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 Amendments to the Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands August 2023 Sector Specific Guidance for Virtual Asset Service Providers No. Section General Comments Authority s Response Consequent Amendments to the Proposed Measure SECTION SPECIFIC COMMENTS 1. Section A.6.: OVERVIEW 6. When determining if an activity falls within the definition of a virtual asset service (VAS), it is important to consider the nature of the service and its function in practice. For example, an activity such as issuing and/or trading in non-fungible tokens or virtual service tokens may still fall under the definition of a virtual asset service if the tokens are to be used for payment or investment purposes in practice. Regardless of the terminology, activities should be considered on a case-by-case basis. This paragraph seems contrary to the VASP Act, which clearly provides that virtual service tokens are not virtual assets and therefore any transaction involving a virtual service token cannot by definition amount to a virtual asset. It also adds to the general confusion on whether non- fungible tokens are virtual assets or not. Additionally, this paragraph seems to take the FATF s guidance a step too far. The FATF guidance on non- fungible tokens states that authorities need to take a functional approach and look beyond the marketing associated with non-fungible tokens to determine if the product or service in question qualifies as a virtual asset, virtual asset service provider, a financial institution, or a designated non- financial business or profession. The Authority confirms that a functional approach will be used in determining if activities, inter alia, related to non-fungible tokens or virtual service tokens are deemed a virtual asset service on a case- by-case basis. No amendment required. 2 No. Section General Comments Authority s Response Consequent Amendments to the Proposed Measure SECTION SPECIFIC COMMENTS Further, the above highlighted paragraph is contrary to Section B.5. SCOPE: Virtual service tokens, as defined in the VASP Act, are not captured in the Guidance Notes. Such items are non-transferrable, 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. 2. Section B.6.: SCOPE 6. The PoCA and VASP Act do not seek to regulate the technology that underlies virtual assets (VAs) but rather the persons that may use technology or software applications to conduct, as a business, virtual assets services on behalf of a natural or legal person. A person who develops or sells either a software application of a new virtual asset platform (i.e. a fintech service provider) therefore does not constitute a VASP when solely developing or selling the application or platform, but they may be a VASP if they also use the new application or platform to engage as a business in exchanging or transferring funds or virtual assets or conducting any of the other virtual asset service or operations on behalf of another natural or legal person. Similarly, a decentralised finance (DeFi) application (i.e. the software program) is not a VASP but the The last line of Section B.6.: SCOPE seems to loosely track the FATF guidance. CMRAI could provide additional examples here from the FATF review. The Authority has reviewed the feedback and while it loosely tracks the FATF guidance, the Authority retains the paragraph to allow for a functional approach in the interpretation as anticipated in the FATF guidelines. However, the Authority takes this opportunity to amend the last line of Section B.6. Scope to read as follows: Section B.6. ...Similarly, a decentralised finance (DeFi) application

(i.e. the software program) is not a VASP but the creators, owners and operators or some other any person who maintains control or sufficient influence in the DeFi arrangements, even if those arrangements seem decentralised, may fall under the FATF definition of a VASP where they are providing or The last sentence of section B.6 now reads as follows: B.6 ... Similarly, a decentralised finance (DeFi) application (i.e. the software program) is not a VASP but any person who maintains control or sufficient influence in the DeFi arrangements, even if those arrangements seem decentralised, may fall under the definition of a VASP where they are providing or actively facilitating VASP services. 3 No. Section General Comments Authority s Response Consequent Amendments to the Proposed Measure SECTION SPECIFIC COMMENTS creators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements, even if those arrangements seem decentralised, may fall under the FATF definition of a VASP where they are providing or actively facilitating VASP services. actively facilitating VASP services. 3. Section C.1.: FACTORS THAT GIVE RISE TO MONEY LAUNDERING, TERRORIST FINANCING, AND PROLIFERATION FINANCING RISKS Privacy and Anonymity VAs due to their features and characteristics, have a higher ML/TF/PF risk associated with them. The context of the first sentence This is a broad statement. What is used to substantiate this? Does the National Risk Assessment support this assertion? Suggest re-stating as may have higher . The Authority has reviewed the suggestion and amended the first sentence of C.1 Privacy and Anonymity as follows: VAs due to their features and characteristics, may have a higher ML/TF/PF risk associated with them. The first sentence of C.1 Privacy and Anonymity now reads as follows: VAs due to their features and characteristics, may have a higher ML/TF/PF risk associated with them. 4. Section I.8.: INTERNAL AND SAR REPORTING PROCEDURES 8. VASPs that control both the originating and beneficiary VASP must consider the information from both to determine whether to file a SAR. VASPs should file the suspicious activity report in the country from which the transfer of virtual assets originated or to which the transfer of virtual assets was destined and make relevant transaction information available to the Financial Reporting Authority and the relevant authorities in the country from which the transfer originated or to which it was destined. While this paragraph is meant to focus solely on Cayman obligations, it separately imposes an obligation to file a SAR in foreign jurisdictions. Such a suggested obligation is not required under Cayman law and goes beyond what other jurisdictions required their financial service providers to do. The Authority has reviewed the feedback and notes that Section I.8 was inserted in accordance with Anti-Money Laundering Regulation (AMLR) 49M and is consistent with AMLR 46 relating to wire transfers. The guidance in section I.8 does not require a SAR to be filed in a foreign jurisdiction if either the originator or beneficiary VASP is in Cayman. No amendment required. 4 No. Section General Comments Authority s Response Consequent Amendments to the Proposed Measure SECTION SPECIFIC COMMENTS 5. J.2 IDENTIFICATION AND RECORD-KEEPING FOR VIRTUAL ASSET TRANSFERS Information to be collected and recorded include the: a) originator s name (i.e., the sending customer) and the name of the beneficiary; b) where an account is used to process the transfer of virtual assets by (i) the originator, the account number of the originator; or (ii) the beneficiary, the account number of the beneficiary; c) the address of the originator/beneficiary (including IP/wallet address), the number of a Government issued document evidencing the originator's/beneficiary s

identity or the originator s/beneficiary s customer identification number or date and place of birth; and d) where an account is not used to process the transfer of virtual assets, the unique transaction reference number that permits traceability of the transaction. Who should collect/record information is unclear Should this not be split into two sections: one for sending VASP and one for receiving VASP? E.g. a receiving VASP should collect and confirm information on the beneficiary, and record information on the originator. A sending VASP should collect and confirm information on the originator and collect information on the receiver. As it stands now it is unclear which entity (receiving/sending VASP) is meant to do what. Should a receiving VASP collect information on the originator or simply receive it and hold it? The Authority has reviewed the comment and takes this opportunity to split the originator and beneficiary requirements into two sections to align with the approach in the AMLRs. Section J.2. (C) and newly inserted Section J.3. (C) have also been amended with regards to the address for an abundance of clarity as follows: 2(C) and 3(C) ..., the IP address, the wallet address (including IP/wallet address), the number of a Government issued document evidencing the ... Section J.2 and J.3 will now read as follows: 2. Information to be collected and recorded for the originating VASP include the: a) originator s name (i.e., the sending customer) and the name of the beneficiary; b) where an account is used to process the transfer of VAs by (i) the originator, the account number of the originator; or (ii) the beneficiary, the account number of the beneficiary; c) the address of the originator, the IP address, the wallet address, the number of a Government issued document evidencing the originator s identity or the originator s customer identification number or date and place of birth; and d) where an account is not used to process the transfer of VAs, the unique transaction reference number that permits traceability of the transaction. 3. Information to be collected and recorded for the

5 No. Section General Comments Authority s Response Consequent Amendments to the Proposed Measure SECTION SPECIFIC COMMENTS beneficiary VASP include the: a) originator s name (i.e., the sending customer) and the name of the beneficiary; b) where an account is used to process the transfer of VAs by (i)the originator, the account number of the originator; or (ii)the beneficiary, the account number of the beneficiary; c) the address of the beneficiary, the IP address, the wallet address, the number of a Government issued document evidencing the beneficiary s identity or the beneficiary s customer identification number or date and place of birth; and d) where an account is not used to process the transfer of VAs, the unique transaction reference number that permits traceability of the transaction. 6. Section P.1.: OBLIGATION OF A VASP TO COMPLY WITH REQUIREMENTS 1. VASPs must comply with all relevant requirements in the countries in which they operate, Similar to the comment related to Section 1 I(8), this paragraph/requirement seems overly broad and seeks to impose obligations outside of the Cayman Islands, which is ultra vires for the purposes of the Cayman AML Guidance Notes. The Authority has reviewed the feedback and notes that Section P.1 was inserted in accordance with AMLR 49L and is consistent with AMLR 45 relating to wire transfers. No amendment required. 6 No. Section General Comments Authority s Response Consequent Amendments to the Proposed Measure SECTION SPECIFIC COMMENTS either directly or through their agents. 7. K.1 TRANSFERS OF VIRTUAL ASSETS K. TRANSFERS OF VIRTUAL ASSETS VASPs must use all relevant documents provided and data obtained to effectively verify the information on the originator before conducting the transfer of virtual

assets. First sentence refers to VASPs but may be best to specify originator VASP Originating/sending VASPs? Surely this does not apply to the receiving VASP. The Authority has reviewed the suggestion and amended section K.1. as follows: K.1 VASPs must use all relevant documents provided and data obtained to effectively verify the information on the originator before when conducting the transfer of virtual assets; and the beneficiary when receiving the transfer of virtual assets. Section K.1. now reads as follows: K.1. VASPs must use all relevant documents and data obtained to effectively verify the information on the originator when conducting the transfer of virtual assets; and the beneficiary when receiving the transfer of virtual assets. 8. Section C: FACTORS THAT GIVE RISE TO MONEY LAUNDERING, TERRORIST FINANCING, AND PROLIFERATION FINANCING RISKS Consider for potential incorporation into the guidance or where further clarification can be considered: ML/TF/PF risks arising from regulatory arbitrage for wallets provided by VASPs in jurisdictions with no or weak AML requirements. The Authority has reviewed the feedback and retains Section C as presented and notes that Section D Risk Management, references ML/TF risks that VASPs must assess prior to engaging in virtual asset services activities which include geographical risk, more specifically that ...VASPs should take into account publicly available information about the regulatory treatment and use of virtual assets in No amendment required. 7 No. Section General Comments Authority s Response Consequent Amendments to the Proposed Measure SECTION SPECIFIC COMMENTS particular jurisdictions to assess geographical risk. 9. Section D: RISK MANAGEMENT Consider for potential incorporation into the guidance or where further clarification can be considered: Specific AML risk considerations on virtual asset tokens interacting with such as the reputational risk, traceability, regulatory and legal risk of the particular token. The Authority has reviewed the feedback and notes that Section D Risk Management broadly covers the risks identified. Section D.2.b gives further considerations for product risks that may apply to virtual service tokens. No amendment required. 10. Section E: CUSTOMER DUE DILIGENCE Consider for potential incorporation into the guidance or where further clarification can be considered: Simplified due diligence and KYC/CDD exemption expectations for low-risk counterparties such as publicly listed companies, regulated financial institutions, government institutions and specific low-risk classification factors (identified in Section 1 C(10) pg.6). The use of on-chain KYC and third-party KYC providers to identify and verify customers. The Authority notes that simplified due diligence and KYC/CDD exemption expectations are referenced in Part IV and Part V of the AMLRs and in Section 5 of the Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands August 2023 which includes e-KYC guidance. No amendment required. 11. Section F: RELATED MEASURES FOR CDD Consider for potential incorporation into the guidance or where further clarification can be considered: The use of Blockchain analysis to: verify asset provenance; The Authority notes that the use of blockchain analysis as suggested is implicit within the Section F Related Measures for CDD. No amendment required. 8 No. Section General Comments Authority s Response Consequent Amendments to the Proposed Measure SECTION SPECIFIC COMMENTS assess wallet risks due to direct and indirect exposures to high-risk activities (hacks, unregulated exchanges, mixers, etc.). Ongoing monitoring (or periodic review) of risk factors related to the customer profile. 12. Section I: INTERNAL AND SAR REPORTING PROCEDURES

Consider for potential incorporation into the guidance or where further clarification can be considered: 1. Timing of reporting. 2. Documentation expectations: -SARs should be clearly documented; -The use of blockchain analysis graphs to illustrate asset movements related to SAR. 3. Review by senior and independent officer (MLRO, etc.) 4. Red flags: - A customer who knows little or is reluctant to disclose basic details about the payee. The Authority notes that the list provided is not exhaustive and need not be updated to incorporate these factors as they are set out within Section 9 of the Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands August 2023, the AMLRs, and in the Guidance on Preparing and Submitting High Quality SARs issued by the Financial Reporting Authority. No amendment required. 13. Section J: IDENTIFICATION AND RECORD KEEPING FOR VIRTUAL ASSET TRANSFERS Consider for potential incorporation into the guidance or where further clarification can be considered: Internal ledger changes/transfers should be recorded as part of the customer's overall transaction history. The Authority has noted the comment and adjustments have been made to Section D.2.a.(ii) with the incorporation of off-chain transactions as one of the examples that VASPs should monitor. Section D.2.a.(ii) now reads as follows: (ii) VASPs should periodically update customer risk profiles of business relationships in order to apply the appropriate level of CDD including ongoing monitoring. Monitoring

transactions involves identifying changes to the customer s business and risk profile (e.g., the customer s behaviour, use of products, whether transactions to/from unhosted wallets, off-chain transactions where applicable and the amounts involved) and keeping it up to date, which may require the application of Enhanced Due Diligence measures. 14. Section K: TRANSFERS OF VIRTUAL ASSETS Consider for potential incorporation into the guidance or where further clarification can be considered: No transaction threshold for identification and record-keeping for virtual asset transfers was indicated. Expectation of de minimis (less than USD/EUR $1,000 FATF Travel Rule) or nominal transactions. The Authority notes that there was no identification of a threshold within the AMLRs and the guidance notes have been aligned with enacted legislation. No amendment required. 15. Section O: REQUIREMENTS FOR INTERMEDIARY VASPS Consider for potential incorporation into the guidance or where further clarification can be considered: Intermediary VASP third-party risk factors. The Authority advises that the VASP risk factors as it exists in the guidance notes in Section C and D will apply to intermediary VASPs. No amendment required.

16. Section P: OBLIGATION OF A VASP TO COMPLY WITH REQUIREMENTS Consider for potential incorporation into the guidance or where further clarification can be considered: Expectations for branches/subsidiaries located elsewhere to apply equivalent or greater AML/CTF measures noted in these Guidelines. The Authority refers to Section D Risk Mitigation whereby branches and subsidiaries are implicit in the VASP parent obligations. No amendment required.