



# 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.

**GUIDANCE NOTES (AMENDMENTS) ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING IN THE CAYMAN ISLANDS**

Issued by the Cayman Monetary Regulatory Authority International Pursuant to Section 34 of the Monetary Authority Act (2020 Revision) These Guidance Notes amend the Guidance Notes issued in August 2023 (the GNs of August 2023) September 2023 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 (2023 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: : Appendix 1 2

1. These Guidance Notes may be cited as the Guidance Notes (Amendment) Virtual Asset Service Providers September 2023. 2. The GNs of August 2023 are amended by deleting Section 1 in Part IX, and replacing it as follows: PART IX SECTOR SPECIFIC GUIDANCE: VIRTUAL ASSET SERVICE PROVIDERS SECTION 1 VIRTUAL ASSET SERVICE PROVIDERS A. OVERVIEW 1. This guidance is issued to assist Virtual Asset Service Providers ( VASPs ), as defined in the Virtual Asset (Service Providers Act), (2022 Revision) (VASP Act), in better understanding and fully implementing their obligations as it relates to anti-money laundering/ countering financing of terrorism/ countering proliferation financing ( AML/CFT/CPF ) 1 . 2. Schedule 6 of the PoCA lists activities falling within the definition of relevant financial business which includes providing virtual asset services . 3. The VASP Act provides a framework for the conduct of virtual asset business in the Islands, the registration and licensing of persons providing virtual asset services and for incidental and connected purposes. 4. Sections 9(3)(d) and (e) of the VASP Act provides that all VASPs: must comply with the Anti-Money Laundering Regulations (2020 Revision) and other laws relating to the combating of money laundering, terrorist financing and proliferation financing; and for the purpose of ensuring compliance with the Anti-Money Laundering Regulations (2020 Revision), put in place anti-money laundering systems and procedures . 5. Both the VASP Act and PoCA define the terms virtual asset and virtual asset service in a similar manner. The VASP Act also defines, among others, the terms virtual asset service provider , virtual asset custodian , virtual asset custody service , virtual asset trading platform and virtual asset issuance . 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 1 In this guidance where AML/CFT omits PF , reference should still be made (for any equivalent PF provisions) to Section 14 of the Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing. 3 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. B. SCOPE 1. 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. The Monetary Authority expects all VASPs to take account of this guidance and to fully comply with relevant obligations as set out in the PoCA and the AMLRs. 2. The AMLRs have been extended to entities providing virtual asset services as defined in the VASP Act and the PoCA. This is regardless of what technology or method of delivery is used by the VASP to conduct the virtual asset activities, and whether the VASP uses a decentralised or centralised platform, smart contract, or some other mechanism. 3. It is the responsibility of each VASP to have systems, policies, procedures and training in place to prevent ML/TF/PF. This means that each VASP must maintain identification verification and ongoing monitoring procedures, record-keeping procedures, and such other procedures and controls appropriate for the purposes of forestalling and preventing ML/TF/PF. 4. In accordance with the VASP Act, the term VASPs includes the following types of persons: (1) Virtual asset trading platforms; (2) Virtual assets custodians such as wallet service providers; (3) Virtual asset issuers, whether registered or licensed; and (4) Professionals that participate in or provide, financial services related to virtual asset issuance or the sale of a virtual asset. (5) Existing licensees conducting virtual asset services (including virtual asset custodial services, virtual asset trading platform services and virtual asset issuance). (6) Any person facilitating (i) the exchange or transfer of virtual assets to/from another virtual asset or fiat currency, (ii) the transfer of virtual assets, or (iii) the exchange between one or more other forms of convertible virtual assets on behalf of another person or entity. 5. Virtual service tokens, as defined in the VASP Act, 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. 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 4 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 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. 7. Further, the PoCA and VASP Act do 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. FACTORS THAT GIVE RISE TO MONEY LAUNDERING, TERRORIST FINANCING, AND PROLIFERATION FINANCING RISKS

Privacy and Anonymity: 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 transaction or activities and inhibit a VASP's ability to know its customers and implement CDD and other effective AML/CFT/CPF 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.

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 volume of transactions is substantial.

Decentralised Nature of VASPs business models: 3. VASPs business models can be centralised or decentralised. Where it is decentralised, there is no central server or service provider that has overall responsibility for identifying users, monitoring transactions, reporting suspicious activity and acting as a contact point for law enforcement. Consequently, individuals and transactions may not be subject to risk assessment and mitigation processes equivalent to those required by AML/CTF/CPF regulation. Where VASPs deal with funds originating from decentralised systems, risk-based mitigation measures, such as blockchain analysis, should be applied.

Cross Border Nature: 4. VASPs connections and links to multiple jurisdictions may give rise to ML/TF/PF risks. VASPs will need to ensure that they are able to effectively apply all AML/CTF/CPF processes in the jurisdictions in which they operate and compensate for any additional risk introduced by the cross-border nature of a transaction on a risk-sensitive basis.

Segmentation: 5. The infrastructure used to operate a virtual asset trading platform, make transfers and execute payments may be complex and may involve several entities in different jurisdictions. This increases the risk through partial oversight of virtual asset systems and may hinder access to relevant actors by law enforcement. In such instances, VASPs should seek to work together with other parties in the value chain so as to compensate for segmentation and provide a more robust AML/CTF/CPF framework. VASPs working with outsourced service providers or agents will retain responsibility for AML/CTF/CPF compliance by outsourced service providers and agents.

Acceptability, Immutability and Convertibility: 6. A wide availability of points of acceptance of virtual assets to conduct transactions, and the ability to exchange virtual assets into money or other virtual assets makes it harder to track transactions and gives rise to new types of financial crime not associated with traditional payment and financial services products including the risk of money laundering. While there may be no single mitigation control, a number of measures may be employed to mitigate the arising risks including documenting and tracking financial crime typologies.

7. Once a transaction has been validated, the record cannot easily be altered. This makes it more difficult for misappropriated virtual assets to be retrieved. Customers should be made aware of such risks to minimise the likelihood of accidental loss.

Operational structure: 8. VASPs should take into account their operational structure in seeking to assess and mitigate risks in their operations. These include: (a) 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); (b) 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); 6 (c) 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 (d) Any parameters or measures in place that may potentially lower the provider's (whether that provider is 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).

9. 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) include: (a) The ability of users to: (i) operate more than one account with the provider; (ii) operate accounts on behalf of third parties. (b) The customer: (i) Is involved in virtual asset mining operations (either directly or indirectly through relationships with third parties) that take place in a high-risk jurisdiction, relate to higher-risk virtual assets (such as privacy coins) or where its organisation gives rise to higher risk; (ii) Uses VPN, TOR, encrypted, anonymous or randomly generated or a temporary service; (iii) Requests an exchange to or from cash, privacy coins or anonymous electronic money; (iv) Sends virtual assets to a newly created address; (v) Persistently avoids thresholds through smaller transactions; (vi) Sends or receives virtual assets to/from peer-to-peer exchanges, or funds/withdraws money without using the platform's other features; or (vii) Exploits technological glitches or failures to his advantage. (c) The virtual asset comes from, or is associated with, the darknet or other illegal/high-risk sources, such as an unregulated exchange, or is associated with market abuse, ransomware, hacking, fraud, Ponzi schemes, sanctioned bitcoin addresses or gambling sites.

10. Specific low risk classification factors VASPs may consider (in addition to the factors set out in Section 3D of Part II of these Guidance Notes) include: (a) A low-risk nature and scope of the account, product, or service (e.g., small value savings and storage accounts that primarily enable financially-excluded customers to store limited value); (b) Product parameters or measures that lower the provider's exposure to risk, such as limitations on transactions or account balance; 7 (c) The customer requests an exchange and either the source of or destination for the money is the customer's own account with a bank in a jurisdiction assessed by the VASP as low risk; (d) The customer requests an exchange and either the source of or destination for the virtual asset is the customer's own wallet that has been whitelisted or otherwise determined as low-risk; (e) The customer requests an exchange and either the source of or destination for the virtual asset relates to low value payments for goods and services; and (f) The results of a blockchain analysis indicate a lower risk.

**D. RISK MANAGEMENT**

**Risk Assessment**

1. Prior to engaging in VAS activities, VASPs must carry out a comprehensive and detailed risk assessment associated with the relevant technology, product, or business practice associated with virtual assets, in accordance with Section 3 C of these Guidance Notes.

2. The obligation to conduct such a risk assessment is enshrined in Regulations 8 and 9 of the AMLRs, which require persons carrying 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, country, 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 mechanisms, and new or developing technologies prior to their launch.

a. Customer risk: (i) A customer's business and risk profile will determine the level and type of ongoing monitoring necessary

and support the VASP's decision whether to enter into, continue, or terminate the business relationship. 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 display homogenous characteristics (e.g., clients conducting similar types of transactions or involving the same virtual asset). (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 and the amounts involved) and keeping it up to date, which may require the application of Enhanced Due Diligence measures. (iii) As part of its ongoing monitoring, a VASP should screen its customer's and counterparty's wallet addresses<sup>8</sup> against any available blacklisted and/or sanctioned 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.

b. Product risk: The features of the service offered as well as the virtual asset which customers may hold, store, transfer or exchange determine the overall risk associated with the product. Any changes to the service or virtual assets offered should be assessed for their impact on risk prior to their introduction. (See also Section 3D (9&10) of Part II of these Guidance Notes on risk assessment in relation to the use or development of new products/services etc).

c. Transaction risk: The risk of a transaction is established by analysing the blockchain, where possible, to obtain transaction information. The transaction is scored for its risk by investigating the provenance of the relevant virtual assets establishing the time that has elapsed since any higher-risk event and the proportion of higher-risk VAs within the transaction. Blockchain analysis (also called blockchain tracing) is sometimes outsourced to an external service provider. However, outsourcing does not remove the VASP's responsibility under the AMLRs, and VASPs should ensure that they undertake due diligence on the outsourced service provider when integrating that service into their business activities. Whether to employ blockchain analysis, the degree of analysis and the use of third parties should be decided using a risk-based approach.

d. Geographical risk: Geographical risk relates both to the customer's place of establishment and the provenance of the virtual asset. Where information about the destination of funds is collected, this will also inform the assessment of geographical risk. Apart from the requirements relating to transactions and relationships involving high-risk third countries, VASPs should take into account publicly available information about the regulatory treatment and use of virtual assets in particular jurisdictions to assess geographical risk.

e. 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<sup>9</sup> being used and the manner by which a VA account is funded.

3. As part of its risk assessment, VASPs should determine whether the relevant risks, discussed above, can be appropriately mitigated and managed. In line with Regulation 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 competent authorities under the PoCA.

Risk Mitigation: AML/CFT Internal Controls

1. Pursuant to Regulation 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 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 VASP's 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 management level; controls to monitor the integrity of staff; ongoing training of staff; and an independent audit function to test the system.

2. In terms of operations, and in particular the conduct of transactions, control measures that may be employed (in addition to those outlined in Section 3E of Part II of these Guidance Notes) include: (a) Transaction limits, including limits on the total value of virtual assets that may be held, stored, transferred or exchanged; (b) Time delays before certain automated and manual transactions can be carried out with a view to restrict the rapid movement of funds, where the delay implemented will depend on the product in question and associated risk typologies; and (c) The prohibition of transfers of money to third parties (i.e., the name on source and destination accounts must match where money is exchanged for virtual assets or virtual assets for money).

3. The internal policies, controls and procedures must furthermore address the various topics detailed in Regulation 5 of the AMLRs, which include: (a) Customer due diligence (CDD) measures; (b) Related Measures for CDD such as Know Your Customer (KYC), Source of Funds etc; (c) Record keeping; (d) Implementation of targeted financial sanctions; and (e) Internal and SAR procedures.

#### E. CUSTOMER DUE DILIGENCE

1. It is important to note who is the customer for the purposes of implementing CDD as it pertains to the use of virtual assets. For virtual asset trading platforms, the customer is generally the person requesting the exchange, regardless of the means of doing so. For custodian service providers, the customer is generally the person on behalf of whom they hold or transfer a virtual asset. For issuers, the customer is generally the person who is purchasing the newly created virtual asset.

2. Pursuant to Regulations 10 to 20 of the AMLRs, VASPs must apply the full set of CDD measures, 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.

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 Regulation 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 and verify the customer's identity using reliable independent source documents, data or information. Such information would include 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 Regulation 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, 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. In cases where a VASP carries out a one-off transaction, VASPs will be expected to undertake CDD measures in respect of each one-off transaction to be conducted.

6. Pursuant to Regulations 18 and 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 SAR to the FRA.

7. As prescribed in Regulations 27 and 28 of the AMLRs, where the ML/TF risk is higher based on the existence of any of the circumstances listed in Regulation 27 of the AMLRs, EDD measures must be taken. For example, VA transfers from or associated with countries with significant levels of organised 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, enforcement and regulatory regimes may present higher risks for ML and TF. Other indicators may be risk factors associated with the VA product, service, transaction, or delivery channel, including whether the activity involves

11 pseudonymous or anonymous transactions, non-face-to-face business relationships or transactions, and/or payments received from unknown or un-associated third parties.

8. EDD measures that may mitigate the potentially higher risks associated with the factors mentioned in Regulation 27 of the AMLR include:

- a. corroborating the identity information received from the customer, such as a national identity number, with information in third-party databases or other reliable sources;
- b. tracing the customer's IP address;
- c. searching the Internet for corroborating information consistent with the customer's transaction profile;
- d. obtaining additional information on the customer and intended nature of the business relationship;
- e. obtaining information on the source of funds of the customer;
- f. obtaining information on the reasons for intended or performed transactions; and
- g. conducting enhanced monitoring of the relationship.

9. VASPs should also apply the requirements of Part VII AMLR on Politically Exposed Persons (PEPs).

**F. RELATED MEASURES FOR CDD**

**1. KYC**

- a. KYC includes identifying and verifying the customer's identity, assessing the purpose and intended nature of the business relationship or transaction and identifying and taking reasonable measures to verify the identity of beneficial owners.
- b. The information collected as part of the KYC process may include wallet addresses and transaction hashes.
- c. Where multiple VASPs are involved in one transaction, it may be helpful to develop reliance or outsourcing agreements on a bilateral basis in order to minimise duplication of KYC processes and improve the customer experience.

**2. Blockchain Analysis**

- a. Blockchain analysis processes are additional to KYC processes and take account of the unique opportunities afforded to virtual asset trading platform and virtual asset custodians by the blockchain. Blockchain analysis helps these providers to assess the risk of transactions. VASPs should consider how blockchain analysis may be appropriate to apply in line with a risk-based approach, including taking into account the nature of the business of the trading platform or virtual asset custodian and whether it would be appropriate to use it for all transactions.

12

**3. Source of Funds**

- a. 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. 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.

4. Ongoing Monitoring a. Monitoring transactions is an essential component in identifying transactions that are potentially suspicious (as discussed in Sections 3F and 16 of Part II of these Guidance Notes) 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. b. 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/PF risks associated with virtual assets, products or services or activities. c. 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 records on transactions and information obtained through CDD measures in line with Part VIII of the AMLRs, 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. 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 VASPs and third-party entities can adequately identify their 13 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 VA) of designated persons or entities and to ensure that no funds or other assets 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 Guidance Notes for more information on sanctions. 2. VASPs should be aware that some sanction lists may now include information on wallet numbers in addition to/instead of names.

I. INTERNAL AND SAR REPORTING PROCEDURES 1. VASPs should have the ability to flag for further analysis any unusual or suspicious movements of funds, value 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 their 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 Regulation 19 of the AMLRs, VASPs must promptly report suspicions of ML/TF to the FRA, including those involving or relating to VAs and/or providers that are suspicious.

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, where applicable, similar to structuring cash transactions or making multiple high-value transactions (1) in a staggered and regular pattern, with no further transactions recorded 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 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/CPF regulation. 14 (iii) Accepting/depositing 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. (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 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 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, initial coin offerings ( ICOs ), or fraudulent ICOs, etc. (vii) Customer has provided forged documents or has edited photographs and/or identification documents as part of the on-boarding process. (viii) A customer provides identification or account credentials (e.g. a non-standard IP address, or flash cookies) shared by another account. 15 (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/CPF controls.

4. In the context of virtual asset issuers and ICOs, factors that could give rise to suspicious activity are:

- a) An ICO-project does not display team members, company information nor physical address. Team members do not have a social media profile.
- b) 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.
- c) 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.
- d) There is a guarantee of high returns that seems impossible to fulfil.
- e) 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.
- f) There are no development goals on a clear timeline.
- g) The ICO intends to convert a portion of the raised funds to fiat.
- h) The virtual currency has anonymity features that aid in the commission of illegal activity, services or transactions.

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 along with the general matters identified at Part II of these Guidance Notes. For more information on red flag indicators, see FATF Report on Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (September 2020), and any subsequent related documents.

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 to restrict the actions that can be performed by its customer in relation to the suspicious funds, freeze the assets/funds (where possible) and report the suspicious activity.

7. VASPs should, where possible, implement the necessary controls to hold incoming virtual assets deemed suspicious and ensure that they are not released to their customers.

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.

16 9. When assessing a transfer of virtual assets, or any related transaction, beneficiary VASPs should consider incomplete information about the originator as a factor in determining whether a transaction is suspicious. Where the transaction has been determined to be suspicious, this must be reported to the FRA.

**J. IDENTIFICATION AND RECORD-KEEPING FOR VIRTUAL ASSET TRANSFERS**

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<sup>2</sup>, and make it available on request to appropriate authorities.
- b) Beneficiary VASPs should obtain and hold required accurate originator information and required accurate beneficiary information on virtual asset transfers and make it available on request to appropriate authorities.
- c) 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) or sending to a non-obliged entity, should obtain the required

originator/beneficiary information from their customer. 2. 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.

3. VASPs are expected to keep records of complete information on the originator and beneficiary which accompanies each transfer of virtual assets for at least five years. 4. Where technical limitations prevent an intermediary VASP from sending the required originator or beneficiary information with the transfer of virtual assets, 2 Immediately means that VASPs should submit the required information prior, simultaneously, or concurrently with the transfer itself. Securely is meant to convey that VASPs should transmit and store the required information in a secure manner. This is to protect the integrity and availability of the required information to, inter alia, facilitate record-keeping, facilitate the use of such information by the receiving VASPs or other obliged entities and protect the information from unauthorised disclosure. 17 including interoperability issues, the intermediary VASP must keep a record of all the information received from the originating VASP, obliged entity or other intermediary, for at least five years.

5. VASPs should submit the required information simultaneously or concurrently with the 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. K. TRANSFERS OF VIRTUAL ASSETS

1. 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. 2. Originating VASPs may provide the required information to beneficiary VASPs either directly, by attaching the information to the transfer, or by providing the information indirectly. 3. VASPs must ensure that transfers of virtual assets are conducted using a system which prevents the unauthorized disclosure of information. L. BATCH FILE TRANSFERS OF VIRTUAL ASSETS

1. VASPs should ensure that, for batch file transfers of virtual assets from a single originator where the transfers of virtual assets are bundled together, the batch file should contain- i. the name of the originator; ii. the account number of the originator, where an account is used to process the transfer of virtual assets by the originator; iii. the address of the originator, 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. 2. A batch file must contain the name, account number or unique identifier of the beneficiary that is traceable in the beneficiary country. M. OBLIGATIONS OF A BENEFICIARY VASP

1. Beneficiary VASPs must have procedures in place to detect whether the system they are using to effect a transfer of virtual assets is obtaining all the required information. This can be either the messaging, or payment and settlement system, or any equivalent system.

18 N. TRANSFERS OF VIRTUAL ASSETS WITH MISSING OR INCOMPLETE INFORMATION ABOUT THE ORIGINATOR 1. Originating VASPs must not execute transfers of virtual assets where they are unable to collect and maintain the required information on the originator and beneficiary. 2. Beneficiary VASPs must have

effective systems in place to detect missing required information on both the originator and beneficiary. 3. Where a beneficiary VASP detects when receiving transfers of virtual assets, that the required originator information is missing or incomplete, the beneficiary VASP must either reject the transfer of virtual assets or request complete information on the originator. 4. Where the required originator or beneficiary information is incomplete, beneficiary VASPs must have risk-based policies and procedures to determine a) whether to execute, reject or suspend a transfer of virtual assets; b) the decision-making process and the resulting actions to be taken (for example any internal escalation and/or external reporting procedures). 5. Where an originating VASP regularly fails to supply the required information on the originator, the beneficiary VASP must adopt reasonable measures to rectify the non-compliance. This includes notifying the originating VASP of the non-compliance, giving reasonable timeframes for rectification, obtaining information as to the reasons for non-compliance and documenting the actions taken. This should be done prior to rejecting any future transfers of virtual assets, restricting its business relationship or terminating its business relationship with that originating VASP. The beneficiary VASP must report to the FRA and to the Authority, its decision to restrict or terminate its business relationship with that originating VASP.

**O. REQUIREMENTS FOR INTERMEDIARY VASPS** 1. Intermediary VASPs must have documented risk-based policies and procedures to determine when to execute, reject or suspend a transfer of virtual assets that is lacking the required originator or required beneficiary information. These policies and procedures must also address that the appropriate follow-up action to be taken which should include documenting the decision-making process.

2. Intermediary VASPs that participate in a transfer of virtual assets must ensure that all information received on the originator and the beneficiary that accompany a transfer of virtual assets is kept with the transfer of virtual assets. 3. Intermediary VASPs must take reasonable measures, which are consistent with straight-through processing, to identify transfers of virtual assets that lack required originator or beneficiary information. 4. Intermediary VASPs must also adopt risk-based policies and procedures for determining when to execute, reject or suspend a transfer of virtual assets for 19 straight-through processing of transfers of virtual assets, where the required originator or beneficiary information is incomplete. The policies and procedures must also include the decision-making process and the resulting actions to be taken (for example any internal escalation and/or external reporting procedures).

**P. OBLIGATION OF A VASP TO COMPLY WITH REQUIREMENTS** 1. VASPs must comply with all relevant requirements in the countries in which they operate, either directly or through their agents.