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 TARGETED FINANCIAL SANCTIONS WHAT S INSIDE National Risk Assessment Sectoral Risk Ratings VASPs and the Travel Rule May 2022 It is more critical than ever that regulated entities have appropriate policies and procedures in place to adequately manage risks around targeted financial sanctions (TFS). This includes provisions for the prompt freezing of assets, non-dealing in funds and timely disclosures to the Financial Reporting Agency, where required. Caymans Islands legal persons and arrangements are susceptible to misuse and abuse by those seeking to evade TFS. There are also specific vulnerabilities for virtual asset service providers (VASPs) as designated persons may seek to circumvent the traditional financial sector through use of virtual assets. Regulated entities must ensure that their sanctions compliance programmes remain fit-for-purpose and contain mechanisms that allow them to quickly respond to the complex, far-reaching and swift changes to TFS regimes. Details of all internal investigations undertaken with respect to suspected TFS breaches or evasion should be formally documented and safely secured should an external TFS investigation be commenced. For further information, regulated entities may refer to guidance previously issued by the Cayman Monetary Regulatory Authority International (CMRAI) and the Financial Reporting Authority in relation to compliance with TFS, including the recent Notice Targeted Financial Sanctions Russia and Belarus. 2 Understanding risk is the cornerstone to an effective national AML/CFT/CPF regime. All countries, including the Cayman Islands, must identify, assess and understand money laundering (ML), terrorist financing (TF), proliferation financing (PF) and (TFS) risks, and apply measures that correspond to the identified level of risk. This risk-based approach (RBA) enables jurisdictions to prioritise their resources and allocate them efficiently. The Cayman Islands has just published a new national risk assessment(NRA 2021) updating the NRA 2015. It was undertaken by 15 working groups comprising representatives from various government authorities and supervisory bodies, as well as private sector stakeholders under the stewardship of the Anti-Money Laundering Steering Group (AMLSG) and the National Coordination Team. The NRA 2021 covers: National threats National vulnerabilities Banking Securities Investments Insurance Trust and Company Service Providers (TCSPs) Real Estate & DPMS Lawyers Accountants Non-profit organisations Virtual assets Legal Persons and Legal Arrangements Proliferation financing Other entities and institutions NATIONAL RISK ASSESSMENT Sector Overall Inherent Risk Mutual Funds Administration Medium High SecuritiesMedium High TCSPsMedium High BanksMedium High VASPsMedium High InsuranceMedium Low High Value DealersMedium Low Dealers of Precious Metals and Stones Medium Low Financial LeasingMedium Low Accountants (Inc. Auditors) Medium Low MSBsMedium High Real EstateMedium High LawyersMedium High Sectoral Risk Ratings Each sector was assigned an overall inherent risk rating through an assessment of the relevant nature, size and complexity, customers, products, services, transactions, delivery channels and geographic risks: 3 Key Findings from the NRA The primary threat facing the Cayman Islands is from ML, as compared to TF and PF. The jurisdiction has a greater exposure to proceeds-generating crimes committed overseas. Given the country s status as an international financial centre, the most prevalent of these foreign proceeds of crime are fraud, corruption, and tax evasion. The most material financial sectors are Securities, Banking and TCSPs. Most supervised FIs, DNFBPs, and VASPs were found to have medium-high sectoral risks. Mitigating measures were generally good, but only satisfactory for VASPs, as they were just recently brought under the country s AML/CFT/CFP framework and subject to supervision. Legal persons and

arrangements were assessed as high risk, and areas of high inherent risk included exempt companies, exempted limited partnerships, and trusts. Emerging risks include cybercrime, fraud and ransomware attacks utilising virtual assets. The 2022-2025 AML/CFT/CFP Strategy Planhas been published to focus on key areas to strengthen the jurisdiction s AML/CFT/CFP regime over the next three years. CMRAI is committed to completing all the actions for which it is responsible, and progress will be regularly monitored and assessed by the AMLSG. VASPs and the Travel Rule The Travel Rule comes into force in the Cayman Islands on 1 July 2022. VASPs will need to consider how they will comply. See Part XA of the Anti-Money Laundering Regulations. What is the Travel Rule? The Financial Action Task Force (FATF) requires both sending and receiving VASPs to obtain, exchange and store originator and beneficiary identification information, in addition to the cryptocurrency addresses and transaction ID, for each transaction. Law enforcement and regulators require the latter since cryptocurrency addresses can be used by multiple beneficiary customers. FATF Interpretative Note to Recommendation 16, paragraph 6, prescribes the following to be collected by the originating VASP, shared with the beneficiary VASP or FI and retained for sharing with appropriate authorities if required: a. Name of the originator b. Originator account number where such an account is used to process the transaction c. Originator s physical (geographical) address, or national identity number, or customer identification number, or date and place of birth d. Name of the beneficiary e. Beneficiary account number where such an account is used to process the transaction The intended purpose of the Travel Rule is to share information which will allow VASPs and other financial institutions to block terrorist financing, prevent ML of virtual assets, stop payments to sanctioned individuals, entities, and countries, as well as support reporting of suspicious activities. 4 Travel Rule: Policies & Procedures VASPS are encouraged to have robust Travel Rule policies and procedures in place to ensure a consistent and adequate approach to obtaining, exchanging and storing the appropriate information. These may include (but are not limited to) procedures for the ongoing monitoring of incoming transactions without full Travel Rule information, a description of the risk indicators that would prompt cancellation of an outgoing or incoming transaction, timelines for restricting funds without complete Travel Rule information, policies to keep records secure, and procedures for the sanction screening of counter parties. VASPs may also set out the criteria by which they have selected any Travel Rule IT solution. There are various automated products which can help identify whether transactions meet/exceed designated thresholds, confirm whether a VASP is transacting with a legitimate receiving VASP and facilitate safe and secure transfer of personal identifiable information (PII) between VASPs. However, sharing sensitive financial transaction and client PII information with unknown VASPs should be managed carefully. It can increase the risk of hacks, PII data leaks, and fake VASPs masquerading as legitimate VASPs to collect PII and sell user PII data. Challenges to Compliance The sunrise issue is a key strategic and operational risk faced by VASPs when executing the Travel Rule. This refers to the staggered implementation of the Travel Rule across different jurisdictions, resulting in varied levels of enforcement. Currently, the United States of America, Singapore and Switzerland are the only jurisdictions in the world to have fully implemented the Travel Rule requirement. This poses a challenge because compliance with the Travel Rule is predicated on all VASPs in a transaction being able to obtain and share PII. It is therefore important for VASPs to conduct due diligence on counterparty VASPs to identify whether the entity is a legitimate VASP, and licensed and regulated in a jurisdiction with a robust VASP regulatory framework. Next Steps VASPs registered, or in the process of registering,

are required to provide information to CMRAI on how they will comply with the Travel Rule , and should have submitted details of their compliance arrangements, policies and procedures, and use of resources by 31 March 2022. Read the full notice here.