue to provide low risk payment services to such customers notwithstanding that they have reached the S\$30,000 limit.</li> </ul> <p>(c) Application of AML/CFT across enterprise</p> <p>(i) In paragraph 2.3 of the Consultation, the MAS indicates that it generally does not encourage PIs to conduct activities outside of payment services unless these are incidental and supportive of their primary business model and AML/CFT obligations could be imposed on such primary businesses.</p> <p>(ii) We are concerned that the MAS is consulting on the AML/CFT obligations for such other businesses separate from the ongoing consultation. It is more useful for the MAS to carry out a consolidated review so that interested parties have a complete overview of what may apply to all their businesses.</p>

S/N	Respondent	Full Responses from Respondent
		<p>(iii) In any case, it is also not clear to us how the MAS intends to regulate or impose AML/CFT obligations on services that are not licensable by the MAS under any legislation, whether under the PSA or other applicable legislative instruments that empowers the MAS. In many cases, these other operations may be so distinct and /or regulated by other legislations that it may not be practicable for the MAS to expect any form of AML/CFT compliance. We quote for example a case where utilities companies may choose to engage in Activity A. It appears that the Utility Company needs to apply AML/CFT requirements on all its activities, including the provision of utilities [water, power etc] when none of these other activities are licensable under the PSA.</p> <p>(d) Payments for Goods and Services</p> <p>(i) We appreciate that the MAS has not dictated how they would determine whether a transaction is a payment for goods and service. We propose that transactions that are payments to a merchant acquired by the PI or to a merchant acquirer be regarded as payments for goods and services and not for other purposes as it is impractical to ask for proof or details of the transaction in every case.</p> <p>(ii) Nonetheless, we note that even where the PI wishes to comply with AML/CFT obligations for these payments, there are practical issues which we cite below.</p> <p>(iii) First, it is not possible for a PI to know in advance the merchants involved in a payment for goods and services. Such payments are dynamic and it is impractical for a customer to lodge details first with the PI, wait for the PI to carry out screening on the merchant and then allow the payment transaction to proceed before the customer can then walk away with the goods and services. We note that increasingly, payments for goods and services are being transacted on the go, with numerous merchants being on-boarded and overseas merchants getting on board. Many merchants are also on-boarded by merchant acquirers and not directly by the PI that is involved in the transaction. There is no way for a PI to screen the thousands of merchants that can possibly be involved with these forms of payments.</p>

S/N	Respondent	Full Responses from Respondent
		<p>(iv) Second, it is also not practical to acquire and then supply the recipient information in relation to these wire transfers (if payments for goods and services are in fact still considered wire transfers) given that there is generally low AML/CFT risks associated with payments for goods and services and the nature of the goods / merchants may vary from time to time.</p> <p>(v) We ask that the MAS permits the PI to implement compliance with AML/CFT obligations for such payments as to take into account the practical difficulties. For example, we propose:</p> <ul style="list-style-type: none"> <li>• removing the need for screening of the merchants and/or providing the required wire transfer information;</li> <li>• requiring the PI to introduce a framework that mitigates the risks, eg carrying out due diligence on merchant acquirers, where possible, implementing velocity checks.</li> </ul> <p><b>Question 4: <u>Simplified Due Diligence</u>. 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)</b></p> <p><u>Response</u></p> <ul style="list-style-type: none"> <li>• We support permitting Simplified Customer Due Diligence for any service that is subject to the CDD obligations in the Notice. In fact, we note that the MAS should consider a phased approach in the proposed notice that permits a PI to first commence Simplified CDD and then progress onto a Standard form of CDD. This levels the playing field so that all parties can commence using a Simplified form of CDD.</li> <li>• We propose this because PIs who are exempted from licensing and who offer exempted products effectively do not carry out any form of CDD. So a major PI who may for example offer a wallet of more than \$1000 [but offer payments with identifiable source of funds] effectively has to perform a Standard form of CDD unless it substantiates that the risks are low. Furthermore, the Major PI cannot perform Simplified CDD when</li> </ul>

S/N	Respondent	Full Responses from Respondent
		<p>the value of transactions of a customer hits S\$20,000. Last, a Major PI is unable to offer any services where the value of transactions for a customer exceeds S\$30,000.</p> <ul style="list-style-type: none"> <li>• In other words, the regulatory requirements seem to penalise a PI; as it is likely that the non-low risk products are those offered by a major PI, it would mean that Major PIs are placed in a worse off situation when offering products and services.</li> <li>• To mitigate this, and unless the MAS is ready to re-calibrate the licensing conditions to remove some of the restrictions on the Major PIs vis-à-vis the wallet sizes and the annual transactions cap at S\$30,000, the MAS can provide the Major PI with some relief by stating that all PIs that are subject to the Draft PS Notice 01 is allowed to commence CDD for its services using Simplified CDD. Until the threshold limit of S\$20,000 per annum is met and /or if there are AML/CFT risks involved, including nationalities and corridors, Standard CDD is not required.</li> </ul> <p><b>Question 5. <u>Third Party Reliance.</u> 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)</b></p> <p><b>Response</b></p> <p>(a) We believe the requirements remain useful. However, in relation to Section 12.2 (d), we believe that as a matter of precaution, PIs or FIs would not agree to supply each other with the personal data of a customer, even in cases where there is reliance on each other in accordance with Section 12 of the AML/CFT notice. Hence, we believe that it is more reasonable for Section 12.2(d) to require that the third party be ready and be willing to provide the data, documents or information to the requesting PI in a form that does not necessarily compromise the third party's obligation to keep the information, including personal data, confidential. For example, in relation to such information, the third party could be allowed to provide this to the regulator.</p> <p>(b) Furthermore, in Section 12.1(c) of the Draft PS Notice 01 excludes a related company who is also a PSA licensee from the definition of a third party. We believe that PSA licensees should be included in the definition.</p> <p><b>Question 6. <u>Correspondent Account Services.</u> MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 3.9 would be applicable to the Activity performed by</b></p>

S/N	Respondent	Full Responses from Respondent
		<p>your institution. <i>(Please refer to paragraph 13 of the draft PS Notice 01 and paragraph 12 of the draft PS Notice 02)</i></p> <p><u>Response</u></p> <p>NA</p> <p><b>Question 7. <u>Bearer Instruments and Cash Payouts.</u></b> MAS seeks comments on the proposal in paragraph 3.10 to apply the prohibition on issuance of bearer negotiable instruments and restriction of cash payout requirements to licensees which perform Activities A, B, C, F and G. <i>(Please refer to paragraph 11 of the draft PS Notice 01 and paragraph 10 of the draft PS Notice 02)</i></p> <p><b>Question 8. <u>Cross-border Transfer.</u></b> MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.</p> <p><b>Question 9. <u>Wire Transfer Requirements for DPT Services.</u></b> 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. <i>(Please refer to paragraph 13 of the draft PS Notice 02)</i></p> <p><b>Question 10. <u>Designated Threshold.</u></b> 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. <i>(Please refer to paragraph 6.3(b) of the draft PS Notice 02)</i></p> <p><b>Question 11. <u>CDD Information.</u></b> 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. <i>(Please refer to paragraph 6.6 of the draft PS Notice 02)</i></p> <p><u>Other comments</u></p> <p>(a) Section V &amp; VI, Paragraphs 7.18-7.25 and 7.42 of draft Notice</p> <ul style="list-style-type: none"> <li>These sections outline the AML/CFT requirements for offering transactions without account opening. It appears out-dated in that in all cases, as long as the licensee / PI offers some services (ie transactions are carried out), some form of CDD is already required.</li> </ul>

S/N	Respondent	Full Responses from Respondent
		<p>It no longer appears relevant for these sections to be retained. The obligations contained therein should apply as long as a PI offers services that attract AML/CFT obligations.</p> <p>(b) 7.51-7.54 of Draft PS Notice 1 on Screening</p> <ul style="list-style-type: none"> <li>We refer to our response to Q3 above. We ask that the MAS specifically includes an exemption from these sections where the payment relates to goods and services.</li> </ul> <p>(c) 15.1-15.20 of Draft PS Notice 1 on Wire Transfers</p> <ul style="list-style-type: none"> <li>We refer to our response to Q3 above. It is not practicable to include these information in relation to payments for goods and services. We ask that the MAS specifically includes an exemption from these sections where the payment relates to goods and services, both domestic and international.</li> <li>It is not the norm in the current payments world that the payment instructions for payments of goods and services carry the type of information that is set out in the Draft PS Notice 1. Generally, the merchant acquirers will dictate the form of information they require for the purpose of ensuring accurate billing and payment.</li> <li>Furthermore, Section 15 emanates from the traditional remittance business where wire transfers are between individuals. In the payment for goods and services world, the merchants are the recipients of funds and the information carried in the instructions may not resemble the typical remittance. For example, the merchant name is not typical and could carry names of merchant aggregators, ecommerce malls. The merchant account number could be a variety of numbers designated by the merchant or bank acquirer. This applies to both domestic and international payments for goods and services.</li> <li>Barring the situations where a customer chooses to transfer the money from its e-wallet to a bank account, the only other situations where a domestic money transfer occurs (without payment for goods and services) is where they transfer money to another person on the same PI's network. For example, some PIs allow their users to transfer value from their e-wallet to another user's e-wallet where both are on the same network. Under those circumstances, there would always naturally be documentation showing the deduction</li> </ul>

S/N	Respondent	Full Responses from Respondent
		<p>and entry of funds from and into the e-wallets. Hence, the requirement in Section 15 may not be necessary.</p> <p>(c) Agent</p> <ul style="list-style-type: none"> <li>We seek clarification as to the scope of the agency arrangements intended in the Draft PS Notice 1. The term “agent” as set out in the Draft PS Notice 1 unfortunately appears to cover technical solutions providers involved in the remittance licensee’s business, given the general understanding of the phrase “assist in the provision of cross-border money transfer service”. We understand for example that banks may rely on technical solutions providers, whether for screening their customers, for processing the bank transactions and these are largely not considered agents as they do not solicit, market, sell or distribute the remittance service. On the contrary, they provide a service to the licensee for the latter to discharge their duties and to carry out their business.</li> <li>Therefore, we propose that the MAS issues a clarification note for this section to ensure that the right type of agency arrangements are covered.</li> <li>Notwithstanding this, we also note that where the arrangement extends to an outsourcing arrangement, the MAS Outsourcing Guidelines will apply.</li> </ul> <p>(d) Definition</p> <ul style="list-style-type: none"> <li>We note that in its Consultation, the MAS refers to Exempted Products and sets out the definition of Exempted Products in the Draft PS Notice 1. However, in its Proposed Payment Services Regulations<sup>13</sup>, it had used the term “non-relevant payment transaction” in S29 (Exemption from requirement to hold a standard payment licence). Where these terms are meant to refer to the same item, we prefer that the MAS standardise the terminology. Otherwise, we would seek clarification from the MAS as to the difference between the two terms and the significance behind using these two terms.</li> </ul>

<sup>13</sup> Consultation on Proposed Payment Services Regulations, April 2019



S/N	Respondent	Full Responses from Respondent
18.	TransferWise Singapore Pte. Ltd.	<p><b>General comments:</b></p> <p>We welcome MAS consultation on the development of the Payment Services Act AML/CFT Notice.</p> <p>It is encouraging to see the move towards a more risk based approach in managing ML/FT risk particularly in the application of SCDD. We believe that the majority of customers are good customers and a risk based approach allows the industry to provide a better experience of the good customers and to focus more on the higher risk customers.</p> <p>We believe MAS should also consider reviewing the mandatory verification of proof of address and nationality. A risk based approach should be adopted which is aligned with the requirements in several jurisdictions such as the UK and EU and also Australia, Malaysia and Hong Kong in the Asia Pacific region.</p> <p><b>Question 1: <u>Scope</u>.</b> 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.</p> <p>No comment.</p> <p><b>Question 2: <u>Alignment with FATF Standards</u>.</b> 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.</p> <p>No comment.</p> <p><b>Question 3: <u>AML/CFT Requirements for Offering of Exempted Products</u>.</b> 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. <i>(Please refer to paragraph 3.3 of the draft PS Notice 01)</i></p> <p>No comment.</p> <p><b>Question 4: <u>Simplified Due Diligence</u>.</b> MAS seeks comments on whether SCDD should be permitted for the various payment services covered under</p>

S/N	Respondent	Full Responses from Respondent
		<p><b>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)</b></p> <p>We are supportive of MAS direction to allow a more risk based approach for the use of SCDD and the removal of the approval requirement to conduct SCDD.</p> <p>Adopting a risk based approach to CDD is a step in the right direction. This is aligned with FATF's Recommendation 1<sup>14</sup> which emphasises the need to apply a risk based approach to mitigating ML/TF risks to ensure that resources are efficiently allocated to address higher risk customers or activities.</p> <p>On the scenarios where SCDD is not permitted under Para 3.2 we fully agree that SCDD should not be applied to customers deemed to be higher risk or where there is suspicion of ML/TF involved. However, we believe that the cumulative transactions of \$20,000 does not necessarily follow a risk based approach as the value and volume of transactions undertaken by each payment service provider would vary significantly. Similar to how an assessment is required prior to conducting SCDD the same requirement should be applied to the setting of the cumulative transaction threshold.</p> <p>We ask MAS to consider allowing the threshold to be set by the payment service provider subject to an internal risk assessment being performed. Criteria for assessing the risk can be published by MAS and thresholds set can be subjected to annual audits.</p> <p><b>Question 5. <u>Third Party Reliance</u>. 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)</b></p> <p>We believe that third party reliance is appropriate particularly in the current environment where there are increasing partnerships between financial institutions and fintech companies with financial institutions.</p> <p><b>Question 6. <u>Correspondent Account Services</u>. MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 3.9 would be applicable to the Activity performed by</b></p>

<sup>14</sup> <https://www.cfatf-gafic.org/index.php/documents/fatf-40r/366-fatf-recommendation-1-assessing-risks-and-applying-a-risk-based-approach>

S/N	Respondent	Full Responses from Respondent
		<p>your institution. <i>(Please refer to paragraph 13 of the draft PS Notice 01 and paragraph 12 of the draft PS Notice 02)</i></p> <p>No comment.</p> <p><b>Question 7. <u>Bearer Instruments and Cash Payouts.</u></b> MAS seeks comments on the proposal in paragraph 3.10 to apply the prohibition on issuance of bearer negotiable instruments and restriction of cash payout requirements to licensees which perform Activities A, B, C, F and G. <i>(Please refer to paragraph 11 of the draft PS Notice 01 and paragraph 10 of the draft PS Notice 02)</i></p> <p>No comment.</p> <p><b>Question 8. <u>Cross-border Transfer.</u></b> MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.</p> <p>No comment.</p> <p><b>Question 9. <u>Wire Transfer Requirements for DPT Services.</u></b> 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. <i>(Please refer to paragraph 13 of the draft PS Notice 02)</i></p> <p>No comment.</p> <p><b>Question 10. <u>Designated Threshold.</u></b> 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. <i>(Please refer to paragraph 6.3(b) of the draft PS Notice 02)</i></p> <p>No comment.</p> <p><b>Question 11. <u>CDD Information.</u></b> 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. <i>(Please refer to paragraph 6.6 of the draft PS Notice 02)</i></p> <p>No comment.</p>

S/N	Respondent	Full Responses from Respondent
19.	Wirecard Asia Holding Pte Ltd (“Wirecard”)	<p><b>General comments:</b></p> <p><b>Question 1: <u>Scope</u>.</b> 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.</p> <p>If the payment service provider conducts additional businesses which are not regulated for ML/TF risk, it would be reasonable for MAS to impose AML/CFT requirements only where such additional business is from an industry posing high ML/TF risk - otherwise, this will run the risk of overregulation.</p> <p>The Precious Stones and Precious Metals Dealers (Prevention of Money Laundering and Terrorism Financing) Act (“PSPM Act”) exempts MAS-regulated financial institutions (except for the cash transaction reporting requirement), therefore there is a danger that unless MAS specifically regulates such payment service providers for their PSPM activities, that these activities will go unregulated.</p> <p>Additionally, it would be beneficial if the regime regulating such additional activities by payment service providers is complementary to and consistent with the draft MAS AML Notices. This will achieve an analogous business operability and reduce regulatory burdens of PSPs.</p> <p><b>Question 2: <u>Alignment with FATF Standards</u>.</b> 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.</p> <p>As DPTs carry an inherent ML/TF risk, we agree that persons facilitating the transfer of DPT and custodian wallet services should be subject to AML/CFT requirements as well. Otherwise, terrorist groups/money launderers may be able to transfer money into the Singapore financial system or within DPT networks by concealing transfers or by benefiting from a certain degree of anonymity.</p> <p>The proposed requirements to regulate these services would also bring Singapore in line with other international movements in this direction – for example, the EU Council has passed the 5<sup>th</sup> Anti-Money Laundering Directive.</p>

S/N	Respondent	Full Responses from Respondent
		<p><b>Question 3: <u>AML/CFT Requirements for Offering of Exempted Products.</u></b> 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. <i>(Please refer to paragraph 3.3 of the draft PS Notice 01)</i></p> <p>It is submitted that accounts with the capacity to store smaller amounts of e-money should be granted relief from AML/CFT requirements.</p> <p>Additionally, it would be helpful if MAS could provide further clarification as to whether the \$20,000 value mentioned in paragraph 3.2(ii)-(iii) of draft Notice 01 refers to the transaction amount transferred at any one point in time, on a per day basis, or throughout the lifecycle of the customer.</p> <p><b>Question 4: <u>Simplified Due Diligence.</u></b> 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. <i>(Please refer to paragraph 8 of the draft PS Notice 01 and paragraph 7 of the draft PS Notice 02)</i></p> <p>It would also be helpful if further guidance could be provided on:</p> <ul style="list-style-type: none"> <li>(a) the exact requirements for SCDD under draft PS Notice 01 (to make sure that there is a minimum standard that all payment service providers are held to); and</li> <li>(b) how an assessment of low risk for DPTs providers should be substantiated under draft PS Notice 02, apart from a consideration of paragraph 7.4 of the same.</li> </ul> <p><b>Question 5. <u>Third Party Reliance.</u></b> MAS seeks comments on whether third party reliance is appropriate for the sector. <i>(Please refer to paragraph 12 of the draft PS Notice 01 and paragraph 11 of the draft PS Notice 02)</i></p> <p>Yes. The financial cost of fulfilling CDD requirements can be quite high, and will particularly impact the smaller financial service providers. Allowing third party reliance will significantly decrease this cost.</p> <p>We agree that third party reliance is suitable for payment service providers covered by PS Notice 01. We additionally proposed that the categories of third party reliance under paragraph 12 of draft PS Notice 01 be further expanded to include payment service providers that are licensed under the Payment Services Act and that are also regulated by the draft AML notices</p>

S/N	Respondent	Full Responses from Respondent
		<p>released by MAS. This is on the basis that such payment service providers would also be regulated for AML/CFT by MAS.</p> <p>It would also be helpful if MAS could standardize and specify the foreign authorities mentioned in 12.1(b) of the draft PS Notice 01, so that all payment service providers employ a common standard.</p> <p><b>Question 6. <u>Correspondent Account Services.</u> MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 3.9 would be applicable to the Activity performed by your institution. (Please refer to paragraph 13 of the draft PS Notice 01 and paragraph 12 of the draft PS Notice 02)</b></p> <p>No comment.</p> <p><b>Question 7. <u>Bearer Instruments and Cash Payouts.</u> MAS seeks comments on the proposal in paragraph 3.10 to apply the prohibition on issuance of bearer negotiable instruments and restriction of cash payout requirements to licensees which perform Activities A, B, C, F and G. (Please refer to paragraph 11 of the draft PS Notice 01 and paragraph 10 of the draft PS Notice 02)</b></p> <p>We agree that this is an appropriate safeguard, and in line with FATF's Guidance Document titled "International Best Practices Detecting and preventing the illicit cross-border transportation of cash and bearer negotiable instruments.</p> <p>However we note that 11.4 of draft PS Notice 01 excludes other traceable methods of disbursement such as internet banking transfers/GIRO batch uploads which leaves a more reliable form of audit trail as compared to maintaining a register of crossed cheques.</p> <p>In addition, the omission of other widely adopted forms of payment will affect the payment eco-system, as there are consumers who may prefer to receive their settlements via online transfers as opposed to manually depositing cheques at physical locations.</p> <p><b>Question 8. <u>Cross-border Transfer.</u> MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.</b></p> <p>Yes they should. Given the relatively high cost of money transfers and the increasing adoption of DPTs, it is likely that consumers will make use of DPTs by conducting value-transfers on a cross-border basis (as opposed to using more traditional methods) - the result of conducting value-transfers to</p>

S/N	Respondent	Full Responses from Respondent
		<p>beneficiaries overseas would have the same effect as cash remittances, and therefore should be similarly regulated.</p> <p><b>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)</b></p> <p>Yes, the wire transfer requirements should apply to DPT services. Certain features of DPTs make them attractive to persons undertaking illicit activities such as ML/TF or tax evasion. These risk factors include their distributed, inherently cross-border nature, their easy transferability, and the potential for anonymous or pseudo-anonymous transactions (particularly if the assets are transferred from jurisdictions that do not regulate DPTs).</p> <p>Apart from the requirements in paragraph 13 of draft PS Notice 02, additional information that would be useful to be attached to the DPT transaction would include (a) the type and characteristics of the DPT (since there are so many variants), as well as (b) an analysis report generated by companies such as Chainanalysis/ Elliptic, that are able to identify the source and provenance of the DPT.</p> <p><b>Question 10. <u>Designated Threshold.</u> 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)</b></p> <p>No comment.</p> <p><b>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)</b></p> <p>A professionally generated report by DPTs tracing companies like Chainanalysis or Elliptic would be useful information that could be included, to ensure that the DPTs have not been used for illicit activities/ML/TF purposes.</p>

S/N	Respondent	Full Responses from Respondent
20.	Xfers Pte.Ltd.	<p><b>General comments:</b></p> <p><b>Question 1: <u>Scope</u>.</b> 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.</p> <p>Xfers Comments: Nil</p> <p><b>Question 2: <u>Alignment with FATF Standards</u>.</b> 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.</p> <p>Xfers Comments: Nil</p> <p><b>Question 3: <u>AML/CFT Requirements for Offering of Exempted Products</u>.</b> 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. <i>(Please refer to paragraph 3.3 of the draft PS Notice 01)</i></p> <p>Xfers Comments: We are supportive of the stratification of risk profiles of different classes of products and we hope MAS continues to apply this principle of proportionality throughout its regulatory requirements.</p> <p><b>Question 4: <u>Simplified Due Diligence</u>.</b> 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. <i>(Please refer to paragraph 8 of the draft PS Notice 01 and paragraph 7 of the draft PS Notice 02)</i></p> <p>Xfers Comments: We agree that SCDD should be permitted for the stated payment services within the criteria proposed.</p>



S/N	Respondent	Full Responses from Respondent
		<p><b>Question 5. Third Party Reliance.</b> MAS seeks comments on whether third party reliance is appropriate for the sector. <i>(Please refer to paragraph 12 of the draft PS Notice 01 and paragraph 11 of the draft PS Notice 02)</i></p> <p>Xfers Comments:</p> <p><b><u>Proposal</u></b></p> <p>We believe that MAS should include MPIs (that carry out “specified payment services”) in the list of financial institutions which are permitted to be relied upon to perform CDD for other payment services licensees (“permitted third parties”).</p> <p>In the alternative, if MAS does not view VASPs to be suitable to act as permitted third parties, MAS should permit third party reliance on MPIs (that carry out specified payment services but not those MPIs acting as VASPs).</p> <p><b><u>Explanation</u></b></p> <ol style="list-style-type: none"> <li><b>FATF Guidance Allows for Third Party Reliance on Other VASPs</b> - Firstly, Draft FATF Guidance on a <i>“Risk-based Approach to Virtual Assets and Virtual Asset Service Providers”</i><sup>15</sup> permits reliance on other financial institutions (e.g: MVTs providers), including even VASPs, to act as permitted third parties. Considering that PS licensees that carry out specified payment services will have to comply with PS-N01 or PS-N02 (or both) and are supervised to ensure compliance with the same AML/CFT laws, this meets the FATF requirements laid out in Recommendation 17 of the above Draft FATF Guidance.</li> <li><b>Seamless Customer Experience for Payments in Singapore</b> - Furthermore, allowing MPIs to act as permitted third parties would also ease customer on-boarding friction, benefiting customers as they would no longer have to go through lengthy KYC processes multiple times to access each PS licensee’s services. This enables a better customer experience as a whole when making payments in Singapore, and would encourage greater competition in the payment services industry by enabling data portability if PS licensees could rely on MPIs for part of the CDD process. We note that the PDPC and IMDA are also encouraging data portability as seen from PDPC’s recent consult paper and IMDA’s new Trusted Data Sharing Framework.</li> </ol>

<sup>15</sup> <http://www.fatf-qaqi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>

S/N	Respondent	Full Responses from Respondent
		<p>3. <b>Reduce Duplicated KYC/CDD Procedures</b> - Likewise, PS licensees who rely on MPIs would likely need to carry out less duplicated KYC processes which the industry has already performed dozens of times for the same consumer, processes which are both time-intensive and resource-wasteful. For example, according to Thomson Reuters, Singapore financial institutions on average, spend above S\$50 million on KYC annually and this figure is rising rapidly<sup>16</sup>. By allowing MPIs to act as third parties, the industry stands to benefit without compromise to AML/CFT standards. On the contrary, with less time and resources dedicated to duplicated KYC processes, resources can more efficiently and effectively be used to carry out CDD processes more thoroughly.</p> <p>Hence, we believe that MAS should permit reliance upon MPIs as third parties because the industry as well as consumers stand to reap significant gains in convenience and efficiency.</p> <p><b>Question 6. <u>Correspondent Account Services.</u> MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 3.9 would be applicable to the Activity performed by your institution. (Please refer to paragraph 13 of the draft PS Notice 01 and paragraph 12 of the draft PS Notice 02)</b></p> <p>Xfers Comments:</p> <p>The proposed requirements set out for Correspondent Account Services would be too wide-reaching as simply the act of providing specified payment services to other financial institutions would render us a Correspondent Financial Institution, regardless of the geographical location of incorporation or regulatory status of the Respondent Institution.</p> <p><b><u>Proposal</u></b></p> <p>We propose that MAS should consider limiting the application of Draft Notice PS-N01 paragraph 12.1(a) and 12.1(b) to only Cross-Border Correspondent Account Services (i.e. where the Respondent Financial Institution is one that operates outside of Singapore).</p> <p><b><u>Explanation</u></b></p> <p>1. <b>FATF Focuses on Cross-Border Risk</b> - We note that MAS' inclusion of Domestic Correspondent Account Services goes above the</p>

<sup>16</sup> Thomson Reuters Report Page 8-  
[https://www.refinitiv.com/content/dam/marketing/en\\_us/documents/reports/kyc-challenges-2017-singapore.pdf](https://www.refinitiv.com/content/dam/marketing/en_us/documents/reports/kyc-challenges-2017-singapore.pdf)

S/N	Respondent	Full Responses from Respondent
		<p>requirements set by FATF because the 2012 FATF Recommendation 13<sup>17</sup> on Correspondent Banking specifically applies to Cross-Border Correspondent Banking and other similar relationships. FATF Guidance on “Correspondent Banking Services” states that for MVTS providers the regulatory focus should be on Cross-Border Correspondent Banking as, “cross-border correspondent banking relationships are seen to be inherently higher risk than domestic correspondent customer relationships.”</p> <p>2. <b>Common Domestic AML/CFT Regime</b> - There is much lesser risk of regulatory arbitrage when both the Correspondent FI and the Respondent FI have to abide by the same AML regime in the same jurisdiction. In most cases, the Correspondent FI would likely already have to conduct enhanced due diligence on the Respondent FI, and having to further comply with these obligations might add further compliance complexity and might even have the unfortunate consequence of PS licensees derisking fellow PS licensees. This might then lead to further silos and fragmentation of the Singapore payments industry.</p> <p>3. <b>Uncertainties of Foreign Supervisory Authorities</b> - There are much fewer AML risks associated with domestic correspondent relations as compared to cross-border relationships, because the following, are highly limited or non-existent in the domain of Domestic Correspondent Account Services:</p> <ul style="list-style-type: none"> <li>a) Lack of oversight over the cross-border counterparty</li> <li>b) Weak AML Regimes/Enforcement in overseas jurisdiction</li> <li>c) The existence and licensing of shell banks and other entities which pose high AML/CFT risk</li> </ul> <p>These factors show that the basis for determining the risk level of Correspondent Account Services is deeply rooted in the conventional <i>cross-border</i> application of those services. Hence, we believe that MAS should consider solely applying their regulatory requirements on cross-border Correspondent Account Services, as is in line with FATFs recommendations.</p> <p><b>Question 7. <u>Bearer Instruments and Cash Payouts.</u> MAS seeks comments on the proposal in paragraph 3.10 to apply the prohibition on issuance of bearer negotiable instruments and restriction of cash payout requirements to licensees which perform Activities A, B, C, F and G. (Please refer to</b></p>

<sup>17</sup> **FATF 40 Recommendations 2012** <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>

S/N	Respondent	Full Responses from Respondent
		<p><i>paragraph 11 of the draft PS Notice 01 and paragraph 10 of the draft PS Notice 02)</i></p> <p>Xfers Comments: Nil</p> <p><b>Question 8. <u>Cross-border Transfer</u>. MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.</b></p> <p>Xfers Comments:</p> <p><b><u>Proposal</u></b></p> <p>We submit that as a matter of principle, MAS should not blanket classify all value transfers as being cross-border in nature. While value transfers of DPT should largely be considered cross-border in nature, we believe that in principle there are certain DPT transactions that can be considered 'domestic', such as where the ordering institution, intermediary institution (if any), and the beneficiary institution are all in Singapore. However, if the value transfer is to a non-custodial DPT wallet address (where there is no beneficiary institution), then it should be presumed to be cross-border because we are not aware of any practical way to conclusively determine the jurisdiction where the non-custodial wallet address resides.</p> <p><b><u>Explanation</u></b></p> <p>When the ordering institution, intermediary institution (if any), and the beneficiary institution are all in Singapore, it is analogous to having a bank in Singapore initiating a funds transfer for its customer to the customer of another bank in Singapore (irrespective of the nationality or location of the originator or beneficiary). In such cases, it would be inconceivable that the transfer be classified as cross-border when both banks are in Singapore - in a similar vein, when both VASPs are in Singapore, the value transfer should be classified as a domestic transfer.</p> <p><b>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)</b></p> <p>Xfers Comments:</p>

	<p><b><u>Potential Issue with Operationalisation of Wire Transfer Requirements</u></b></p> <p>We would like to point out that operationalising this in practice would likely require industry cooperation, eventually on a global level. The infrastructure required to carry this out would need significant time and effort to develop, adopt and mature.</p> <p>Due to the present infeasibility of applying the wire transfer requirements, this will result in slow adoption and significant disruption to VASPs. VASPs may not be able to carry out a large proportion of DPT transactions where they cannot meet the wire transfer requirements of “immediately and securely submit(ing) (originator and beneficiary information) to the beneficiary institution” under paragraph 13.9 of PS-N02, causing end-users to be unable to withdraw or transfer out their DPTs.</p> <p><b><u>Best-Case Scenario in Implementation</u></b></p> <p>The best case scenario is one where MAS imposes regulations which are in step with the technical capabilities of VASPs, allowing VASPs to continue to function as normal.</p> <ol style="list-style-type: none"> <li>1. <b>Visibility into the Cryptocurrency Space</b> - This ensures that a situation does not arise whereby individuals choose to transact outside the regulated space of VASPs due to the shocks faced by end-users when VASPs are disrupted and delayed in servicing their users’ demands.</li> <li>2. <b>Consumer Confidence</b> - This ensures that large disruptions do not weaken the consumers’ perception of cryptocurrency and trust in local VASPs when they are no longer able, for some time, to perform expected transfers and withdrawals.</li> </ol> <p><b>Question 10. <u>Designated Threshold.</u> 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)</b></p> <p>Xfers Comments:</p> <p>In view of MAS going beyond the USD/EUR 1,000 threshold under FATF Recommendation 15 of the Draft Guidance on a “Risk-based Approach to Virtual Assets and Virtual Asset Service Providers,” we urge MAS to consider our above proposals in areas such as wire transfer requirements (Q9), cross-border transfer (Q8), third party reliance (Q5) etc, because the ML preventative effect of requiring CDD from the 1st dollar would synergistically improve these other AML measures.</p>
--	--

S/N	Respondent	Full Responses from Respondent
		<p><b>Question 11. CDD Information.</b> 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. <i>(Please refer to paragraph 6.6 of the draft PS Notice 02)</i></p> <p>Xfers Comments: Nil</p>
21.	Respondent A (confidentiality of identity requested)	<p><b>General comments:</b></p> <p><i>As the largest Bitcoin ATM operator in Singapore, we recognise the importance of this new regulation in combating money laundering and terrorist financing. We believe that the current proposal to implement anti-money laundering and counter-terrorist financing (AML/CFT) measures on the digital payment token industry will definitely help in protecting the industry from abuse.</i></p> <p><i>Although we generally agree with the objectives of the PS Act and the proposed regulations, we have noted that most of the proposals are extremely onerous and impractical to implement.</i></p> <p><i>We believe that because of the infancy of digital payment tokens and blockchain technology, isolating the theoretical (e.g. what the blockchain technology can do in theory) from the practical component (i.e. what is practical given the currently available resources on the blockchain technology) is essential to allow the industry and the technology to grow and mature in Singapore.</i></p> <p><b>Question 1: Scope.</b> 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.</p> <p><i>The Precious Stones and Precious Metals Prevention of Money Laundering and Terrorism Financing Act 2019 (PSPM Act) and related regulations, covers in its scope, the dealing of asset-backed tokens. An asset-backed token under the scope of the PSPM Act is defined as a token, certificate or other instrument backed by one or more precious metals, precious stones or precious products that entitle the holder to the precious metal, precious stone or precious</i></p>

S/N	Respondent	Full Responses from Respondent
		<p><i>product, or part of it. An example of such asset-backed token is the Digix Gold Token (DGX).</i></p> <p><i>For all intents and purposes, such asset-backed tokens are also “digital payment tokens” under the Payment Services Act 2019 (PS Act) and it is currently unclear whether such asset-backed tokens will continue to be under the scope of the PSPM Act and related regulations, or, such asset-backed tokens will instead be regulated under the PS Act.</i></p> <p><i>We are of the opinion that if these asset-backed tokens will be covered by the PS Act, no asset-backed token (backed by precious metals and precious stone) will ever be under the scope of the PSPM Act which is contrary to the purpose of the PSPM Act and related regulations on asset-backed token backed by precious metals and precious stone.</i></p> <p><i>In view of the above, we would like to request for clarification on (1) how the PS Act and PS Notice 02 will apply to such asset-backed token that are already under the scope of the PSPM Act, and (2) which of the two (2) regulations (PSPM Act and PS Act) should the industry comply to.</i></p> <p><b>Question 2: <u>Alignment with FATF Standards.</u></b> 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.</p> <p><i>We are of the opinion that focusing on a risk-based approach is more appropriate as this allows industry players to adapt to newer challenges related to digital payment tokens. This will allow industry players to adopt relevant AML/CFT risk measures based on the nature of their business, nature of technology being used, and the size of the entity.</i></p> <p><i>A more principle-based (instead of rule-based) approach would also allow industry players to implement newer AML/CFT measures as a result of new developments in the digital payment token space that would have not been identified otherwise by previous regulations.</i></p> <p><b>Question 3: <u>AML/CFT Requirements for Offering of Exempted Products.</u></b> 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)</p>

S/N	Respondent	Full Responses from Respondent
		<p><i>We agree with the proposed requirement for Exempted Products.</i></p> <p><b>Question 4: <u>Simplified Due Diligence</u>.</b> 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. <i>(Please refer to paragraph 8 of the draft PS Notice 01 and paragraph 7 of the draft PS Notice 02)</i></p> <p><i>We agree with the proposal to allow SCDD on various payment services covered by the Notice and to implement a risk-based approach in applying the PS Act.</i></p> <p><i>However, we are of the opinion that requiring a per transaction based limit (e.g. S\$5,000/transaction) instead of a cumulative annual limit (i.e. S\$20,000) for digital payment tokens would be more appropriate for the following reason:</i></p> <ul style="list-style-type: none"> <li><i>a. The proposed limit of S\$20,000 per year will prohibit new players from entering Singapore's the digital token payment industry, therefore inhibiting industry growth, due to administrative and financial burden such exercise will entail. For example, a bitcoin ATM operator would have the majority of their customers exceed the S\$20,000 annual limit as these customers will normally buy and sell the same digital payment token on the ATM machine.</i></li> <li><i>b. Allowing a transaction based limit of S\$5,000/transaction would mean that digital payment token transactions will continue to be fast and efficient (one of the major advantages of digital payment token) and therefore allowing the industry to grow and evolve in Singapore. On the other-hand an annual cumulative limit would mean a delay transaction execution due to administrative processing by operators.</i></li> <li><i>c. A risk-based approach and continuous monitoring of customer transaction behaviours to identify red flags can be a more appropriate measure as this would allow faster transaction execution but still minimise the risk of ML/TF.</i></li> <li><i>d. A transaction based limit approach would be consistent to other activities regulated by the PS Act.</i></li> </ul> <p><b>Question 5. <u>Third Party Reliance</u>.</b> MAS seeks comments on whether third party reliance is appropriate for the sector. <i>(Please refer to paragraph 12 of the draft PS Notice 01 and paragraph 11 of the draft PS Notice 02)</i></p>



S/N	Respondent	Full Responses from Respondent
		<p><i>We agree that third party reliance is appropriate for the sector. We, however, suggest that the third party reliance on CDD procedures be expanded to not just include financial institutions and related parties but also third parties that are already implementing AML/CFT measures.</i></p> <p><i>For example, a bitcoin ATM operator may have ATMs placed in a host location with the host is already implementing AML/CFT measures to its customers (albeit in compliance with a different regulation such as the PSPM Act). If the hosts cross-sells the bitcoin ATM services to its customer, we believe that relying on the CDD procedures conducted by the host to the target customer is more appropriate since this will provide the bitcoin ATM operator a better understanding of the customer's specific risk and behaviour (based on his/her previous dealings with the host).</i></p> <p><b>Question 6. <u>Correspondent Account Services.</u> MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 3.9 would be applicable to the Activity performed by your institution. (Please refer to paragraph 13 of the draft PS Notice 01 and paragraph 12 of the draft PS Notice 02)</b></p> <p><i>We do not believe that the proposed requirements on Correspondent Account Services are applicable to the services we perform.</i></p> <p><b>Question 7. <u>Bearer Instruments and Cash Payouts.</u> MAS seeks comments on the proposal in paragraph 3.10 to apply the prohibition on issuance of bearer negotiable instruments and restriction of cash payout requirements to licensees which perform Activities A, B, C, F and G. (Please refer to paragraph 11 of the draft PS Notice 01 and paragraph 10 of the draft PS Notice 02)</b></p> <p><i>As an entity operating bitcoin ATMs in Singapore, restricting cash payout to S\$20,000 would have a tremendous negative impact on our business – being a cash-based business. And unlike other businesses covered by the PS Act, we are unable to issue cheques and are therefore left with no practical alternative due to the very nature of our business which is the placement of stand-alone bitcoin ATMs across Singapore.</i></p> <p><i>We believe that setting a higher threshold (e.g. S\$50,000) would lessen the impact of such requirement to industry operators.</i></p> <p><b>Question 8. <u>Cross-border Transfer.</u> MAS seeks comments on whether all value transfers of DPT should be considered cross-border in nature. Please elaborate on your comment.</b></p>

S/N	Respondent	Full Responses from Respondent
		<p><i>We are of the opinion that this exercise is ineffective because of the following inherent features of digital payment tokens:</i></p> <ul style="list-style-type: none"> <li><i>a. Industry players would be unable to prove with reasonable certainty that the information provided about the originator or beneficiary are true and accurate due to nature of digital payment token wallets being available in different forms and readily available to users. It is extremely easy to generate digital payment token addresses.</i></li> <li><i>b. Based on our experience, value transfers only represents a small portion of transactions involving digital payment tokens since users can just generate their own digital payment token addresses whenever they want as mentioned in point (a) above.</i></li> <li><i>c. Services that facilitate value transfers (e.g. digital payment token escrow service) are not widely used and it would not be appropriate to impose a blanket regulation that is only relevant for an extremely small portion of digital payment token transactions.</i></li> <li><i>d. Applying the wire transfer requirement will impose undue cost and effort to industry operators with an expected result that may prove to be little to no value in combating ML/TF.</i></li> </ul> <p><b>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)</b></p> <p><i>We believe that this exercise is impractical and extremely difficult to comply to because of the following inherent features of digital payment tokens:</i></p> <ul style="list-style-type: none"> <li><i>a. Industry players would be unable to prove with reasonable certainty that the information provided about the originator or beneficiary are true and accurate due to nature of digital payment token wallets being available in different forms and readily available to users. Users can just generate their own digital payment token addresses whenever and wherever they want.</i></li> <li><i>b. Applying the wire transfer requirement will impose undue cost and effort to industry operators with an expected result that may prove to be little to no value in combating ML/TF.</i></li> </ul>

S/N	Respondent	Full Responses from Respondent
		<p><b>Question 10. Designated Threshold.</b> 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. <i>(Please refer to paragraph 6.3(b) of the draft PS Notice 02)</i></p> <p><i>We believe that since digital payment tokens are viewed as a game-changer in Singapore's cashless payment drive, requiring CDD on transactions involving trivial amounts is counterproductive to Singapore's Smart Nation initiative.</i></p> <p><i>Performing due diligence on customers who are paying SGD 5 for their coffee is both absurd and unconscionable. We believe that using the payment threshold of SGD 1,000 per transaction is an acceptable compromise will still be in line with the FATF recommendations of USD/EUR 1,000.</i></p> <p><b>Question 11. CDD Information.</b> 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. <i>(Please refer to paragraph 6.6 of the draft PS Notice 02)</i></p> <p><i>We are of the opinion that the proposed collection of the alternative CDD information features in Table 2 are impracticable, entails undue cost and effort to industry operators, and might fail to obtain information that are relevant in combating ML/TF.</i></p> <p><i>Following are the reasons why we believe that the proposed alternative CDD information is impracticable:</i></p> <ol style="list-style-type: none"> <li><b>1. DPT Sending/Receiving Addresses ("Source of funds")</b> <ul style="list-style-type: none"> <li><i>– Requiring DPT sending/receiving address might prove to have little to no value in combating ML/TF since users who use exchange wallets would normally have their DPT mixed into a combined address. As a result obtaining reasonable information about the source of funds can be ineffective and time consuming.</i></li> </ul> </li> <li><b>2. Receipts/documentation on original purchase of cryptocurrency from an exchange or similar intermediary</b> <ul style="list-style-type: none"> <li><i>– Similar to point 1 above, collecting this information will also be impractical, time-consuming and may prove to be of little to no value in combating ML/TF specially if the cryptocurrency are</i></li> </ul> </li> </ol>

S/N	Respondent	Full Responses from Respondent
		<p>coming from micro-transactions and other non-purchase methods such as cryptocurrency mining, gifts, airdrops, forks, etc.</p> <ul style="list-style-type: none"><li>Exchange purchases would normally not include receipts unless for a large purchase from over-the-counter (OTC) providers.</li><li>Small amounts of cryptocurrencies consolidated into a single address are also very common and would not be practical to trace unless there is a strong suspicion of ML/TF.</li><li>Cryptocurrencies created through hard-forks would mean that any documentary evidence of original purchase will not be available.</li></ul> <p><b>3. 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.</b></p> <ul style="list-style-type: none"><li>Collecting this information is also impractical, time-consuming and may have little informational value in combating ML/TF specially if a single transaction has more than 1 input as shown in <a href="#">bitcoin transaction hash 838102b602351bf06bfc11d41c51374b20235a6120d324f697d04fe971aee9fb</a> that contains 8 inputs and 1 output.</li></ul> <div><div>Transaction View information about a bitcoin transaction</div><div><div>838102b602351bf06bfc11d41c51374b20235a6120d324f697d04fe971aee9fb</div><div><div>3Du566q6JTTT0ipjka6h9HkAzVsPQez9Zr 36TeonQMD7KNUFC5C5HfY3aP4XxEqmYs6 3DPVJ5RWR9hTiwFPpGJUR9aR5ETO1dc44H 3LLgW8HRVijR1x1FpEXkFmuUS2kH5DKwk 32GpbRmuGkFNYVNMxLlygKBCoRm6qPjpth 3CynNB61pQ2sDP7B8qy8VxVHXvYnYthS2 33DXxXoUMs8YtjGdC3wCBGfagZMe1cPdK 3Kd2AKHwmuErTFjgEZxkhDQ4Mxm6m6g48q</div><div><div>➡</div><div>1NHv6q3xu6haWj8rgeLqw8eyJqm4JT28R6</div><div>13.18086564 BTC</div></div></div><div><div>13.18086564 BTC</div></div></div><div><div><div><div>Summary</div><div><div>Size</div><div>1590 (bytes)</div></div><div><div>Weight</div><div>3450</div></div><div><div>Received Time</div><div>2019-06-22 20:58:59</div></div><div><div>Included In Blocks</div><div>581919 ( 2019-06-22 21:00:12 + 1 minutes )</div></div><div><div>Confirmations</div><div>1861</div></div><div><div>Visualize</div><div><a href="#">View Tree Chart</a></div></div></div><div><div><div>Inputs and Outputs</div><div><div>Total Input</div><div>13.1816688 BTC</div></div><div><div>Total Output</div><div>13.18086564 BTC</div></div><div><div>Fees</div><div>0.00080316 BTC</div></div><div><div>Fee per byte</div><div>50.513 sat/B</div></div><div><div>Fee per weight unit</div><div>23.28 sat/WU</div></div><div><div>Estimated BTC Transacted</div><div>13.18086564 BTC</div></div><div><div>Scripts</div><div><a href="#">Show scripts &amp; coinbase</a></div></div></div></div></div><ul style="list-style-type: none"><li>Analysing transactions like this, which is now very common specially for those using exchange wallets, can be cumbersome</li></ul></div></div>

S/N	Respondent	Full Responses from Respondent
		<p><i>and impractical. Some transactions can even have 10s or 100s inputs which would be extremely hard to analyse.</i></p> <p><b>4. Reasons for purchase of DPT.</b></p> <ul style="list-style-type: none"> <li><i>– This requirement for Bitcoin ATM operators like us will entail undue cost and effort to collect and the resulting information may have little informational value in combating ML/TF.</i></li> </ul> <p><b>5. Reasons for current transaction, if applicable.</b></p> <ul style="list-style-type: none"> <li><i>– This requirement for Bitcoin ATM operators like us will entail undue cost and effort to collect and the resulting information may have little informational value in combating ML/TF.</i></li> </ul>