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.

ANCHOR The AML/CFT NEWSLETTER VASP REGISTRATION/NOTIFICATION NOW OPEN Registration/notification for entities wishing to provide virtual asset services (VASPs) is now open, effective 31 October 2020, as part of a phased implementation of the Virtual Asset (Service Providers) Law, 2020 (the VASP Law) and will end on 12 December 2020. Registration or notification can be done through the VASP Application Form on the Authority s Regulatory Enhanced Electronic Forms Submission (REEFS) online platform. This registration/notification phase focuses on anti-money laundering (AML), countering the financing of terrorism (CFT) and countering proliferation financing (CPF) compliance, supervision and enforcement, and other key areas of risk. It is for: 1. Entities wishing to perform virtual asset services for the first time; 2. Entities providing virtual asset services prior to the commencement of the VASP Law; and 3. Existing Authority licensees that provide or propose to provide virtual asset services. For further guidance and FAQs on this process, please see Supervisory Information Circular. WHAT S INSIDE VASP Registration/ Notification Now Open VASPs AML/CFT Obligations Countering Proliferation Financing November 2020 2 It is the responsibility of each VASP to have systems and training in place to prevent money laundering (ML), terrorist financing (TF) and proliferation financing (PF). Internal Controls In accordance with Regulation 5 of the AMLRs, VASPs are required to implement internal polices, controls and procedures in relation to: 1. Customer due diligence (CDD) measures; 2. Risk-based approach; 3. Ongoing monitoring; 4. Record keeping; 5. Targeted financial sanctions; and 6. Internal and suspicious activity reporting. Customer Due Diligence Measures VASPs are required to: 1. Identify and verify the identity of customers and beneficial owners; 2. Understand and obtain information on the purpose and intended nature of a business relationship; and 3. Conduct ongoing monitoring. Where VASPs carry out one-off transactions, the designated threshold above which VASPs are required to conduct CDD is KYD 10,000 (see AMLRs). However international best practice suggests VASPs conduct CDD for any one-off transaction above USD/EUR 1,000 (see FATF Guidance for a Risk-Based Approach to Virtual Assets). Additionally, where higher risks are present, VASPs should: 1. Corroborate the identity information received from the customer, such as a national identity number, with information in third-party databases or other reliable sources; 2. Trace the customer s Internet Protocol (IP) address; 3. Search the Internet for corroborating information consistent with the customer s transaction profile; 4. Obtain additional information on the customer and intended nature of the business relationship; 5. Obtain information on the source of funds of the customer; 6. Obtain information on the reasons for intended or performed transactions; and 7. Conduct enhanced monitoring of the relationship. AML/CFT OBLIGATIONS FOR VASPs Furthermore, VASPs should implement additional CDD measures set out in Part VII of the AMLRs in relation to Politically Exposed Persons (PEPs). Risk Based Approach VASPs must take steps appropriate to the nature and size of the business to identify, assess, and understand its ML and TF risks. Ongoing Monitoring VASPs should determine the risk profile of its customers to determine the level of ongoing monitoring required for the business relationship. VASPs should screen customers and counterparties wallet addresses against any available blacklisted wallet addresses and monitor customer transactions to identify (1) changes to the customer s risk profile and (2) transactions that are potentially suspicious. Such monitoring should be carried out on a continuous basis or as a result of a triggering event. Record Keeping VASPs must maintain transaction records and information obtained through the CDD measures, sufficient to be able to reconstruct transactions. It is not sufficient to rely solely

on such blockchain/ledgers. Additional information and procedures will be necessary to associate wallet address to a private key controlled by a natural or legal person. Additionally, when engaging in or providing services related to transfers of virtual assets in or from within the Cayman Islands, VASPs are expected to collect and record certain information in relation to originators and beneficiaries. Targeted Financial Sanctions VASPs are required to have procedures in place to identify assets subject to targeted financial sanctions. VASPs are obligated to freeze these assets (including virtual assets) without delay and should ensure that no funds or assets are made available to or for the benefit of designated persons or entities. VASPs must comply with their obligation to report. Internal and Suspicious Activity Reporting VASPs should maintain internal reporting procedures have the appropriate systems to scrutinize transactions and determine whether the transactions are suspicious. For further guidance in relation to AML/CFT obligations for VASPs, click here. 3 COUNTERING PROLIFERATION FINANCING Fund Raising Obscure Procure & Ship Financial Service Providers (FSPs) should have in place processes to identify, assess, monitor, manage and mitigate PF risks. This may be done within the framework of existing targeted financial sanctions and/or compliance programmes. What is Proliferation and Proliferation Financing? Proliferationis the manufacture, acquisition, possession,developing,export,transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related material (including both technologies and dual-use goods used from non- legitimate purposes, such as hydrogen peroxide, which can be usedfor paper bleach and missile propellant), in contravention of national laws or, where applicable, international obligation. It includes technology, goods, software, services and expertise. Proliferation Financing (PF)is the act of providing funds or financial services which are used, in whole or in part, to make proliferation possible. Financing can include financial transfers, mortgages, credit lines, insurance services, middlemen services, trust and corporate services and company formation. Essentially, proliferation financing facilitates the movements and development of proliferation-sensitive goods. What are the stages of PF? The stages of PF differ from the placement-layering- integration cycle associated with money laundering. PF is a linear, raise- obscure- procure and ship. Stage 1: Fund Raising - proliferators raise funds from overseas criminal activities, states budgets and overseas commercial enterprises. Stage 2: Disguising Funds - proliferators transfer these funds into the international financial system. If the country is not sanctioned, this is straightforward. For states subject to comprehensive sanctions like North Korea and Iran, it is more of a challenge. During this stage proliferators rely on extensive networks of businesses and middlemen to obscure any connection on paper to sanction countries. Stage 3: Procurement - proliferators uses these funds in the international financial system to pay for goods, materials, technology, and logistics needed for its weapons of mass destruction. Financial institutions will be involved in processing the related transaction.s. Possible Indicators of PF Customer is vague and resistant to providing additional information when asked Customer s activity does not match its business profile Transaction involves designated persons (meaning a person, including any subsidiary or other entity owned or controlled by that person, to whom the Security Council of the United Nations anti-proliferation financing measures relate) Transactioninvolveshigherrisk jurisdictions which are known to be involved in proliferation or PF Transaction involves front or shell companies Products subject to export control (as per the Export of Goods, Transfer of Technology and Provision of Technical

Assistance(Control)(Overseas Territories) Order 2004) Shipment of goods takes a circuitous route or the financial transaction is structured in a circuitous manner Inconsistencies in the information provided in trade documents and financial flows What are the steps to detect PF? FSPs should carry out appropriate customer due diligence on their clients, which includes screening names of clients and clients counterparties, including shipping companies, beneficiaries of letters of credit and freight companies, against sanctions lists. FSPs should take note of PF red flags and implement risk-based systems and controls (including policies and procedures, ongoing monitoring, and training) to detect PF. FSPs should carry out a risk assessment to determine their exposure to PF risk. The risk assessment should consider risks relating to geography, customers and products and services. For further guidance in relation to CPF, click here.