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 GUIDANCE NOTES (AMENDMENTS) ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE CAYMAN ISLANDS Issued by the Cayman Monetary Regulatory Authority International Pursuant to section 34 of the Monetary Authority Law (2020 Revision) These Guidance Notes amend the Guidance Notes issued on December 13, 2017 (the GN of December 13, 2017) February 2020 This document is intended to provide general guidance to Financial Service Providers (FSPs). It should therefore, not be relied upon as a source of law. Reference for that purpose should be made to the appropriate statutory provisions. However, FSPs should be aware of the enforcement powers of the Supervisory Authorities under the Anti-Money Laundering Regulations (2020 Revision) (AMLRs) and amendments thereto as they relate to supervisory or regulatory guidance. Contact: Cayman Monetary Regulatory Authority International 171 Elgin Avenue, SIX, Cricket Square P.O. Box 10052 Grand Cayman KY1-1001 Cayman Islands : 345-949-7089 Fax: 345-945-6131 Website: : 2 1. These Guidance Notes may be cited as the Guidance Notes (Amendment) (No.5), February 2020. 2. The GNs of December 13, 2017 are amended to include Section 1 in Part IX, as follows: Section 1 VIRTUAL ASSET SERVICE PROVIDERS The purpose of this part of the Guidance Notes is to provide guidance for virtual asset service providers (VASPs) that require further explanation on issues than are dealt with in the general body of these Guidance Notes. This section must be read in conjunction with Part I and Part II of the Guidance Notes and the Appendices. A. OVERVIEW 1. The guidance notes are issued to assist the Monetary Authority s registrants and licensees in better understanding and fully implementing their obligations as it relates to anti-money laundering/countering financing of terrorism (AML/CFT) when acting as virtual asset service providers (VASPs). The Monetary Authority expects all financial service providers (FSPs) to take account of this guidance and to fully comply with the obligations set out in the Proceeds of Crime Law (POCL) and the Anti-Money Laundering Regulations (AMLRs) when providing relevant virtual asset services. 2. Schedule 6 of POCL lists activities falling within the definition of relevant financial business. Activities include but are not limited to: (1) Money or value transfer services; (2) Issuing and managing means of payment including electronic money; and (3) Providing virtual asset services. 3. Section 2 of the Proceeds of Crime Law (as amended)(POCL)defines (1) virtual asset as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes ; and (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 (a) exchanging between virtual assets and fiat currencies; (b) exchanging between one or more other forms of convertible virtual assets; (c) transferring virtual assets; (d) safekeeping or administering virtual assets or instruments enabling control over virtual assets; and (e) participating in and providing financial services related to an issuer s offer or sale of a virtual asset; . 4. It should be noted that the applicability of regulations other than the AML/CFT legislation to initial coin offerings (ICOs) or virtual asset issuers should always be assessed on a case-by-case basis as virtual assets issued in ICOs vary in terms of their features. Virtual assets which are issued to the public may have the characteristics of securities and therefore may fall within scope of the definition of a security. 3 5. The definition of a security as established in the Securities Investment Business Law is a list of instruments that are common in today's financial markets. Depending on the situation, this can mean that the issuance of virtual assets may also be required to be registered or licensed with the Monetary Authority as

a security provider. Furthermore, the use of virtual assets as a means of payment can also require a virtual asset issuer to consider the registration as a money services business under the Money Services Law (MSL) if it includes the business of providing money transmission or currency exchange. Similarly, if an exchange service accepts fiat currency (such as dollars) from buyers or transmits to sellers, fiat currency, it must give due consideration to regulation concerning money services businesses. B. SCOPE 1. A natural or legal person which falls within the scope of the definition of virtual asset service by virtue of the activities it carries out is referred to in this Guidance Notes as a VASP. 2. Whether a natural or legal person engaged in virtual asset activities is considered a VASP depends on two considerations: (1) whether the person (natural or legal) is engaged as a business in any of the activities described in Schedule 6 of the POCL, and whether the relevant virtual asset services are conducted for or on behalf of another person; and (2) whether there is custody or control of the virtual asset, or ability to actively facilitate the financial activity on the part of the natural or legal person that conducts the business for a customer. 3. The sector specific guidance contained in this section seeks to provide practical assistance to VASPs in complying with the AMLRs, interpreting and applying the general provisions of these Guidance Notes, and for VASPs to adopt sound risk management and internal controls for their operations. 4. The AMLRs apply to VASPs as indicated in the list of activities falling within the definition of Relevant Financial Business in the Sixth Schedule of the POCL. This is regardless of what technology is used by the VASP to conduct the covered virtual asset activities, and whether the VASP uses a decentralised or centralised platform, smart contract, or some other mechanism. 5. It is the responsibility of each VASP to have systems and training in place to prevent ML/TF/PF. This means that each VASP must maintain identification procedures, record-keeping procedures, and such other procedures and controls appropriate for the purposes of forestalling and preventing ML/TF/PF. 6. In practice, the term VASPs will most likely extend, but not be limited to, the following types of companies: (1) Virtual asset exchanges; (2) Wallet service providers; (3) Providers of financial services relating to the issuance, offer or sale of virtual assets, such as through ICOs; (4) Professionals that facilitate the issuance of or assist parties in setting up ICOs; 4 (5) Financial service providers that deal with virtual assets for or on behalf of another person; and (6) Financial service providers that have customers that deal with virtual assets. 6. Closed-loop items are not captured in the GN. 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. 7. The POCL does not seek to regulate the technology that underlies VA or VASPs but rather the natural or legal persons that may use technology or software applications to conduct as a business virtual assets services on behalf of another natural or legal person. A person who develops or sells either a software application of a new virtual asset platform (i.e. a software developer) 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 conducting any of the other financial activities on behalf of another natural or legal person. 8. Further, Schedule 6 of the POCL does not aim to capture natural or legal persons that provide ancillary services or products to a virtual asset network, including hardware wallet manufacture and non-custodial wallets, to the extent that they do not also engage in or facilitate as a business any of the aforementioned VA activities on behalf of their customers. C. MONEY

LAUNDERING, TERRORIST FINANCING, AND PROLIFERATION FINANCING RISKS 1. Virtual assets due to their features and characteristics, have a higher ML/TF/PF risk associated with them. For example, 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. Similarly, VA products or services that facilitate pseudonymous or anonymity-enhanced transactions also pose higher ML/TF/PF risks, particularly if they inhibit a VASP s ability to identify the beneficiary. The range of providers in the VA space and their presence across several, if not nearly all, jurisdictions can increase the ML/TF/PF risks associated with VAs and VA financial activities due to potential gaps in customer and transaction information. 2. These considerations highlight the importance of the Monetary Authority s registrants and licensees, prior to engaging in VASP activities, in carrying out a comprehensive and detailed risk assessment associated with the relevant technology, product, or business practice associated with virtual assets. The obligation to conduct such a risk assessment is enshrined in sections 8 and 9 of the AMLRs, which require FSPs to take steps, appropriate to the nature and size of the business, to identify, assess, and understand its money laundering and terrorism financing 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. 3. In conducting such a risk assessment, the Monetary Authority s registrants and licensees should consider the following elements: 5 (1) The potentially higher risks associated both with VAs that move value into and out of fiat currency and the traditional financial system and with virtual-to- virtual transactions; (2) The risks associated with centralised and decentralised VASP business models; (3) The specific types of VAs that the VASP offers or plans to offer and any unique features of each VA, such as Anonymity-Enhanced Cryptocurrencies (AECs), embedded mixers or tumblers, or other products and services that may present higher risks by potentially obfuscating the transactions or undermining a VASP s ability to know its customers and implement effective customer due diligence (CDD) and other AML/CFT measures; (4) The specific business model of the VASP and whether that business model introduces or exacerbates specific risks; (5) Whether the VASP operates entirely online (e.g. platform-based exchanges) or in person (e.g. trading platforms that facilitate peer-to-peer exchanges or kiosk-based exchanges); (6) Exposure to Internet Protocol (IP) anonymizers such as The Onion Router (TOR) or Invisible Internet Project (I2P), which may further obfuscate transactions or activities and inhibit a VASP s ability to know its customers and implement CDD and other effective AML/CFT measures; (7) The potential ML/TF risks associated with a VASP s connections and links to several jurisdictions; (8) The nature and scope of the VA account, product, or service (e.g., small value savings and storage accounts that primarily enable financially-excluded customers to store limited value); (9) The nature and scope of the VA payment channel or system (e.g., open- versus closed-loop systems or systems intended to facilitate micro-payments or government-to-person/person-to-government payments); and (10) Any parameters or measures in place that may potentially lower the provider s (whether a VASP or other obliged entity that engages in VA activities or provides VA products and services) exposure to risk (e.g., limitations on transactions or account balance). 4. Registered or licensed financial institutions that provide financial and other services related to virtual assets and the issuance of virtual assets 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, virtual asset issuers 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. D. AML/CFT INTERNAL CONTROLS 1. Pursuant to section 8 (2)(e) of the AMLRs, VASPs are required to implement policies, controls and procedures that enable them to manage and mitigate the risks that have been identified either at the national level through the National Risk Assessment (NRA) or by the VASP itself through its business risk assessment as set out in Chapter C, and to have such policies, controls and procedures approved by senior management. Such internal controls must be adequate to ensure proper risk management across the VASPs operations, departments, branches and subsidiaries, both domestically and, where relevant, abroad, and include appropriate governance arrangements where responsibility for AML/CFT is clearly allocated and a compliance officer is appointed at 6 management level; controls to monitor the integrity of staff; ongoing training of staff; and an independent audit function to test the system. 2. The internal policies, controls and procedures must furthermore address the various topics detailed in section 5 of the AMLRs, which include: (1) Customer due diligence (CDD) measures; (2) Ongoing monitoring; (3) Record keeping; (4) Implementation of targeted financial sanctions; and (5) Internal and suspicious activity reporting (SAR) procedures. E. CUSTOMER DUE DILIGENCE 1. Pursuant to sections 10 to 20 of the AMLRs, VASPs have to apply the full set of CDD measures as pertains to all FSPs, including identification and verification measures in relation to customers and beneficial owners, obtaining information on the purpose and intended nature of the business relationship, and to conduct ongoing CDD throughout the lifespan of the business relationship. 2. In practice, VASPs typically open and maintain accounts or establish a customer relationship and collect the relevant CDD information when they provide services to or engage in covered VA activities on behalf of their customers. In cases where a VASP carries out a one-off transaction, however, 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. 3. Regardless of the nature of the relationship or transaction, VASPs must have in place effective procedures to identify and verify the identity of a customer, including when establishing business relations with that customer; where VASPs may have suspicions of ML/TF/PF, regardless of any exemption of thresholds; and where they have doubts about the veracity or adequacy of previously obtained identification data. 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. Such information could include, for example an IP address with an associated time stamp; geo-location data; device identifiers; wallet addresses; and transaction hashes. VASPs may also match a customer s addresses against a list of blacklisted addresses on popular blockchains, e.g. addresses that have been misused or have been found to have been used by malicious individuals. The VASP should also seek to determine the provenance of a virtual asset e.g. if it has been moved from a blacklisted address recently. 5. Pursuant to section 18 and section 19 of the AMLRs, if a VASP is unable to obtain customer information, the transaction should not proceed and the VASP should consider filing a suspicious activity report to the Financial Reporting Authority (FRA). 7 6. As prescribed in sections 27 and 28 of the AMLRs, where the ML/TF risk is higher based on the existence of any of the circumstances listed in section 27 of the AMLRs, enhanced CDD measures must be taken. For example, VA transfers from or associated with countries with significant levels of organized crime, corruption, terrorist or other criminal activity, including source or transit countries for illegal drugs, human trafficking, smuggling, and illegal gambling, or countries subject to sanctions or embargos, or countries with weak governance, law enforcement and regulatory regimes may present higher risks for money laundering or terrorist financing. Other indicators may be risk factors associated with the VA product, service, transaction, or delivery channel, including whether the activity involves pseudonymous or anonymous transactions, non-face-to-face business relationships or transactions, and/or payments received from unknown or un-associated third parties. 7. Enhanced CDD measures that may mitigate the potentially higher risks associated with the factors mentioned in section 27 of the AMLR include: (1) corroborating the identity information received from the customer, such as a national identity number, with information in third-party databases or other reliable sources; (2) tracing the customer s IP address; (3) searching the Internet for corroborating information consistent with the customer s transaction profile; (4) obtaining additional information on the customer and intended nature of the business relationship; (5) obtaining information on the source of funds of the customer; (6) obtaining information on the reasons for intended or performed transactions; and (7) conducting enhanced monitoring of the relationship. 8. VASPs should also apply the requirements of Part VII AMLR on Politically Exposed Persons (PEPs). F. ONGOING MONITORING 1. Based on a holistic view of the information obtained in the context of the application of CDD measures, VASPs must prepare a customer business and risk profile. A customer s business and risk profile will determine the level and type of ongoing monitoring potentially necessary and support the VASP s decision whether to enter into, continue, or terminate the business relationship. 2. Risk profiles can apply at the customer level (e.g., nature and volume of trading activity, origin of virtual funds deposited, etc.) or at a cluster level, where a cluster of customers displays homogenous characteristics (e.g., clients conducting similar types of transactions or involving the same virtual asset). VASPs should periodically update customer risk profiles of business relationships in order to apply the appropriate level of CDD. As part of its ongoing monitoring, a VASP should screen its customer s and counterparty s wallet addresses against any available blacklisted wallet addresses that countries might have made available. If there is a positive hit, the VASP should determine whether additional mitigating or preventive actions are warranted, and where necessary not establish or continue the business relations. A VASP should make its own risk-based assessment and

determined whether additional mitigating or preventive actions are warranted if there is a positive hit. 3. Monitoring transactions also involves identifying changes to the customer s business and risk profile (e.g., the customer s behaviour, use of products, and the amounts involved) and keeping it up to date, which may require the application of EDD measures. Monitoring transactions is an essential component in identifying 8 transactions that are potentially suspicious, including in the context of virtual asset transactions. Transactions that do not fit the behaviour expected from a customer profile, or that deviate from the usual pattern of transactions, may be potentially suspicious. 4. Monitoring should be carried out on a continuous basis and may also be triggered by specific transactions. Where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring transactions, and flagged transactions should go through expert analysis to determine if such transactions are suspicious. VASPs and other related entities should understand their operating rules, verify their integrity on a regular basis, and check that they account for the identified ML/TF risks associated with virtual assets, products or services or activities. 5. Monitoring under a risk-based approach allows VASPs and other related entities to create monetary or other thresholds to determine which activities will be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the risk levels established. G. RECORD KEEPING 1. VASPs are to maintain transaction records on transactions and information obtained through CDD measures in line with Part VIII of the AML Regulation, which shall include: information relating to the identification of the relevant parties, the public keys (or equivalent identifiers), addresses or accounts involved (or equivalent identifiers), the nature and date of the transaction, and the amount transferred, for example. 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. Additional information and procedures will therefore be necessary to associate the address to a private key controlled by a natural or legal person. H. IMPLEMENTATION OF TARGETED FINANCIAL SANCTIONS 1. VASPs are under a clear obligation to freeze without delay the funds or other assets including VAs of designated persons or entities and to ensure that no funds or other assets including VAs are made available to or for the benefit of designated persons or entities in relation to the targeted financial sanctions related to terrorism or terrorist financing, or proliferation of weapons of mass destruction. Please refer to section 13 of Part II of the GN for more information on sanctions. I. INTERNAL AND SAR REPORTING PROCEDURES 1. VASPs should have the ability to flag for further analysis any unusual or suspicious movements of funds or transactions or activity that is otherwise indicative of potential involvement in illicit activity regardless of whether the transactions or activities are fiat-to-fiat, virtual-to-virtual, fiat-to-virtual, or virtual-to-fiat in nature. 2. VASPs and other related entities should have appropriate systems so that such funds or transactions are scrutinised in a timely manner and a determination can be made as to whether funds or transactions are suspicious. Pursuant to section 19 of the AML Regulations, VASPs must promptly report suspicions of money laundering or terrorist 9

financing to the FRA, including those involving or relating to virtual assets and/or providers that are suspicious. 3. Some indicators of unusual or suspicious activities related to virtual assets are: (1) Customers that are active on the dark web. (2) Large amounts sent via virtual assets, in one transfer or in multiple transfer which in aggregate amount to large amounts (3) Large quantities of virtual assets from private persons, which quantities are not common for an average private person. (4) The services of a virtual asset provider serve to generate anonymity. (5) Paying and willingness to pay high commission fees for converting (selling) virtual assets in exchange for fiat currency or against cash, compared to commission fees charged by normal virtual asset exchanges. (6) The virtual assets have a history (above average) of one or more mixers or trade history on the Dark web. (7) A trader cannot be found under his own name on the internet or is not registered with a business association or not known with the tax authority for exchange activities. 4. In the context of virtual asset issuers and ICOs, factors that could give rise to suspicious activity are: (1) An ICO-project 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 misleading, incomplete or suspicious 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. (8) The virtual currency has anonymity features that aid in the commission of illegal activity, services or transactions. J. INFORMATION TO KEEP WITH A VIRTUAL ASSET TRANSFER 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. 2. The POCL defines transfer, in relation to a virtual asset, as conducting a transaction on behalf of a natural or legal person that moves a virtual asset from one virtual asset address or account to another. 3. The required information includes the: 10 (1) originator s name (i.e., the sending customer); (2) originator s address; or (3) originator s date and place of birth; (4) originator s customer identification number; or (5) number of a Government-issued document evidencing the originator s identity; (6) originator s account number (where such an account is used to process the transaction, e.g., the virtual asset wallet) or a unique identifier which allows the transaction to be traced back to the originator; (7) beneficiary s name; and (8) beneficiary account number (where such an account is used to process the transaction, e.g., the virtual asset wallet) or unique transaction reference in order to facilitate the traceability of the transaction. 4. It is not necessary for the information to be attached directly to the virtual asset transfer, meaning that the required information need not be communicated as part of (or incorporated into) the transfer on the blockchain or other distributed ledger platform itself. 5. The information can be submitted either directly

or indirectly. VASPs should submit the required information simultaneously or concurrently with the transfer. Submitting information to the beneficiary VASP could thus be an entirely distinct process from that of the blockchain or other distributed ledger transfer. 6. Other requirements such as monitoring of the availability of information and taking freezing action and prohibiting transactions with designated persons and entities also apply. The same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.