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 Cayman Monetary Regulatory Authority International SUMMARY OF PRIVATE SECTOR CONSULTATION AND FEEDBACK STATEMENT 2020 AMENDMENTS TO THE GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCINGIN THE CAYMAN ISLANDS VIRTUAL ASSETS SERVICE PROVIDERS Section Industry comment Authority s response Consequent amendments to the draft GN A. Overview 3. Section 2 of the Proceeds of Crime Law (POCL) defines... (2) virtual asset service as the business of conducting one or more of the following activities or operations for or on behalf of a person - ... (d) safekeeping or administering virtual assets or instruments enabling control over virtual assets; ... This will bring investment managers in scope. This is an overly broad statement. The definition of virtual asset service is in The Proceeds of Crime (Amendment) Law, 2019. None. B. Scope 6. Closed-loop items are not captured in the GN. Such items are non- transferable, non-exchangeable and Will a closed-loop system be a system where the customer can only redeem The intention of the Authority is to show what is None 2 non-refundable such as airline miles, credit card awards, or similar loyalty program rewards or points, which an individual cannot sell onward in a secondary market. directly with the service provider and rewards or points are non-transferrable between participants in the system, or can rewards or points be transferrable within the closed-loop system? captured by the GN per the activities listed in the POCL, the definition of virtual asset and virtual asset service in The Proceeds of Crime (Amendment) Law, 2019, and any other legislation or guidance. C. Money Laundering, Terrorist Financing, and Proliferation Financing Risks 4. Regulated or licensed financial institutions that provide financial and other services related to virtual assets and ICOs or to customers involved in virtual asset activities or that engage in virtual asset activities themselves should consider the risks identified above. They should apply a risk-based approach when considering establishing or continuing relationships with VASPs, ICOs or customers involved in virtual asset activities, evaluate the ML/TF risks of the business relationship, and assess whether those risks can be appropriately mitigated and managed. In line with section 8 of the AMLRs, the risk assessment must be documented, kept current, and be kept in a way that it is readily available to the Monetary Authority and other authorities competent under the POCL. We would suggest the Authority may wish to consider adding a provision relating to assessing the nature, extent and appropriateness of the VASP s onboarding process, risk assessment methodology, ongoing monitoring and sanctions compliance programmes. The risk assessment elements listed above are not intended to be exhaustve. The nature, extent, and appropriateness of the VASPs onboarding process, risk assessment methodology, ongoing monitoring and sanctions compliance programmes should form part of the overall risk assessment where deemed appropriate based on the FSPs obligation to conduct a comprehensive risk assessment. Please refer to section 3 of Part II of the Guidance Notes and to section 8 and 9 of the AMLRs. None E. AML/CFT Internal Controls Customer Due Diligence 4. Pursuant to section 12 of the AMLRs, VASPs and other related parties should collect the relevant CDD information on We recommend removing transaction hashes as the transaction hashes cannot The transaction hashes are supplemented data points to None 3 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. Such information could include, for example an IP address with an associated time stamp; geo-location data; device identifiers; wallet addresses; and transaction hashes. be used to identify a specific individual. assist with establishing a customer profile. G. Record Keeping 4 2. The public information on the blockchain or other relevant distributed ledger of a particular virtual asset may provide a beginning foundation for record keeping, provided providers and other entities can adequately identify their customers. However, reliance solely on the blockchain or other type of distributed ledger underlying the virtual asset for recordkeeping is not sufficient. For example, the information available on the blockchain or other type of distributed ledger may enable relevant authorities to trace transactions back to a wallet address, though may not readily link the wallet address to the name of an individual. The wallet address contains a user code that serves as a digital signature in the distributed ledger (i.e., a private key) in the form of a unique string of numbers and letters. Additional information will therefore be necessary to associate the address to a real or natural person.
We recommend updating this paragraph. The wallet address is normally the public key or derived from the public key of a user. In certain chains one can create an unlimited number of addresses. The private key will be controlled by an individual person and is normally held offline and only used to sign transactions. The private key is not contained in the wallet address. Therefore, the following update is recommended: ... trace transactions back to a wallet address, though may not readily link the wallet address to the name of an individual. Additional information and procedures will therefore be necessary to associate the address to a private key controlled by a real or natural person. Noted. The following will be deleted: The wallet address contains a user code that serves as a digital signature in the distributed ledger (i.e., a private key) in the form of a unique string of numbers and letters. The sentence will be amended to read: ... For example, the information available on the blockchain or other type of distributed ledger may enable relevant authorities to trace transactions back to a wallet address, though may not readily link the wallet address to the name of an individual. Additional information and procedures will therefore be necessary to associate the address to a private key controlled by a real or natural person. Amended I. Internal and SAR Reporting Procedures 5 4. In the context of ICOs, factors that could give rise to suspicious activity are: (1) An ICO-project is attempting to be anonymous, it does not display team members, company information nor physical address. Team members do not have a social media profile. (2) An ICO-project is trying to hide the amount of funds raised, by providing false information on their website or not providing proof of investments. (3) An ICO-project either has no cap as to the amount of money required to develop its product or has set an extremely high cap. (4) There is a guarantee of high returns that seems impossible to fulfil. (5) An ICO-project has lack of information on the project or lack of detail on how the technology works, there is no well-designed website. (6) There are no development goals on a clear timeline. (7) The ICO intends to convert a portion of the raised funds to fiat. Regarding subsection (7), this would be normal activity for an ICO as they have to

fund the project development through the liquidation of some of the assets. While the Authority is aware that the conversion of raised funds to fiat can be used to fund the project development, the Authority is aware there may be instances where the purposes of the conversion to fiat is unclear. None I. Information to keep with a virtual asset transfer 6 1. When engaging in or providing services related to transfers of virtual assets in or from within Cayman Islands, the wire transfer obligations as set out in Part X of the AMLRs must be complied with as follows: (1) Originating VASPs should obtain and hold required and accurate originator information and required 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.; (2) Beneficiary VASPs should obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers and make it available on request to appropriate authorities. Reference is made to Part X of the AMLRs. Part X of the AMLRs Identification and record- keeping requirements relating to Wire Transfers is applicable to the transfer of funds in any currency. None