Cayman Monetary Regulatory Authority International

At the forefront of financial regulation, the Cayman Monetary Regulatory Authority International (CMRAI) is dedicated to upholding the highest standards of financial oversight and compliance. Our mission is to safeguard the stability and integrity of the global financial system by ensuring that financial services operate within a framework of transparency, accountability, and excellence.

As a trusted partner to financial institutions worldwide, CMRAI provides rigorous supervision, innovative solutions, and strategic guidance to foster a secure and thriving financial environment. With decades of experience and a commitment to global standards, we stand as a pillar of trust and security in an ever-evolving financial landscape.

With a legacy of excellence in financial oversight, the Cayman Monetary Regulatory Authority International (CMRAI) is a beacon of trust in the international financial community. Our role extends beyond regulation; we are innovators, collaborators, and protectors of the global financial ecosystem. By fostering compliance, promoting best practices, and embracing technological advancements, CMRAI ensures that financial services remain resilient and adaptable in a dynamic global market.

Our comprehensive approach to regulation encompasses a deep understanding of financial risks and a proactive stance on emerging challenges. We are committed to empowering financial institutions with the tools and guidance necessary to navigate complex regulatory landscapes, thereby contributing to global economic stability and growth.

1 SUMMARY OF PRIVATE SECTOR CONSULTATION AND FEEDBACK STATEMENT GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING IN THE CAYMAN ISLANDS No. Section Comments from the Private Sector Authority s Response Consequent Amendments to the Proposed Measure 1. B.5 Closed-loop items are not captured in the Guidance Notes. Such items are non-transferable, non- exchangeable and non- refundable such as credit card awards, or similar loyalty program rewards or points, which an individual cannot sell onward in a secondary market. closed-loop items are not captured : how about a platform where customer can only buy and exchange crypto such as BTC or other eg for instance Revolut: user can only buy, hold and exchange. Also most of the time loyalty points are exchangeable within the group. Activities that fall within the definition of virtual asset services as defined in the VASP Law will be captured. The term closed loop items will be replaced by virtual asset tokens which is defined in the VASP Act. Amended to substitute the term closed loop items. 2. C.1. VAs due to their features and characteristics, have a higher ML/TF/PF risk associated with them. VASPs should be aware that a significant proportion of virtual assets held or used in a transaction may be associated with privacy- enhancing features or products and services that potentially obfuscate Internet Protocol (IP) anonymizers is a very broad term. We would recommend some more specific references here in line with the FATF Red Flag Indicators Report. The broad term was used to provide a general example of a product/service that may obfuscate a transaction by inhibiting identity. Section J(3)(b) gives further examples No amendments required. 2 No. Section Comments from the Private Sector Authority s Response Consequent Amendments to the Proposed Measure transaction or activities and inhibit a VASP s ability to know its customers and implement CDD and other effective AML/CFT measures, such as: a) Mixers or tumblers; b) Anonymity Enhanced Currencies (AEC) c) Obfuscated ledger technology; d) Internet Protocol (IP) anonymizers; e) Ring signatures; f) Stealth addresses; g) Ring confidential transactions; h) Atomic swaps; i) Non-interactive zero-knowledge proofs; j) Privacy coins; and k) A significant proportion of the virtual assets held or used in a transaction is associated with third party escrow services;

It is unclear what type of transactions associated with third party escrow services are covered under paragraph (k). We would recommend some examples to illustrate. of anonymity. J (5) also refers to the FATF Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (September 2020) which provides further examples. It is therefore not necessary to give further examples in these amended GNs. A third-party escrow service involves a third party holding [virtual] assets on behalf of two parties that are in the process of executing a transaction. The broad use of the term third party escrow services is meant to capture those transactions where a third party holds virtual assets for relevant parties in relation to a transaction that may involve anonymizers. The example is placed here so that VASPS are aware that the use of anonymizers is possible in such situations. 3 No. Section Comments from the Private Sector Authority s Response Consequent Amendments to the Proposed Measure Have these factors been cross referenced to the FATF Red flag indicators report point 13 - Red flag indicators related to Anonymity? (gafi.org/media/fatf/documents/recommendations/Virtual- Assets-Red-Flag-Indicators.pdf [nam11.safelinks.protection.outlook.com]) Concepts such as anonymity-enhanced

cryptocurrency (AEC) (Point b) or privacy coins (Point j) are one concept and are covered together in this report and should not be split up to avoid confusion. Internet Protocol (IP) anonymizers is a very broad term. We would recommend some more specific references here in line with FATF guidance. Ring signatures and ring confidential transactions are the same concept and should not be split up to avoid confusion. Additionally, ring signatures are not covered in any FATF guidance. See reference to the FATF Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (September 2020) at section J (5) Section J (3) lists some of the examples found in the FATF Report. These terms were used to provide very general examples and was not meant to capture every product or service (or features of same) that may inhibit identity etc. Similar examples have been used by other jurisdictions. No amendments required. Vasp are required to do KYC on their customer so even if the customer will transfer a so called privacy coins to his wallet, the vasp will have first required identification before opening the account and allowing the transfer. Also with the application of the travel rule the risk is considerably reduced. Plus, blockchain investigation tools will give information on the provenance of the coins which will allow the vasp to see if the coins have been through a mixer/tumbler or anonymizer; in those cases depending on the vasp internal controls further documents will be required. It should be noted that now some blockchain investigations tools allow the tracking of privacy coins. The Authority encourages the CDD techniques described in this comment. No amendments required. 4 No. Section Comments from the Private Sector Authority s Response Consequent Amendments to the Proposed Measure Finally, a vasp could restrict the transfer of privacy coins such as zcash to only transaction where identification is possible. 3. C. 2 VAs can enable non-face- to-face business relationships and can be used to quickly move funds globally to facilitate a range of financial activities from money or value transfer services to securities, commodities or derivatives-related activity, among others. Risk-based scrutiny of customers and transactions should be applied in accordance with the type of business conducted and the value and volume of transactions. VASPs should consider utilizing a range of monitoring and digital footprint tools to mitigate risks such as; undertaking an analysis of the relevant blockchain, for the purpose of assessing any nexus to sources of risk, including the darknet and blacklisted addresses, particularly where the risk is significant or the Instead of or on top of undertaking an analysis of the relevant blockchain , the Regulator should strongly recommend the use of blockchain investigation tools which allows real-time and/or post transaction monitoring, those systems could be tailored made to the exchange risk based approach. For instance, if exposure to sanction, child porn, TF transaction is stopped. However that may raise technical problems as the question to what to do with the coins. Option here could be to allow customers to only do transactions with white labelled addresses but the risk of indirect exposure will still exist. The use of the phrase monitoring and digital footprint tools is meant to capture blockchain investigative tools, among other things. No amendments required. 5 No. Section Comments from the Private Sector Authority s Response Consequent Amendments to the Proposed Measure volume of transactions is substantial. 4. C.5 Factors that give rise to money laundering, terrorist financing and proliferation financing risks (5) Segmentation The reference to work together with other parties in the value chain" is very broad. Does this include all counter parties and protocol developers involved in the value chain or would it only be Blockchain Analysis companies such as Ciphertrace and

Chainalysis? This sentence could potentially state; work together with other VASPsparties in the value chain so as to provide a more robust AML/CTF framework. It may be necessary, in some instances for VASPs to work with parties (other than VASPs) in the value chain. It is therefore prudent to leave the term as is. No amendments required. 5. C. 9. (a). (i) The following are specific higher-risk factors that VASPs should have regard to, in addition to the higher-risk classification factors set out in Section 3D of Part II of these Guidance Notes: (a) The ability of users to: (i) make or accept payments in money from/to unknown or un- associated third parties; This should be prohibited. Travel rule application as per the FATF guidance. Feedback noted and amendment made. Amended to remove. Some clarification may be necessary around unknown or un-associated parties . Does this refer to unknown parties to the customer or the VASP? For example, if A sends a transaction to B, does B have to be a customer of the same VASP to not be classified as an unknown or un-associated party? Feedback noted and amendment made. Amended. 6. D.2.e. The obligation to conduct such a risk assessment is enshrined in Sections 8 and 9 of the AMLRs, which require persons carrying Should also be taken into account if the customer is allowed to fund the account with credit card/gift card/wire transfer, etc. The comment was noted and accepted. Adjustments have been made to reflect same. Delivery channel risk: The risks related to how customers access a VASP s products or platform need to be considered. For example, 6 No. Section Comments from the Private Sector Authority s Response Consequent Amendments to the Proposed Measure out relevant financial business to take steps, appropriate to the nature and size of the business, to identify, assess, and understand its ML/TF risks in relation to customers, geographic region, products, services or transactions, and delivery channels, and to undertake such a risk assessment in relation to new products and business practices, new delivery channels, and new or developing technologies prior to their launch. Delivery channel risk: The risks related to how customers access a VASP s products or platform need to be considered. For example, whether they are only accessible online or whether physical infrastructures are being used. whether they are only accessible online or whether physical infrastructures are being used and the manner by which a VA account is funded. 7. E. Customer due diligence Paragraph 4 of this section incorrectly suggests that Section 12 of the AMLRs require VASPs to authenticate the identity of customers. In fact, Section 12 does not require authentication. Please correct the wording as follows: Feedback was noted and accepted. Wording changed to reflect Amended. 7 No. Section Comments from the Private Sector Authority s Response Consequent Amendments to the Proposed Measure "4. Pursuant to Section 12 of the AMLRs, VASPs and other related parties should collect the relevant CDD information on their customers when they provide services to or engage in virtual asset activities on behalf of their customers, including information on the customer s name and further identifiers such as physical address, date of birth, and a unique national identifier number (e.g., national identity number or passport number). As stipulated in Section 12 of the AMLRs, VASPs are also required to collect additional information to assist in verifying the customer s identity when establishing the business relationship at onboarding, authenticate the identity of customers, determine the customer s business and risk profile and conduct ongoing due diligence on the business relationship...". section 12 of the AMLRs. 8. E.5 In cases where a VASP carries out a one-off transaction, the designated threshold above which VASPs are required to conduct CDD

is KYD 10,000, in accordance with Section 11 of the AMLRs. International best practices set out by the FATF call for VASPs to conduct CDD for any one- off transaction above USD/EUR 1,000 or equivalent. While this is not yet a legal requirement in Cayman Islands, adoption of best practices is recommended. USD 1000 threshold should be mandatory to follow international standards. Also how about a customer doing a one off in different shops to avoid suspicion? (10 000 as a threshold is too high) Adjustments have been made to address the issue of one-off transactions. Amended. 8 No. Section Comments from the Private Sector Authority s Response Consequent Amendments to the Proposed Measure 9. F.3.a Source of Funds Evidence of the source of funds must be collected with respect to all transactions that present a higher risk, including those that involve: An exchange of virtual assets for money or vice versa; An exchange of one virtual asset for another if the customer claims the virtual asset has been obtained through mining; and The transfer of a customer s virtual assets from one exchange to another. For transactions carried out under a business relationship, this evidence may only need to be collected once. It will useful if the Regulator could give example of documents a VASP can ask a customer for crypto source of funds, would a report from a blockchain analysis provider sufficient? Should the customer take screenshots of the accounts where the funds were held? Should micro transaction be mandatory? Please be guided by Sections E, F and K of the Guidance Notes which identifies the relevant information that VASPs are responsible for collecting in relation to transactions, including conducting customer due diligence. No amendments required. 9 No. Section Comments from the Private Sector Authority s Response Consequent Amendments to the Proposed Measure 10. F.3.b It is good practice to collect information about the destination of funds in order to inform the assessment of risk (e.g., geographical risk) and aid transaction monitoring processes. Where a recipient s name has been collected, sanctions obligations apply in the usual way. Is the use of blockchain investigation tool enough? How about application of the travel rule? See Section K which addresses the travel rule. No amendments required. 11. J. 3 Some indicators of unusual or suspicious activities related to VAs are: (a) In Relation to Transactions: (i) Structuring VA transactions (e.g. exchange or transfer) in small amounts under record-keeping or reporting thresholds, similar to structuring cash transactions or making multiple high-value transactions (1) in a staggered and regular pattern, with no further transactions recorded Indicators to be added: A customer provides identification or account credentials (e g, non-standard password, IP address, or flash cookies) shared by another account. Attempt to conceal location - IP address & GSM/Mobile & POA different from each other. IP does not match registration details Telephone number does not match registration details Inability to obtain sufficient information or information is unavailable to positively identify originators or beneficiaries of wallets Customers have no concern regarding the cost of transaction or fees - When BTC/crypto is increasing with high velocity, clients may ignore high costs as the short term profit is relatively high. Meanwhile in a stable crypto-currency market this may be relevant The list at J3 is non exhaustive, as noted at J5. J5 also references the FATF Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (September 2020) which contains several examples including those outlined here. No amendments required. 10 No. Section Comments from the Private Sector Authority s Response Consequent Amendments to the Proposed Measure during a long period afterwards, which is particularly common in ransom ware-related

cases; or (2) to a newly created or to a previously inactive account. (ii) Transferring virtual assets immediately to multiple VASPs, especially to VASPs entities registered or operating in another jurisdiction, including obliged entities, where there is no relation to where the customer lives or there is a non-existent or weak AML/CFT regulation. (iii) Accepting/depositi ng funds from VA addresses that have been identified as holding stolen funds, or VA addresses linked to the holders of stolen funds. (iv) Depositing VAs at an exchange and then immediately withdrawing the VAs from a VASP immediately to a private wallet. This effectively turns the exchange/VASP into an ML mixer. 11 No. Section Comments from the Private Sector Authority s Response Consequent Amendments to the Proposed Measure (v) Converting a large amount of fiat currency into VAs, or a large amount of one type of VA into other types of VAs with no logical business explanation. (b) In relation to Anonymity: (i) The services of a VASP serve to generate anonymity. (ii) The VAs have a history (above average) of one or more mixers or trade history on the Dark web. (iii) Moving a VA that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange and then immediately trading it for an AEC or privacy coin. (iv) VAs transferred to or from wallets that show previous patterns of activity associated with the use of VASPs that operate mixing or tumbling services or P2P platforms. (v) Funds deposited or withdrawn from a VA address or wallet with 12 No. Section Comments from the Private Sector Authority s Response Consequent Amendments to the Proposed Measure direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports. (c) In relation to Customers (whether sender or receiver): (i) Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by VASPs. (ii) Incomplete or insufficient CDD information, or a customer declines requests for CDD documents or inquiries regarding source of funds. (iii) A customer s VA address appears on public forums associated with illegal activity. (iv) A customer significantly older than the average age of platform users opens an account and engages in large numbers of 13 No. Section Comments from the Private Sector Authority s Response Consequent Amendments to the Proposed Measure transactions, suggesting their potential role as a VA money mule or a victim of elder financial exploitation. (v) A customer frequently changes his or her identification information, including addresses, IP addresses, or financial information, which may also indicate account takeover against a customer. (vi) Bulk of a customer s source of wealth is derived from investments in VAs, ICOs, or fraudulent ICOs, etc. (d) In relation to Geographical risks: (i) Customer s funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located. (ii) Customer sends funds to VASPs operating in jurisdictions that have no VA regulation, or have not implemented AML/CFT controls. 14 No. Section Comments from the Private Sector Authority s Response Consequent Amendments to the Proposed Measure 12. J.5 The above noted indicators (at paras 3 and 4) are neither exhaustive nor applicable in every situation. Indicators should be considered in the context of other characteristics about the customer and relationship, or a logical business explanation. For more information on red flag indicators, see FATF Report on Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (September 2020). It should be emphasize that VASPs have to also take into account classic AML red flags. Feedback noted. Minor

amendment made to reference general requirements in the Guidance Notes. Amended. 13. J.6. Where a VASP detects suspicious activity, in relation to an incoming transfer of virtual assets from an external party that cannot be stopped due to processes associated with the blockchain, steps should be taken restrict the actions that can be performed by its customer in relation to the suspicious funds, freeze the assets/funds (where possible) and VASPs do not have the possibility to freeze outgoing funds, the only possible action could be white listed addresses and this won t fully make the risk disappear, or application of the travel rule. The 2019 FATF Guidance for a Risk- Based Approach to Virtual Assets and Virtual Asset Service Providers recommends that authorities should require both originating and beneficiary entities to take freezing actions (where possible) and prohibit transactions with designated persons and entities. The Guidance at section J6 is in line with this recommendation. No amendments required. 15 No. Section Comments from the Private Sector Authority s Response Consequent Amendments to the Proposed Measure report the suspicious activity. 14. K.1. When engaging in or providing services related to transfers of VAs in or from within Cayman Islands, VASPs are expected to collect and record information as follows: a) Originating VASPs should obtain and hold accurate originator and beneficiary information on virtual asset transfers, submit this information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities; b) Beneficiary VASPs should obtain and hold required originator information and required and accurate beneficiary Does that also apply to private wallets, P2P and Defi? K 1 is applicable to all transfers of virtual assets , as defined in the VASP Law. No amendments required. Technological solutions are still in beta versions (such as OpenVasp, trisa, sygna, trp), how should vasp proceed without one ? (secured emails???). How about data protection? Should an agreement be in place between 2 Vasps to transfer the personal data? The Authority encourages technological solutions to optimize the CDD process for VASPs. No amendments required. This section appears to reflect the VA additions to FATF Recommendation 16 on wire transfers. FATF recognises that VA transfers are different to conventional wire transfers and it would be helpful to similarly recognise this in the GNs - see following from FATF Guidance for a Risk- Based Approach: Virtual Assets and Virtual Asset Service Providers: 117. The FATF recognizes that unlike traditional fiat wire transfers, not every VA transfer may involve (or be bookended by) two obliged entities, whether a VASP or other obliged entity such as a FI... VASPs receiving a VA transfer from an entity that is not a VASP or other obliged entity (e.g., from an individual VA user using his/her own DLT software, such as an unhosted wallet), should obtain the required originator information from their customer. The GNs should be updated to reflect the practical reality that VASPs will face the above situation, so that it is clear that when a VA transfer involves a customer and an individual using an unhosted wallet, the VASP needs to obtain all necessary information via their customer (i.e. it is the customer that needs to provide information on the Feedback was noted and accepted and amendments have been made to reflect same. Amended. 16 No. Section Comments from the Private Sector Authority s Response Consequent Amendments to the Proposed Measure information on virtual asset transfers and make it available on request to appropriate authorities. non-obliged originator/beneficiary that they are receiving from / sending to, in the absence of an obliged entity bookending the other side of the transfer from / to the VASP).