Monetary Authority of Singapore

GUIDELINES TO MAS NOTICE VCC-N01 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

4 DECEMBER 2020

TABLE OF CONTENTS

For ease of reference, the chapter numbers in these Guidelines mirror the corresponding paragraph numbers in the Notice MAS Notice VCC-N01 on Prevention of Money Laundering and Countering the Financing of Terrorism – Variable Capital Companies (e.g. Chapter 2 of the Guidelines provides guidance in relation to paragraph 2 of the Notice). Not every paragraph in the Notice has a corresponding paragraph in these Guidelines and this explains why not all chapter numbers are utilised in these Guidelines.

GUIDELINES TO MAS NOTICE VCC-N01 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

1 Introduction

1-1 These Guidelines provide guidance to all variable capital companies ("VCCs") incorporated under the Variable Capital Companies Act (Act 44 of 2018) ("VCC Act") on some of the requirements in MAS Notice VCC-N01 on Prevention of Money Laundering and Countering the Financing Of Terrorism – Variable Capital Companies ("the Notice"). These Guidelines should be read in conjunction with the Notice.

1-2 The expressions used in these Guidelines have the same meanings as those found in the Notice, except where expressly defined in these Guidelines or where the context otherwise requires. For the purposes of these Guidelines, a reference to "CDD measures" shall mean the measures as required by paragraphs 7, 8 and 9 of the Notice.

1-3 The degree of observance with these Guidelines by a VCC may have an impact on the Authority's overall ML/TF risk assessment of the VCC, including the quality of its board and senior management oversight, governance, internal controls and risk management.

1-4 Structure of a VCC and its Relationship with its eligible financial institution ("EFI")

1-4-1 Given its specific and limited purpose, a VCC might not have its own employees or officers who can perform the VCC's AML/CFT obligations. To prevent the abuse of a VCC for unlawful purposes, the VCC is required under paragraph 4 of the Notice to engage an EFI for the purposes of conducting the necessary checks and performing the measures in order for the VCC to comply with its obligations under the Notice except for those in paragraphs 3, 4 and 10.

1-4-2 Notwithstanding that the EFI will be the entity conducting checks and performing the measures set out in the Notice, a VCC remains responsible for its AML/CFT obligations under the Notice. This includes ensuring that appropriate policies and procedures have been put in place for adequate oversight of the checks and measures the EFI will perform on the VCC's behalf. The VCC may choose to adapt the policies and procedures of its EFI, with appropriate modifications to suit the VCC's context. When determining the policies and procedures, a VCC should incorporate the guiding principles set out in the corresponding paragraphs (i.e. paragraphs 5 to 9, and paragraphs 13 and 14 of these Guidelines).

1-4-3 In the Notice and these Guidelines:

(a) a reference to a VCC's board refers to the VCC's director(s);

(b) a reference to senior management of a VCC refers to any person the board may appoint as the VCC's senior management. Examples of persons who could be appointed to this role are:

(i) VCC's directors;

(ii) employees or officers of the VCC, if any; and

(iii) employees or officers of the VCC's EFI.

(c) a reference to employees includes employees of the EFI appointed by the VCC's board to perform the relevant checks and measures on behalf of the VCC;

(d) a reference to the AML/CFT compliance officer refers to any person the board has appointed to carry out the relevant AML/CFT function for the VCC. Examples of persons who could be appointed to this role are:

(i) VCC's directors;

(ii) employees or officers of the VCC, if any; and

(iii) employees or officers of the VCC's EFI.

1-5 Key Concepts

Money Laundering

1-5-1 Money laundering ("ML") is a process intended to mask the benefits derived from criminal conduct so that they appear to have originated from a legitimate source. Singapore's primary legislation to combat ML is the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A). A VCC should refer to the website of the Singapore Police Force's Commercial Affairs Department for more information.

1-5-2 Generally, the process of ML comprises three stages, namely —

(a) Placement – The physical or financial disposal of the benefits derived from criminal conduct.

(b) Layering – The separation of these benefits from their original source by creating layers of financial transactions designed to disguise the ultimate source and transfer of these benefits.

(c) Integration – The provision of apparent legitimacy to the benefits derived from criminal conduct. If the layering process succeeds, the integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate funds.

1-5-3 As VCC transactions are unlikely to be cash based, they are more likely to be used in the layering stage rather than placement stage of money laundering. However, where the transactions are in cash, there is still the risk of VCC transactions being used at the placement stage.

1-5-4 VCC transactions offer a vast array of opportunities for transforming money into a diverse range of assets. The ease with which these assets can be converted to other types of assets, especially if they are liquid and marketable, also aids the layering process. Hence, VCC transactions could be attractive to money-launderers for layering their illicit proceeds for eventual integration into the general economy.

Terrorism Financing

1-5-5 Acts of terrorism seek to influence or compel governments into a particular course of action or to intimidate the public or a section of the public. VCCs are reminded of the broad definitions of "terrorist" and "terrorist acts" set out in the Terrorism (Suppression of Financing) Act (Cap. 325) ("TSOFA").

1-5-6 Terrorists require funds to carry out acts of terrorism and support their nefarious activities. Terrorism financing ("TF") is the act of providing these funds.

1-5-7 The funds or assets may be raised or obtained from criminal activities such as robbery, drug-trafficking, kidnapping, extortion, fraud or hacking of online accounts. They can also be moved through various means, before being converted and put to use for illicit purposes. In cases where they are raised or obtained from criminal activities, there may also be an element of ML involved to disguise the source of funds or to move them.

1-5-8 However, funding for terrorist acts and organisations may also be raised from legitimate sources such as donations from charities, legitimate business operations, self-funding by individuals, etc. Coupled with the fact that TF need not always involve large sums of money, TF can be hard to detect and VCCs should remain vigilant.

1-5-9 Singapore's primary legislation to combat TF is the TSOFA. VCCs may refer to the Inter-Ministry Committee on Terrorist Designation's website for more information.

The Three Lines of Defence

1-5-10 A VCC should take note of the concept of the "three lines of defence" for AML/CFT in relation to the performance of roles and responsibilities by its fund manager and EFI. The VCC should ensure that its fund manager and EFI have an appropriate segregation of roles and responsibilities with regard to (i) dealing with the VCC's customers; (ii) performing checks and measures in accordance with the VCC's AML/CFT policies and procedures; and (iii) conducting internal audits. A VCC should also ensure that:

(a) relevant employees and officers, including the AML/CFT compliance officer, facilitating the VCC's compliance with AML/CFT requirements are adequately trained in and aware of their obligations;

(b) its senior management or board of directors is alerted to potential ML/TF risks and concerns;

(c) there are periodic evaluations of the effectiveness of the execution of the VCC's ML/TF risk management framework and controls, the results of which are reported to the VCC's board of directors.

Governance

1-5-11 Strong board and senior management leadership is indispensable in the oversight of the development and implementation of a sound AML/CFT risk management framework across the VCC. The VCC's board of directors and senior management should ensure that the VCC's AML/CFT processes are robust and properly executed by the EFI, and there are adequate risk mitigating measures in place. The successful implementation and effective operation of a risk-based approach to AML/CFT thus depends on the VCC ensuring that the EFI has a good understanding of the ML/TF risks inherent in the VCC's business.

1-5-12 A VCC's board of directors and senior management should similarly understand the ML/TF risks the VCC is exposed to and how the VCC's AML/CFT control framework operates to mitigate those risks. This should involve the board of directors and senior management —

(a) receiving sufficient, timely and objective information to form an accurate picture of the ML/TF risks including emerging or new ML/TF risks, which the VCC is exposed to through its activities and business relations;

(b) receiving sufficient and objective information to assess whether the VCC's AML/CFT controls are adequate and effective;

(c) receiving information on legal and regulatory developments and the impact these have on the VCC's AML/CFT framework; and

(d) ensuring that processes are in place to escalate important decisions that directly impact the ability of the VCC to address and control ML/TF risks, especially where AML/CFT controls are assessed to be inadequate or ineffective.

2 Notice Paragraph 2 – Definitions, Clarifications and Examples

Connected Party

2-1 The term "partnership" as it appears in the definition of "connected party" includes foreign partnerships. The term "manager" as it appears in limb (b) of the definition of "connected party" takes reference from section 2(1) of the Limited Liability Partnership Act (Cap. 163A) and section 28 of the Limited Partnership Act (Cap. 163B).

2-2 Examples of natural persons with executive authority in a company include the Chairman and Chief Executive Officer. An example of a natural person with executive authority in a partnership is the Managing Partner.

Customer

2-3 When performing Customer Due Diligence ("CDD") measures in the scenarios below, the following approaches may be adopted:

(a) Engagement of Distributors

A distributor may have been engaged to market a VCC's fund(s), and may use omnibus accounts in its own name to transact in or subscribe to units or shares in the VCC on behalf of its clients, who are the underlying investors of the VCC. Under this arrangement, the VCC's customer would be the distributor. However, the relevant CDD measures to be performed on beneficial owners should be focused on the underlying investors who have engaged the distributors' service to invest into the VCC, i.e. persons on whose behalf the distributor establishes business relations with the VCC.

The VCC may not have visibility of the underlying investors, and for legitimate business reasons, the distributor may also not be prepared to reveal the identity of the underlying investors. In such circumstances, where the distributor meets one or more of the criteria in paragraph 7.15 of the Notice (e.g. a financial institution subject to and supervised by MAS for compliance with AML/CFT requirements consistent with the standards set by the FATF), the VCC shall not be required to inquire about the existence of the beneficial owners, subject to the conditions in the said paragraph. Otherwise, the VCC will not be able to rely on the distributor to perform CDD on its behalf, and would be required to perform appropriate CDD measures on the underlying investors. Alternatively, it may also perform Simplified Due Diligence (SCDD) measures on these investors, subject to the conditions in paragraph 8 of the Notice. The VCC may also consider whether the SCDD measures are applicable in relation to the distributors.

It may also be possible for a distributor to act as an introducer to the VCC, with the investors investing directly in the VCC, instead of through the distributor. In such cases, where the distributor acts purely as an introducer, the investors, and not the distributor, would be the VCC's customers, and CDD would have to be performed on them. However, if these investors are also customers of the distributor, subject to the requirements in paragraph 10 of the Notice, the

distributor may be relied on to perform the measures as required by paragraphs 7, 8 and 9.

(b) Existing members of re-domiciled VCCs

Where a foreign corporate entity transfers its registration and is re-domiciled in Singapore as a VCC, persons that were members of the foreign corporate entity at the time of transfer of registration would need to be registered in the register of members under section 17 of the VCC Act and thus would fall within the definition of "customers" under the Notice, and the necessary CDD measures have to be performed on these persons.

The VCC may however rely on the measures already performed on these customers prior to the VCC's transfer of registration to Singapore, provided that the VCC is satisfied that these earlier measures meet the Notice requirements, and relevant laws in Singapore.

Where the VCC has any reasonable grounds to suspect that the assets or funds of a customer are proceeds of drug dealing or criminal conduct as defined in the CDSA, or are property related to the facilitation or carrying out of any terrorism financing offence as defined in the TSOFA, the VCC should ensure that the EFI files a Suspicious Transaction Report ("STR") on its behalf. The VCC should also ensure that the EFI takes the appropriate risk mitigation measures, including putting in place additional control measures (e.g. performing enhanced customer due diligence measures) or the VCC should terminate its business relationship with the customer.

Legal Arrangements

2-4 In relation to the definition of "legal arrangement" in the Notice, examples of legal arrangements are trust, fiducie, treuhand and fideicomiso.

Legal Persons

2-5 In relation to the definition of "legal person" in the Notice, examples of legal persons are companies, bodies corporate, foundations, anstalt, partnerships, joint ventures or associations.

4 Notice Paragraph 4 – Eligible Financial Institution

4-1 The VCC should engage a single EFI for the purposes of paragraph 4 of the Notice. There should be a formal documentation of the engagement of the EFI, for instance through a legally-binding contract. *Inter alia*, this documentation should include the policies and procedures which the EFI is expected to perform on the VCC's behalf, as well as the identity of any of the EFI's employees and officers appointed to fulfil senior management and key AML/CFT roles for the VCC as set out under paragraphs 13.1(a) and 14.9 of the Notice.

4-2 For the avoidance of doubt, the EFI is not prohibited from outsourcing the performance of the checks and measures necessary for compliance with the VCC's AML/CFT requirements to other parties on behalf of the VCC. Nonetheless, as the VCC remains ultimately responsible for its compliance with its AML/CFT obligations under the Notice, the VCC's board of directors should have oversight of its EFI's outsourcing arrangements.

5 Notice Paragraph 5 – Assessing Risks and Applying a Risk-Based Approach

Countries or Jurisdictions of its Customers

5-1 In relation to a customer who is a natural person, this refers to the nationality and place of domicile, business or work. For a customer who is a legal person or arrangement, this refers to:

(a) the country or jurisdiction of establishment, incorporation, or registration; and

(b) the country or jurisdiction of operations, if different from the country or jurisdiction of establishment, incorporation or registration.

Other Relevant Authorities in Singapore

5-2 Examples include law enforcement authorities (e.g. Singapore Police Force, Commercial Affairs Department, Corrupt Practices Investigation Bureau) and other government authorities (e.g. Attorney General's Chambers, Ministry of Home Affairs, Ministry of Finance, Ministry of Law).

Risk Assessment

5-3 A VCC should have a holistic ML/TF risk assessment that is approved by its board of directors or senior management and periodically updated. This is intended to facilitate a better understanding of the VCC's overall vulnerability to ML/TF risks and forms the basis for the VCC's overall risk-based approach.

5-4 The risk assessment shall include a consolidated assessment of the VCC's ML/TF risks that exist across all its sub-funds (if any), product lines and delivery channels. For the purposes of the risk assessment, the ML/TF risks of a VCC's branches and subsidiaries, including those outside Singapore, shall be taken into account.

5-5 The broad ML/TF risk factors that should be considered include —

(a) in relation to the VCC's customers —

(i) target customer markets and segments;

(ii) profile and number of customers identified as higher risk;

(iii) volumes and sizes of its customers' transactions and funds transfers, considering the usual activities and the risk profiles of its customers;

(b) in relation to the countries or jurisdictions its customers are from or in, or where the VCC has investments in —

(i) countries or jurisdictions the VCC is exposed to, either through its own activities (including where its branches and subsidiaries operate in) or the activities of its customers, especially countries or jurisdictions with relatively higher levels of corruption, organised crime or inadequate AML/CFT measures, as identified by the FATF;

(ii) when assessing ML/TF risks of countries and jurisdictions, the following criteria may be considered:

- reliable evidence of adverse news or relevant public criticism of a country or jurisdiction, including FATF public documents on High Risk and Other Monitored jurisdictions;

- independent and public assessment of the country's or jurisdiction's overall AML/CFT regime such as FATF or FATF-Styled Regional Bodies' ("FSRBs") Mutual Evaluation reports and the IMF / World Bank Financial Sector Assessment Programme Reports or Reports on the Observance of Standards and Codes for guidance on the country's or jurisdiction's AML/CFT measures;

- the AML/CFT laws, regulations and standards of the country or jurisdiction;

- implementation standards (including quality and effectiveness of supervision) of the AML/CFT regime;

- whether the country or jurisdiction is a member of international groups that only admit countries or jurisdictions which meet certain AML/CFT benchmarks;

- contextual factors, such as political stability, maturity and sophistication of the regulatory and supervisory regime, level of corruption, financial inclusion etc;

(c) in relation to the products, services, transactions and delivery channels of the VCC —

(i) the nature, scale, diversity and complexity of the VCC's business activities;

(ii) the nature of products and services offered by the VCC; and

(iii) the extent to which the VCC deals directly with the customer, relies on third parties to perform CDD measures, or uses technology.

5-6 The scale and scope of the risk assessment should be commensurate with the nature and complexity of the VCC's business.

Singapore's National ML/TF Risk Assessment ("NRA") Report

5-7 The results of Singapore's NRA Report or relevant risk information from the authorities should be incorporated into a VCC's ML/TF risk assessment process. Any financial or non-financial sector that has been identified as presenting higher ML/TF risks should also be taken into account, when performing the holistic ML/TF risk assessment. When assessing the ML/TF risks presented by customers, the NRA results and risk assessment results should also be considered.

5-8 The NRA also identifies certain prevailing crime types as presenting higher ML/TF risks. These results should be considered when assessing the ML/TF risks of its products, services, transactions and delivery channels and whether it is more susceptible to the higher risk prevailing crime types. Where appropriate, the NRA results should also be taken into account as part of the ongoing monitoring of the conduct of VCC's customers and the scrutiny of customers' transactions.

Risk Mitigation

5-9 The nature and extent of AML/CFT risk management systems and controls implemented should be commensurate with the ML/TF risks identified via the risk assessment. There should be adequate policies, procedures and controls to mitigate the ML/TF risks.

5-10 The effectiveness of the implementation of the VCC's risk mitigation procedures and controls should be assessed, by monitoring the following:

(a) the ability to identify changes in a customer profile (e.g. Politically Exposed Persons status) and transactional behaviour observed in the course of its business;

(b) the potential for abuse of new business initiatives, products, practices and services for ML/TF purposes;

(c) the compliance arrangements (through its internal audit or quality assurance processes or external review);

(d) the balance between the use of technology-based or automated solutions with that of manual or people-based processes, for AML/CFT risk management purposes;

(e) the coordination between AML/CFT compliance and other functions of the EFI or manager;

(f) the adequacy of training provided to the relevant employees and officers conducting the necessary checks and performing the VCC's AML/CFT measures in order for the VCC to comply with the Notice, and awareness of these employees and officers on AML/CFT matters relating to the VCC;

(g) the process of management reporting and escalation of pertinent AML/CFT issues to the single reference point for suspicious transactions reporting within the VCC or to the AML/CFT compliance officer;

(h) the coordination between the VCC and regulatory or law enforcement agencies; and

(i) the performance of third parties relied upon by the EFI to carry out CDD measures.

Documentation

5-11 The documentation to be compiled by the EFI should include —

(a) the holistic ML/TF risk assessment of the VCC;

(b) details of the implementation of the AML/CFT risk management systems and controls as guided by the ML/TF risk assessment;

(c) the reports to the VCC's board of directors or senior management on the results of the ML/TF risk assessment and the implementation of the AML/CFT risk management systems and controls; and

(d) details of the frequency of review of the VCC's ML/TF risk assessment.

5-12 A VCC should ensure that its ML/TF risk assessment is made available to the Authority upon request.

Frequency of Review

5-13 A VCC's risk assessment should be reviewed at least once every two years or when material trigger events occur, whichever is earlier, so as to keep its ML/TF risk assessment up-to-date. Such material trigger events include, but are not limited to, the acquisition of new customer segments or delivery channels, or the launch of new products and services by the VCC. The results of these reviews should be documented and approved by the board of directors or senior management even if there are no significant changes to the VCC's risk assessment.

6 Notice Paragraph 6 – New Products, Practices and Technologies

6-1 International developments of new technologies and payment methods in the provision of financial services are fast-changing and growing at an accelerated pace. A VCC should keep abreast of such new developments and the ML/TF risks associated with them.

6-2 An assessment of the VCC's ML/TF risks in relation to new products, practices and technologies is separate from, and in addition to, the assessment of other risks such as credit risks, operational risks or market risks. For example, in the assessment of ML/TF risks, attention should be given to new products, practices and technologies that deal with customer funds or the movement of such funds. These assessments should be approved by senior management or the VCC's board of directors.

6-3 An example of a "delivery mechanism" as set out in paragraph 6 of the Notice is mobile trading.

7 Notice Paragraph 7 – Customer Due Diligence

Notice Paragraph 7.2

7-1 Where There Are Reasonable Grounds for Suspicion prior to the Establishment of Business Relations

7-1-1 In arriving at its decision for each case, the relevant facts of the case, including information that may be made available by the authorities, should be taken into account, and a proper risk assessment conducted.

Notice Paragraphs 7.4 to 7.16

7-2 CDD Measures under Paragraphs 7.4 to 7.16

7-2-1 When relying on documents, a VCC and EFI should be aware that the best documents to verify the identity of the VCC's customer are those most difficult to obtain illicitly or to counterfeit. These may include government-issued identity cards or passports, checks against independent or official public company registries, published or audited annual reports and other reliable sources of information. The rigour of the verification process should be commensurate with the customer's risk profile.

7-2-2 A VCC should ensure that its EFI exercises greater caution when dealing with an unfamiliar or new customer on behalf of the VCC for the purposes of conducting the necessary checks and performing AML/CFT measures in relation to the VCC. Apart from obtaining the identification information required by paragraph 7.5 of the Notice, the VCC should ensure that the EFI, for the purposes of conducting the necessary checks and performing AML/CFT measures in relation to the VCC, also obtain additional information on the customer's background such as occupation, employer's name, nature of business, range of annual income and whether the customer holds or has held a prominent public function. Such additional identification information would provide a better knowledge of this customer's risk profile, as well as the purpose and intended nature of the business relations.

Notice Paragraph 7.5

7-3 Identification of Customer

7-3-1 With respect to paragraph 7.5(c) of the Notice, a P.O. box address should only be used for jurisdictions where the residential address (e.g. street name or house number) is not applicable or available in the local context.

7-3-2 The VCC should ensure that the EFI obtains the contact details of the VCC's customer, such as personal, office or work telephone numbers.

Notice Paragraph 7.7

7-4 Identification of Customer that is a Legal Person or Legal Arrangement

7-4-1 Paragraph 7 and paragraph 9 of the Notice require all connected parties of a customer of a VCC to be identified and screened. However, their identities may be verified using a risk-based approach[1].

7-4-2 Identification of connected parties may be done using publicly available sources or databases such as company registries, annual reports or based on substantiated information provided by the customers.

7-4-3 In relation to legal arrangements, CDD measures shall be performed on the customer by identifying the settlors, trustees, the protector (if any), the beneficiaries (including every beneficiary that falls within a designated characteristic or class) and any natural person exercising ultimate ownership, ultimate control or ultimate effective control over the trust (including through a chain of control or ownership), as required by paragraph 7.13 of the Notice.

Notice Paragraph 7.8

7-5 Verification of Identity of Customer

7-5-1 Where the customer is a natural person, a VCC should ensure that its EFI obtains identification documents that contain a clear photograph of that customer. EFIs that have been given access to a VCC's customer's personal data through the government's MyInfo platform are not required to obtain additional documents, including identification documents that contain a clear photograph of the customer, to verify his/her identity.

7-5-2 In verifying the identity of a customer, an EFI may obtain the following documents:

(a) Natural Persons —

(i) name, unique identification number, date of birth and nationality based on a valid passport or a national identity card that bears a photograph of the customer; and

(ii) residential address based on national identity card, recent utility or telephone bill, bank statement or correspondence from a government agency;

(b) Legal Persons or Legal Arrangements —

(i) name, legal form, proof of existence and constitution based on certificate of incorporation, certificate of good standing, partnership agreement, trust

[1] For the guidance on SCDD measures in relation to the identification and verification of the identities of connected parties of a customer, VCCs are to refer to paragraph 8-3 of these Guidelines.

deed, constitutional document, certificate of registration or any other documentation from a reliable independent source; and

(ii) powers that regulate and bind the legal person or arrangement based on memorandum and articles of association, and board resolution authorising the establishment of business relations and appointment of authorised signatories.

7-5-3 Further guidance on verification of different types of customers (including legal persons or legal arrangements) is set out in Appendix A.

7-5-4 In exceptional circumstances where a copy of the documentation used to verify the customer's identity cannot be retained, the EFI should record the following information:

(a) information that the original documentation had served to verify;

(b) title and description of the original documentation produced to the relevant EFI employee or officer for verification, including any particular or unique features or condition of that documentation (e.g. whether it is worn out, or damaged);

(c) reasons why a copy of that documentation could not be made; and

(d) name of the relevant EFI employee or officer who carried out the verification, a statement by that employee or officer certifying verification of the information against the documentation and the date of the verification.

Reliability of Information and Documentation

7-5-5 Where a customer or a third party provides data, documents or information, the VCC should ensure that the EFI checks that such data, documents or information is current at the time they are provided.

7-5-6 Where the customer is unable to produce an original document, a VCC may allow its EFI to accept a copy of the document —

(a) that is certified to be a true copy by a suitably qualified person (e.g. a notary public, a lawyer or certified public or professional accountant); or

(b) a staff member of the VCC or EFI independent of the customer relationship has confirmed that he has sighted the original document.

7-5-7 Where a document is in a foreign language, the VCC should ensure that the EFI takes appropriate steps to be reasonably satisfied that the document does, in fact, provide evidence of the customer's identity, and that any document that is critical for performance of any measures required under the Notice is translated into English by a suitably qualified translator. Alternatively, the EFI may rely on a

translation of such document by a staff of the VCC or EFI who is independent of the customer relationship, and who is conversant in that foreign language.

7-5-8 A VCC should ensure that the EFI checks that documents obtained for performing any measures required under the Notice are clear and legible. This is important for the establishment of a customer's identity, particularly in situations where business relations are established without face-to-face contact.

Notice Paragraphs 7.9 to 7.11

7-6 Identification and Verification of Identity of Natural Person Appointed to Act on a Customer's Behalf

7-6-1 Appropriate documentary evidence of a customer's appointment of a natural person to act on its behalf includes a board resolution or similar authorisation documents.

7-6-2 Where there is a long list of natural persons appointed to act on behalf of the customer (e.g. a list comprising more than 10 authorised signatories), at least those natural persons who will deal directly with the VCC, its manager, or its EFI should be verified.

Notice Paragraphs 7.12 to 7.16

7-7 Identification and Verification of Identity of Beneficial Owner

7-7-1 A VCC should note that measures listed under paragraph 7.13(a)(i), (ii) and (iii) as well as paragraph 7.13(b)(i) and (ii) of the Notice are not alternative measures but cascading measures with each to be used where the immediately preceding measure has been applied but has not resulted in the identification of a beneficial owner.

7-7-2 In relation to paragraph 7.13(a)(i) and (b)(i) of the Notice, when identifying the natural person who ultimately owns the legal person or legal arrangement, the shareholdings within the ownership structure of the legal person or legal arrangement should be considered. It may be based on a threshold (e.g. any person owning more than 25% of the legal person or legal arrangement, taking into account any aggregated ownership for companies with cross-shareholdings).

7-7-3 A natural person who does not meet the shareholding threshold referred to in paragraph 7-7-2 above but who controls the customer (e.g. through exercising significant influence), is a beneficial owner under the Notice.

7-7-4 A VCC may consider requiring its EFI to obtain an undertaking or declaration from the customer on the identity of, and the information relating to, the beneficial owner. Notwithstanding the obtaining of such an undertaking or declaration, the VCC remains responsible for complying with its obligations under the Notice to ensure

that reasonable measures have been taken to verify the identity of the beneficial owner by, for example, researching publicly available information on the beneficial owner or arranging a face-to-face meeting with the beneficial owner, to corroborate the undertaking or declaration provided by the customer.

7-7-5 Where the customer is not a natural person and has a complex ownership or control structure, enough information should be obtained to sufficiently understand if there are legitimate reasons for such ownership or control structure.

7-7-6 Particular care should be taken when dealing with companies with bearer shares, since the beneficial ownership is difficult to establish. For such companies, the VCC should have procedures to establish the identities of the beneficial owners of such shares and ensure that the VCC is notified whenever there is a change of beneficial owner of such shares. At a minimum, these procedures should ensure that the EFI obtains an undertaking in writing from the beneficial owner of such bearer shares stating that the VCC shall be immediately notified if the shares are transferred to another natural person, legal person or legal arrangement. Depending on its risk assessment of the customer, the VCC may require that the bearer shares be held by a named custodian, with an undertaking from the custodian that the VCC will be notified of any changes to ownership of these shares or the named custodian.

7-7-7 For the purposes of paragraph 7.15 of the Notice, where the customer is a legal person publicly listed on a stock exchange and subject to regulatory disclosure requirements relating to adequate transparency in respect of its beneficial owners (imposed through stock exchange rules, law or other enforceable means), it is not necessary to identify and verify the identities of the beneficial owners of the customer.

7-7-8 A VCC should ensure its EFI has a process with clear criteria to assess if a foreign stock exchange imposes regulatory disclosure and adequate transparency requirements, taking into account, amongst others, the country risk and the level of the country's compliance with the FATF standards.

7-7-9 Where a customer is a majority-owned subsidiary of a publicly listed legal person, it is not necessary to identify and verify the identities of the beneficial owners of the customer. However, for such a customer, if there are other non-publicly listed legal persons who own more than 25% of the customer or who otherwise control the customer, the beneficial owners of such non-publicly listed legal persons should be identified and verified.

7-7-10 Where a customer is one which falls within paragraph 7.15 of the Notice, this does not in itself constitute an adequate analysis of low ML/TF risks for the purpose of performing SCDD measures under paragraph 8 of the Notice.

Notice Paragraphs 7.17 to 7.24

7-8 Maintenance of Register of Beneficial Owners of the VCC and Register of Nominee Directors

7-8-1 A member of the VCC is a VCC's customer, as defined in the Notice. Accordingly, the beneficial owners of a VCC's members are also the beneficial owners of its customers. In relation to paragraphs 7.17 of the Notice, the register of beneficial owners of a VCC should be kept updated when the VCC's customers' CDD data, documents or information indicate a change in its customers' beneficial owners. Such changes could be observed as part of the ongoing monitoring process, including through transaction monitoring and subjecting customers to periodic review, or from information obtained from other reliable information sources, such as independent or official public company registries, published, or audited annual reports.

7-8-2 In relation to paragraph 7.21 of the Notice, a VCC's register of nominee directors should be kept accurate and up to date. For instance, this could include measures requiring new directors to notify the VCC if they are acting as nominees and requiring existing directors to similarly notify the VCC if they subsequently become nominees.

7-8-3 In relation to paragraphs 7.17 and 7.21 of the Notice, the details of the VCC's beneficial owners and nominee directors in the respective registers should be updated no later than 2 business days after the information has been provided to the VCC.

Notice Paragraph 7.25

7-9 Information on Purpose and Intended Nature of Business Relations

7-9-1 The VCC should ensure that the measures taken by its EFI to understand the purpose and intended nature of business relations between the VCC and its customer is commensurate with the complexity of the customer's business and risk profile. For higher risk customers, the VCC should ensure that its EFI seeks to understand the nature of business relations and expected transaction activity (e.g. types of transactions likely to pass through, expected amount for each transaction) and consider, as part of ongoing monitoring whether the activity corresponds with the stated purpose of the business relations. This will enable a more effective ongoing monitoring of the customer's business relations and transactions.

Notice Paragraphs 7.26 to 7.33

7-10 Ongoing Monitoring

7-10-1 Ongoing monitoring of business relations is a fundamental feature of an effective AML/CFT risk management system. Ongoing monitoring should be conducted in relation to all business relations, but the extent and depth of monitoring of a customer may be adjusted according to the customer's ML/TF risk profile. The adequacy of monitoring systems and the factors leading to adjustment of the level of monitoring should be reviewed regularly for effectiveness in mitigating the VCC's ML/TF risks.

7-10-2 Further enquiries should be made when a customer performs frequent and cumulatively large transactions without any apparent or visible economic or lawful purpose. For example, frequent subscriptions in and redemption of units or shares from the VCC (leading to losses) in small tranches of which each might not be substantial, but the total of which is substantial.

7-10-3 Where there are indications that the risks associated with an existing business relation may have increased, the additional information should be requested, and the VCC should ensure that its EFI conducts a review of the customer's risk profile in order to determine if additional measures are necessary.

7-10-4 A key part of ongoing monitoring includes maintaining relevant and up-to-date CDD data, documents and information so that changes to the customer's risk profile can be identified —

(a) for higher risk categories of customers, updated CDD information (including updated copies of the customers' passport or identity documents if these have expired) should be obtained, as part of the periodic CDD review, or upon the occurrence of a trigger event, whichever is earlier; and

(b) for all other risk categories of customers, updated CDD information should be obtained upon the occurrence of a trigger event.

7-10-5 Examples of trigger events are when (i) a significant transaction takes place, (ii) a material change to the VCC's business relations with a customer occurs, (iii) the VCC's policies, procedures or standards relating to the documentation of CDD information change substantially, and (iv) the VCC or its EFI becomes aware that it lacks sufficient information about the customer concerned.

7-10-6 The frequency of CDD review may vary depending on each customer's risk profile. Higher risk customers should be subject to more frequent periodic review (e.g. on an annual basis) to ensure that CDD information such as nationality, passport details, certificate of incumbency, ownership and control information that was previously obtained remain relevant and up-to-date.

7-10-7 In determining what would constitute suspicious, complex, unusually large or unusual pattern of transactions, the VCC should ensure that its EFI considers,

amongst others, international typologies and information obtained from law enforcement and other authorities that may point to jurisdiction-specific considerations. As part of ongoing monitoring, an EFI should pay attention to transaction characteristics, such as —

(a) the nature of a transaction (e.g. abnormal size or frequency for that customer or peer group);

(b) whether a series of transactions is conducted with the intent to avoid reporting thresholds (e.g. by structuring an otherwise single subscription or redemption into a number of small tranches);

(c) the geographic destination or origin of a payment (e.g. to or from a higher risk country); and

(d) the parties concerned (e.g. a request to make a payment to or from a person on a sanctions list).

7-10-8 The transaction monitoring processes or systems used by the EFI may vary in scope or sophistication (e.g. using spreadsheets to automated and complex systems). The degree of automation or sophistication of processes and systems depends on the size and complexity of the VCC's business.

7-10-9 Nevertheless, the processes and systems should provide relevant employees and officers including the AML/CFT compliance officer with timely information needed to identify, analyse and effectively monitor customer transactions for ML/TF.

7-10-10 The transaction monitoring processes and systems should enable the EFI to identify any suspicious transactions. In the event that the EFI discovers suspicious transactions in relation to a VCC's customer, such information should be shared with the VCC. In addition, the VCC should ensure that the EFI performs trend analyses of transactions to identify unusual or suspicious transactions. The VCC should ensure that the EFI also monitors transactions with parties in high risk countries or jurisdictions.

7-10-11 Customers with multiple units or shares in the sub-funds of an umbrella VCC should be monitored holistically, so as to better understand the risks associated with such customer groups, identify potential ML/TF risks and report suspicious transactions.

7-10-12 The parameters and thresholds used by the EFI to identify suspicious transactions should be properly documented and independently validated to ensure that they are appropriate to its operations and context. The VCC should ensure that the EFI periodically reviews the appropriateness of the parameters and thresholds used in the monitoring process.

Notice Paragraphs 7.34 to 7.36

7-11 CDD Measures for Non-Face-to-Face Business Relations

7-11-1 A reference to "specific risks" in paragraph 7.34 of the Notice includes risks arising from establishing business relations and undertaking transactions according to instructions conveyed by customers over the internet, post, fax or telephone. It should be noted that applications and transactions undertaken across the internet may pose greater risks than other non-face-to-face business due to the following factors:

(a) the ease of unauthorised access to the facility, across time zones and location;

(b) the ease of making multiple fictitious applications without incurring extra cost or the risk of detection;

(c) the absence of physical documents; and

(d) the speed of electronic transactions,

that may, taken together, aggravate the ML/TF risks.

7-11-2 The measures taken by an EFI for verification of an identity in respect of non-face-to-face business relations with or transactions for the VCC's customer will depend on the nature and characteristics of the product or service provided and the customer's risk profile.

7-11-3 Where verification of identity is performed without face-to-face contact (e.g. electronically), a VCC should ensure its EFI applies additional checks to manage the risk of impersonation. The additional checks may consist of robust anti-fraud checks that the EFI routinely undertakes as part of its existing procedures, which may include —

(a) telephone contact with the customer at a residential or business number that can be verified independently;

(b) confirmation of the customer's address through an exchange of correspondence or other appropriate method;

(c) subject to the customer's consent, telephone confirmation of the customer's employment status with his employer's department at a listed business number of the employer;

(d) confirmation of the customer's salary details by requiring the presentation of recent bank statements from a bank, where applicable;

(e) provision of certified identification documents by lawyers or notaries public;

(f) requiring the customer to make an initial investment into the VCC from funds held by the customer in an account with a bank in Singapore;

(g) holding real-time video conference that is comparable to face-to-face communication, in addition to providing electronic copies of identification documents;

(h) verifying the identity of a customer through a document that the customer has signed with a secure digital signature using a set of Public Key Infrastructure-based credentials issued by a certified Certificate Authority under the Electronic Transaction Act (Cap.88); or

(i) using new technology solutions [2] including, but not limited to, biometric technologies (e.g fingerprint or iris scans, facial recognition), which should be linked incontrovertibly to the customer.

Notice Paragraph 7.37

7-12 Reliance by Acquiring VCC on Measures Already Performed

7-12-1 When a VCC acquires the business of, units or shares in another VCC, collective investment scheme or investment vehicle, either in whole or in part, it is not necessary for the identity of all existing customers to be verified again, provided that the requirements of paragraph 7.37 of the Notice are met. Proper records of the due diligence review performed on the acquired business shall be maintained. The VCC is reminded of its obligation to comply with ongoing monitoring requirements set out in paragraphs 7.26 to 7.33 of the Notice in relation to the new customers.

7-12-2 Notwithstanding the reliance on identification and verification that has already been performed, an acquiring VCC is responsible for its obligations under the Notice.

Notice Paragraphs 7.38 to 7.40

7-13 Timing for Verification

7-13-1 One way to effectively manage the ML/TF risks arising from the deferral of completion of verification is to put in place appropriate limits on the financial services available to the customer (e.g. limits on the number, type and value of transactions that can be effected) and institute closer monitoring procedures, until the verification has been completed.

7-13-2 With reference to paragraph 7.40 of the Notice —

[2] A technology will be considered new if it is new to, or has yet to be widely adopted, by financial institutions or VCCs in Singapore for the purposes of onboarding customers

(a) the completion of verification should not exceed 30 business days after the establishment of business relations;

(b) the VCC should suspend business relations with the customer and refrain from carrying out further transactions (except to return funds to their sources, to the extent that this is possible) if such verification remains uncompleted 30 business days after the establishment of business relations;

(c) the VCC should terminate business relations with the customer if such verification remains uncompleted 120 business days after the establishment of business relations; and

(d) the VCC should factor these time limitations in its policies, procedures and controls.

Notice Paragraphs 7.43 to 7.45

7-14 Screening

7-14-1 Screening is intended to be a preventive measure. A VCC is reminded that all parties identified pursuant to the Notice must be screened, irrespective of the risk profile of the customer.

7-14-2 Where screening results in a positive hit against sanctions lists, a VCC is reminded of its obligations to freeze without delay and without prior notice, the funds or other assets of designated persons and entities that it has control over, so as to comply with applicable laws and regulations in Singapore, including the TSOFA and VCC Regulations issued under section 83 of the VCC Act relating to sanctions and freezing of assets of persons. Any such assets should be reported promptly to the relevant authorities and an STR should be filed.

7-14-3 A VCC should have policies, procedures and controls for the EFI to screen the VCC's customers, natural persons appointed to act on behalf of the customer, connected parties of the customer and beneficial owners of the customer. These policies and procedures should clearly set out —

(a) the ML/TF information sources to be used for screening (including commercial databases used to identify adverse information on individuals and entities, individuals and entities covered under VCC Regulations issued pursuant to section 83 of the VCC Act, TSOFA, individuals and entities identified by other sources such as the lists and information provided by the Authority and relevant authorities in Singapore);

(b) the roles and responsibilities of the relevant EFI employees involved in the screening, reviewing and dismissing of alerts, maintaining and updating of the various screening databases and escalating hits;

(c) the frequency of review of such policies, procedures and controls;

(d) the frequency of periodic screening;

(e) how apparent matches from screening are to be resolved, including the process for determining that an apparent match is a positive hit and for dismissing an apparent match as a false hit; and

(f) the steps to be taken for reporting positive hits to the VCC's senior management and to the relevant authorities.

7-14-4 The level of automation used in the screening process should take into account the nature, size and risk profile of a VCC's business. A VCC and its EFI should be aware of any shortcomings in automated screening systems. In particular, it is important to consider "fuzzy matching" to identify non-exact matches. The VCC should ensure that the EFI's fuzzy matching process is calibrated to the VCC's risk profile.

7-14-5 A VCC and its EFI should be aware that performing screening after business relations have been established could lead to a breach of relevant laws and regulations in Singapore relating to sanctioned parties. When the VCC or EFI becomes aware of such breaches, it should immediately take the necessary actions and inform the relevant authorities.

7-14-6 In screening periodically as required by paragraph 7.44(b) of the Notice, a VCC should ensure that its EFI pays particular attention to changes in customer status (e.g. whether the customer has over time become subject to prohibitions and sanctions) or customer risks (e.g. a connected party of a customer, a beneficial owner of the customer or a natural person appointed to act on behalf of the customer subsequently becomes a Politically Exposed Person or presents higher ML/TF risks, or a customer subsequently becomes a Politically Exposed Person or presents higher ML/TF risks) and assess whether to subject the customer to the appropriate ML/TF risk mitigation measures (e.g. enhanced CDD measures).

7-14-7 A VCC should ensure that its EFI enters the identification information of a customer, a connected party of the customer, a natural person appointed to act on behalf of the customer, or a beneficial owner of the customer into the VCC's customer database for periodic name screening purposes. This is to help promptly identify any existing customers who have subsequently become higher risk parties.

7-14-8 In determining the frequency of periodic name screening in its policies and procedures, a VCC should consider its customers' risk profile.

7-14-9 The VCC should ensure that the EFI screens the VCC's customer database when there are changes to the lists of sanctioned individuals and entities, covered by the TSOFA, VCC Regulations issued under section 83 of the VCC Act[3]. The VCC should ensure that the EFI implements "four-eye checks" on alerts from sanctions

[3] Please refer to the following link for the relevant MAS ML/TF Regulations - https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions/regulations-for-targeted-financial-sanctions

reviews before closing an alert, or conduct quality assurance checks on the closure of such alerts on a sample basis.

8 Notice Paragraph 8 – Simplified Customer Due Diligence

8-1 Paragraph 8.1 of the Notice permits the adoption of a risk-based approach in assessing the necessary measures to be performed, and to perform appropriate simplified customer due diligence ("SCDD") measures in cases where the VCC is satisfied that the ML/TF risks are low.

8-2 Where SCDD measures are applied, ongoing monitoring of business relations must still be performed under the Notice.

8-3 Under SCDD, a risk-based approach may be adopted in assessing whether any measures should be performed for connected parties of the customers.

8-4 Where the VCC is satisfied that the ML/TF risks are low, it may allow the EFI to perform SCDD measures. Examples of possible SCDD measures include —

(a) reducing the frequency of updates of customer identification information;

(b) reducing the degree of ongoing monitoring and scrutiny of transactions, based on a reasonable monetary threshold; or

(c) choosing another method to understand the purpose and intended nature of business relations by inferring this from the type of transactions, instead of collecting information as to the purpose and intended nature of business relations.

8-5 Subject to the requirement that the assessment of low ML/TF risks is supported by an adequate analysis, examples of potentially lower ML/TF risk situations include —

(a) Customer risk

(i) a Singapore Government entity;

(ii) entities listed on a stock exchange and subject to regulatory disclosure requirements (relating to adequate transparency in respect of beneficial owners (imposed through stock exchange rules, law or other enforceable means); and

(iii) an FI incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

9 Notice Paragraph 9 – Enhanced Customer Due Diligence

9-1 Where the ML/TF risks are identified to be higher, enhanced CDD ("ECDD") measures shall be taken to mitigate and manage those risks.

9-2 Examples of potentially higher risk categories under paragraph 9.7 of the Notice include —

(a) Customer risk

(i) customers from higher risk businesses / activities / sectors identified in Singapore's NRA, as well as other higher risk businesses / activities / sectors identified by the VCC or its EFI;

(ii) the ownership structure of the legal person or arrangement appears unusual or excessively complex given the nature of the legal person's or legal arrangement's business;

(iii) legal persons or legal arrangements that are personal asset holding vehicles;

(iv) the business relations is conducted under unusual circumstances (e.g. significant unexplained geographic distance between the VCC and the customer);

(v) companies that have nominee shareholders or shares in bearer form; and

(vi) cash-intensive businesses.

(b) Country or geographic risk

(i) countries or jurisdictions the VCC is exposed to, either through its own activities (including where its branches and subsidiaries operate in) or the activities of its customers which have relatively higher levels of corruption, organised crime or inadequate AML/CFT measures, as identified by the FATF. This should take into account, where appropriate, variations in ML/TF risks across different regions or areas within a country; and

(ii) countries identified by credible bodies (e.g. reputable international bodies such as Transparency International) as having significant levels of corruption, terrorism financing or other criminal activity.

(c) Product, service, transaction or delivery channel risk

(i) frequent payments for subscription purposes received from unknown or unassociated third parties.

Notice Paragraph 9.1

9-3 Politically Exposed Persons ("PEPs") Definitions

9-3-1 The definitions in paragraph 9.1 of the Notice are drawn from the FATF Recommendations. The definition of PEPs is not intended to cover middle-ranking or more junior individuals in the categories listed.

9-3-2 In the context of Singapore, domestic PEPs should include at least all Government Ministers, Members of Parliament, Nominated Members of Parliament and Non-Constituency Members of Parliament.

9-3-3 When determining whether a person is a "close associate" of a PEP, the VCC may allow its EFI to consider factors such as the level of influence the PEP has on such a person or the extent of his exposure to the PEP. The EFI may rely on information available from public sources and information obtained through customer interaction.

9-3-4 With reference to paragraph 9.1 of the Notice, examples of an "international organisation" include the United Nations and affiliated agencies such as the International Maritime Organisation and the International Monetary Fund; regional international organisations such as the Asian Development Bank, Association of Southeast Asian Nations Secretariat, institutions of the European Union, the Organisation for Security and Cooperation in Europe; military international organisations such as the North Atlantic Treaty Organisation; and economic organisations such as the World Trade Organisation or the Asia-Pacific Economic Cooperation Secretariat.

9-3-5 Examples of persons who are or have been entrusted with prominent functions by an international organisation are members of senior management such as directors, deputy directors and members of the board or equivalent functions. Other than relying on the information from a customer, the EFI may consider information from public sources, in determining whether a person has been or is entrusted with prominent functions by an international organisation.

Notice Paragraphs 9.2 to 9.4

9-4 PEPs

9-4-1 Where a natural person appointed to act on behalf of a customer or any connected party of a customer is determined to be a PEP, the VCC should ensure that the EFI assesses the ML/TF risks presented and consider factors such as the level of influence that the PEP has on the customer. The EFI should consider factors such as whether the PEP is able to exercise substantial influence over the customer, to determine the overall ML/TF risks presented by the customer. Where the customer presents higher ML/TF risks, the VCC should ensure that the EFI applies ECDD measures on the customer accordingly.

9-4-2 It is generally acceptable for a VCC to allow its EFI to refer to commercially available databases to identify PEPs. However, the details of the customer's occupation and the name of his employer should be obtained. In addition, an EFI should consider other non-public information that it is aware of. Sound judgment shall be exercised in identifying any PEP, having regard to the risks and the circumstances.

9-4-3 In relation to paragraph 9.3(a) of the Notice, the approval shall be obtained from the VCC's senior management. Inputs should also be obtained from the VCC's AML/CFT compliance officer.

9-4-4 In relation to paragraph 9.3(b) of the Notice, a VCC may allow its EFI to refer to information sources such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include information about an official's source of wealth and current business interests. It should be noted that not all declarations are publicly available. It should also be noted that certain jurisdictions impose restrictions on their PEPs' ability to hold foreign investment accounts, to hold other office or paid employment.

9-4-5 Source of wealth generally refers to the origin of the customer's and beneficial owner's entire body of wealth (i.e. total assets). This relates to how the customer and beneficial owner of the customer have acquired the wealth which is distinct from identifying the assets that they own. Source of wealth information should give an indication about the size of wealth the customer and beneficial owner would be expected to have, and how the customer and beneficial owner acquired the wealth. Although there may not be specific information about assets that are not invested in the VCC, it may be possible to obtain general information from the customer, commercial databases or other open sources. Examples of appropriate and reasonable means of establishing source of wealth are information and documents such as evidence of title, copies of trust deeds, audited accounts, salary details, tax returns and bank statements.

9-4-6 Source of funds refers to the origin of the particular funds or other assets which are the subject of the establishment of business relations (e.g. the amounts being invested as part of the business relations). In order to ensure that the funds are not proceeds of crime, the VCC should ensure that the EFI does not limit its source of funds inquiry to identifying the FI from which the funds have been transferred, but more importantly, the activity that generated the funds. The information obtained should be substantive and facilitate the establishment of the provenance of the funds or reason for the funds having been acquired. Examples of appropriate and reasonable means of establishing source of funds are information such as salary payments or sale proceeds.

9-4-7 Based on its risk assessment of the PEP, a VCC should consider requiring its EFI to corroborate the information regarding source of wealth and source of funds. In relation to paragraph 9.3(b) of the Notice, examples of "appropriate and reasonable means" for establishing source of wealth or source of funds are financial statements of the legal person or legal arrangement owned or controlled by the PEP, site visits, a copy of the will (in cases where the source of wealth or

funds is an inheritance), and conveyancing documents (in cases where the source of wealth or funds is a sale of property).

9-4-8 In relation to paragraph 9.3 of the Notice, other ECDD measures that may be performed include —

(a) requiring the first payment for subscription purposes to be carried out through an account in the customer's name with an FI subject to similar or equivalent CDD standards;

(b) using public sources of information (e.g. websites) to gain a better understanding of the reputation of the customer or any beneficial owner of a customer. Where the VCC or EFI finds information containing allegations of wrongdoing by a customer or a beneficial owner of a customer, an assessment as to how this affects the level of risk associated with the business relations should be made;

(c) commissioning external intelligence reports where it is not possible for a VCC or EFI to easily obtain information through public sources or where there are doubts about the reliability of public information.

9-4-9 In relation to paragraphs 9.4(a) and (b) of the Notice, where the EFI assesses that the business relations or transactions with a domestic PEP or an international organisation PEP do not present higher ML/TF risks and that therefore ECDD measures need not be applied, the measures under paragraph 7 of the Notice shall nevertheless be applied on the customer. However, where changes in events, circumstances or other factors lead to the EFI's assessment that that the business relations or transactions with the customer present higher ML/TF risks, the VCC should ensure that the EFI reviews the customer risk assessment and applies ECDD measures.

9-4-10 While domestic PEPs and international organisation PEPs may be subject to a risk-based approach, it does not preclude such persons from presenting the same ML/TF risks as a foreign PEP.

9-4-11 With reference to paragraph 9.4(c) of the Notice, while the time elapsed since stepping down from a prominent public function is a relevant factor to consider when determining the level of influence a PEP continues to exercise, it should not be the sole determining factor. Other risk factors are —

(a) the seniority of the position that the individual previously held when he was a PEP; and

(b) whether the individual's previous PEP position and current function are linked in any way (e.g. whether the ex-PEP was appointed to his current position or function by his successor, or whether the ex-PEP continues to substantively exercise the same powers in his current position or function).

Notice Paragraphs 9.5 to 9.8

9-5 Other Higher Risk Categories

9-5-1 In relation to paragraph 9.7 of the Notice, a VCC and its EFI may refer to the preceding paragraph 9-4-8 of these Guidelines for further guidance on the ECDD measures to be performed.

9-5-2 Customers highlighted in paragraph 9.6(a) of the Notice, shall be assessed as customers presenting higher ML/TF risks. For such customers, ECDD measures performed shall be commensurate with the risks. For customers highlighted in paragraph 9.6(b) of the Notice, an assessment shall be made as to whether any such customer presents a higher risk for ML/TF. Measures performed under paragraph 7 of the Notice, or ECDD measures where the customer presents a higher risk for ML/TF, should be commensurate with the risk.

9-5-3 With reference to paragraph 9.6(a) of the Notice, in considering the appropriate internal risk management systems, policies, procedures and controls under paragraph 9.5 of the Notice, a VCC should refer to the FATF Public Statement on High Risk and Other Monitored Jurisdictions on which FATF has called for counter-measures[4]. FATF updates this Public Statement on a periodic basis and VCCs should regularly refer to the FATF website for the latest updates[5].

9-5-4 For high net worth individuals, in considering the appropriate internal risk management systems, policies, procedures and controls under paragraph 9.5 of the Notice, a VCC and its EFI should, regardless of the internal risk classification of the customer, refer to the sound practices highlighted in the MAS Information Paper, "Guidance on Private Banking Controls"[6]. Such practices include ensuring that –

(a) information obtained on the source of wealth of the customers and beneficial owners should be independently corroborated against documentary evidence or public information sources;

(b) parties screened should include operating companies and individual benefactors contributing to the customer's and beneficial owner's wealth/ funds;

(c) periodic reviews of such customers should be conducted; and

(d) where the VCC or its EFI is aware of customers having a common beneficial owner or a customer having multiple units or shares in the sub-funds of an umbrella VCC, transactions of the customer should be scrutinised holistically

[4] http://www.fatf-gafi.org/countries/#high-risk

[5] The link to the FATF website is as follows: http://www.fatf-gafi.org/

[6] https://www.mas.gov.sg/-/media/MAS/About-MAS/Monographs-and-information-papers/Guidance-on-PB-Controls--June2014.pdf

to better identify suspicious, complex, unusually large or unusual patterns of transactions, and perform periodic reviews on a consolidated basis.

9-5-5 For the purposes of paragraph 9.8 of the Notice, regulations issued by the Authority include the Regulations relating to the freezing of assets of persons and sanctioning of persons.

9-5-6 With regard to tax and other serious crimes, as a preventive measure, a VCC is expected to reject a prospective customer where there are reasonable grounds to suspect that the customer's assets are the proceeds of serious crimes, including wilful and fraudulent tax evasion. Where there are grounds for suspicion in an existing customer relationship, a VCC should ensure that its EFI conducts enhanced monitoring and where appropriate, have the relationship between the customer and VCC discontinued. If the VCC is inclined to retain the customer, approval shall be obtained from the VCC's senior management with the substantiating reasons properly documented, and the business relations and transactions subjected to close monitoring and commensurate risk mitigation measures. This requirement applies to serious foreign tax offences, even if the foreign offence is in relation to the type of tax for which an equivalent obligation does not exist in Singapore. Examples of tax crime related suspicious transactions are set out in Appendix B of these Guidelines.

10 Notice Paragraph 10 – Reliance on Third Parties

10-1 As stated in paragraph 10 of the Notice, a VCC may allow the EFI to rely on a third party to perform the CDD measures in paragraphs 7, 8 and 9 of the Notice, subject to the requirements in paragraph 10. The VCC remains ultimately responsible for the proper performance of the CDD measures by any third party that the EFI relies on. The VCC should have oversight on the third party reliance arrangements of its EFI, where such arrangements relate to conducting the necessary checks and performing the measures in order for the VCC to comply with the Notice.

10-2 Third party reliance is different from the arrangement between the VCC and its EFI. In a third party reliance scenario, the third party will typically have an existing relationship with the customer that is independent of the relationship to be formed by the customer with the VCC or the EFI. The third party will therefore perform the CDD measures on the customer according to its own AML/CFT policies, procedures and controls. In contrast to a third party reliance scenario, the VCC's EFI performs the CDD measures on behalf of the VCC, in accordance with the VCC's AML/CFT policies, procedures and standards.

10-3 Measures that may be taken to satisfy the requirements in paragraphs 10.1(b) and 10.1(c) of the Notice include—

(a) referring to any independent and public assessment of the overall AML/CFT regime to which the third party is subject, such as the FATF or FSRBs' Mutual Evaluation reports and the IMF / World Bank Financial Sector Assessment Programme Reports / Reports on the Observance of Standards and Codes;

(b) referring to any publicly available reports or material on the quality of that third party's compliance with applicable AML/CFT rules;

(c) obtaining professional advice as to the extent of AML/CFT obligations to which the third party is subject to with respect to the laws of the jurisdiction in which the third party operates;

(d) examining the AML/CFT laws in the jurisdiction where the third party operates and determining its comparability with the AML/CFT laws of Singapore;

(e) reviewing the policies and procedures of the third party.

10-4 The reference to "documents" in paragraph 10.1(e) of the Notice includes a reference to the underlying CDD-related documents and records obtained by the third party to support the CDD measures performed (e.g. copies of identification information, CDD/Know Your Customer forms). Where these documents and records are kept by the third party, the third party should provide an undertaking to keep all underlying CDD-related documents and records for at least five years following the termination of the VCC's business relations with the customer or the completion of transactions undertaken.

10-5 The VCC shall engage an EFI to perform the ongoing monitoring processes as required by paragraph 4.1 of the Notice. In turn, paragraph 10.2 of the Notice requires the VCC to ensure that the EFI does not rely on a third party to carry out ongoing monitoring. Paragraph 10.2 of the Notice on ongoing monitoring should be read with the ongoing monitoring requirements in Part (IX) of paragraph 7 of the Notice.

13 Notice Paragraph 13 – Suspicious Transactions Reporting

13-1 A VCC should ensure that the internal process for evaluating whether a matter should be referred to the Suspicious Transaction Reporting Office ("STRO") via an STR is completed without delay and should not exceed 15 business days of the case being referred by the relevant employee or officer, unless the circumstances are exceptional or extraordinary.

13-2 A VCC should note that an STR filed with STRO would also meet the reporting obligations under the TSOFA. For the avoidance of doubt, the STR may be filed by the EFI, on behalf of the VCC.

13-3 Examples of suspicious transactions are set out in Appendix B of these Guidelines. These examples are not intended to be exhaustive and are only examples of the most basic ways in which money may be laundered or used for TF purposes. Identification of suspicious transactions should prompt further enquiries and where necessary, investigations into the source of funds. A VCC should also consider filing an STR if there is any adverse news on its customers in relation to financial crimes. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.

13-4 Once suspicion has been raised in relation to a customer or any transaction for that customer, in addition to reporting the suspicious activity, a VCC should ensure that appropriate action is taken to adequately mitigate the risk of the VCC being used for ML/TF activities. This may include strengthening its AML/CFT processes; reviewing of either the risk classification of the customer, or the business relations with the customer; and escalating the issue to the appropriate decision making level, taking into account any other relevant factors, such as cooperation with law enforcement agencies.

13-5 VCCs are strongly encouraged to use the online system provided by STRO to lodge STRs. In the event that the VCC is of the view that STRO should be informed on an urgent basis, particularly where a transaction is known to be part of an ongoing investigation by the relevant authorities, the VCC should give initial notification to STRO by telephone or email and follow up with such other means of reporting as STRO may direct.

13-6 A VCC should ensure the documentation of all transactions that have been brought to the attention of its AML/CFT compliance officer, including transactions that are not reported to STRO. To ensure that there is proper accountability for decisions made, the basis for not submitting STRs for any suspicious transactions escalated should be properly substantiated and documented.

13-7 VCCs are reminded to read paragraph 13.4 of the Notice together with paragraphs 7.41 and 7.42 of the Notice. Where the performance of CDD measures is stopped as permitted under paragraph 13.4 and CDD measures cannot be completed (as specified under paragraph 7.42), the VCC is reminded that it shall not commence or continue business relations with that customer or undertake any transaction for that customer.

14 Notice Paragraph 14 – Internal Policies, Compliance, Audit and Training

14-1 A VCC's policies and procedures should be updated in a timely manner, to take into account new operational, legal and regulatory developments and emerging or new ML/TF risks.

14-2 A VCC may adopt the internal policies and procedures as developed by its EFI, but should make appropriate modifications to the internal policies and procedures to ensure that the policies and procedures is applicable and relevant to the VCC's context.

14-3 As the VCC remains ultimately responsible for its compliance with the Notice, the VCC's senior management and board of directors should be the final authority approving the VCC's internal policies and procedures.

Notice Paragraphs 14.3 to 14.8

14-4 Group Policy

14-4-1 For the avoidance of doubt, a VCC that is a subsidiary of an FI incorporated outside Singapore need not comply with paragraphs 14.3 to 14.8 of the Notice. Paragraphs 14.3 to 14.8 of the Notice are intended to be applied by a VCC to its branches and subsidiaries, but not to its parent entity and the VCC's other related corporations.

14-4-2 In relation to paragraph 14.5 of the Notice, examples of the types of information that should be shared with its branches and subsidiaries which are financial institutions or VCCs for risk management purposes are positive name matches arising from screening performed against ML/TF information sources, a list of customers who have been exited by the VCC, its branches and subsidiaries based on suspicion of ML/TF and names of parties on whom STRs have been filed. Such information should be shared by a branch or subsidiary of a VCC with the VCC's group level compliance, audit, and AML/CFT functions, for risk management purposes.

Notice Paragraphs 14.9 to 14.10

14-5 Compliance

14-5-1 A VCC should ensure that its AML/CFT compliance officer has the necessary seniority and authority within the VCC to effectively perform his responsibilities.

14-5-2 The responsibilities of the AML/CFT compliance officer should include —

(a) carrying out, or overseeing the carrying out of, ongoing monitoring of business relations and sample review of business relations with customers for compliance with the Notice and these Guidelines;

(b) promoting compliance with the Notice and these Guidelines, as well as VCC Regulations issued under section 83 of the VCC Act, and taking overall charge of all AML/CFT matters within the organisation;

(c) informing board and senior management promptly of regulatory changes;

(d) ensuring a speedy and appropriate reaction to any matter in which ML/TF is suspected;

(e) reporting, or overseeing the reporting of, suspicious transactions;

(f) advising and training board and senior management on its internal policies, procedures and controls on AML/CFT;

(g) reporting to senior management on the outcome of reviews of the VCC's compliance with the Notice and these Guidelines, as well as VCC Regulations issued under section 83 of the VCC Act and risk assessment procedures; and

(h) reporting regularly on key AML/CFT risk management and control issues (including information outlined in paragraph 1-5-12 of the Guidelines), and any necessary remedial actions, arising from audit, inspection, and compliance reviews, to the VCC's senior management and to the board of directors, at least annually and as and when needed.

Notice Paragraph 14.11

14-6 Audit

14-6-1 Periodic audits should be performed on the VCC's AML/CFT framework (including sample testing). Such audits should include the evaluation of adequacy of the checks and measures performed by EFI in its discharge of the VCC's AML/CFT obligations. For avoidance of doubt, such audits need not be conducted solely on the VCC, but may be scoped into the audit of the EFI's own activities. Auditors should assess the effectiveness of measures taken to prevent ML/TF. This would include, among others —

(a) determining the adequacy of the VCC's AML/CFT policies, procedures and controls, ML/TF risk assessment framework and application of risk-based approach;

(b) reviewing the content and frequency of AML/CFT training programmes, and the extent of employees' and officers' compliance with established AML/CFT policies and procedures; and

(c) assessing whether instances of non-compliance are reported to board of directors or senior management of the VCC on a timely basis.

14-6-2 The frequency and extent of the audit should be commensurate with the ML/TF risks presented and the size and complexity of the VCC's business.

Notice Paragraph 14.12

14-7 Employee Hiring

14-7-1 The screening procedures applied when a VCC in Singapore hires employees and appoints officers should include —

(a) background checks with past employers;

(b) screening against ML/TF information sources; and

(c) bankruptcy searches.

14-7-2 In addition, a VCC should conduct credit history checks, on a risk-based approach, when hiring employees and appointing officers.

14-7-3 For the avoidance of doubt, screening need not be re-performed on employees and officers of the EFI who have been appointed to roles within the VCC, if the EFI has already previously screened them in line with the VCC's procedures, and the VCC is satisfied that there has been no material change in their risk profile.

Notice Paragraph 14.13

14-8 Training

14-8-1 A VCC should ensure that its EFI adequately trains the relevant employees and officers (whether from the EFI or VCC) facilitating the VCC's compliance with AML/CFT requirements, to implement the VCC's AML/CFT policies and procedures. The scope and frequency of training should be tailored to the specific risks faced by the VCC and pitched according to the job functions, responsibilities and experience of the employees and officers. New employees and officers should be required to attend training as soon as possible after being hired or appointed.

14-8-2 Apart from the initial training, refresher training should also be provided at least once every two years, or more regularly as appropriate, to ensure that employees and officers (whether from the EFI or VCC) are reminded of their responsibilities and are kept informed of new developments related to ML/TF. The training records should be maintained for audit purposes.

14-8-3 A VCC should ensure that the effectiveness of the training provided to the employees and officers (whether from the EFI or VCC) facilitating the VCC's compliance with AML/CFT requirements, is being monitored. This may be achieved by —

(a) testing employees' and officers' understanding of the VCC's policies and procedures to combat ML/TF, their obligations under relevant laws and regulations, and their ability to recognise suspicious transactions;

(b) monitoring employees' and officers' compliance with the VCC's AML/CFT policies, procedures and controls as well as the quality and quantity of internal reports so that further training needs may be identified and appropriate action taken; and

(c) monitoring attendance and following up with employees and officers who miss such training without reasonable cause.

I Other Key Topics - Guidance to VCCs on Proliferation Financing

I-1 Overview

I-1-1 MAS issues Regulations under section 27A of the VCC Act in order to discharge or facilitate the discharge of any obligation binding on Singapore by virtue of a United Nations Security Council Resolution ("UNSCR")[7] and these Regulations apply to all financial institutions regulated by MAS. Similar obligations also apply to VCCs through the Variable Capital Companies (Sanctions and Freezing of Assets of Persons) Regulations 2020 made in exercise of the powers conferred by section 83(1)(b) of the VCC Act which generally impose financial sanctions on designated persons.

I-1-2 Specifically, a UNSCR may designate certain individuals and entities involved in the proliferation of weapons of mass destruction and its financing. The relevant information and full listings of persons designated by UNSCRs can be found on the UN website[8].

I-1-3 MAS has given effect to UNSCRs as listed by the FATF Recommendations (2012) to be relevant to combating proliferation financing by issuing Regulations. Examples of such Regulations are the MAS (Sanctions and Freezing of Assets of Persons – Iran) Regulations 2016, the MAS (Sanctions and Freezing of Assets of Persons – Democratic People's Republic of Korea) Regulations 2016, and the VCC (Sanctions and Freezing of Assets of Persons) Regulations 2020.

I-1-4 A VCC should rely on its CDD measures (including screening measures) under the Notice to detect and prevent proliferation financing activities and transactions. Where necessary, suspicious transactions reports should be filed promptly with STRO.

I-1-5 A VCC should also ensure compliance with legal instruments issued by MAS relating to proliferation financing risks.

I-2 CDD and Internal Controls

I-2-1 It is important to ensure that name screening, as required under the Notice, is performed against the latest UN listings as they are updated from time to time. A VCC should have in place policies, procedures and controls to continuously monitor the listings and take necessary follow-up action within a reasonable period of time, as required under the applicable laws and regulations.

I-2-2 A VCC should also have policies and procedures to detect attempts by its employees or officers, to circumvent the applicable laws and regulations (including MAS Regulations), such as:

[7] Please refer to the MAS website for a full listing of Regulations issued by MAS pursuant to the United Nations Security Council Resolutions.

[8] Please see: https://www.un.org/securitycouncil/sanctions/1718 and https://www.un.org/securitycouncil/content/2231/list.

(a) omitting, deleting or altering information in payment messages for the purpose of avoiding detection of that information by the VCC itself or other VCCs or FIs involved in the payment process; and
(b) structuring transactions with the purpose of concealing the involvement of designated persons.

I-2-3 A VCC should have policies and procedures to prevent such attempts, and take appropriate measures against such employees and officers.

I-3 Obligation of VCC to Freeze without Delay

I-3-1 A VCC is reminded of its obligations under the VCC Regulations issued under section 83 of the VCC Act[9] to immediately freeze any funds, financial assets or economic resources owned or controlled, directly or indirectly, by designated persons that the VCC has in its possession, custody or control. The VCC should also ensure that the EFI files an STR on its behalf in such cases.

I-4 Potential Indicators of Proliferation Financing

I-4-1 A VCC should develop indicators that would alert it to customers and transactions (actual or proposed) that are possibly associated with proliferation financing-related activities, including indicators such as whether —

(a) the customer is vague and resistant to providing additional information when asked;

(b) the customer's activity or information does not match its business profile;

(c) the transaction involves designated persons;

(d) the transaction involves higher risk countries or jurisdictions which are known to be involved in proliferation of weapons of mass destruction or proliferation financing activities;

(e) the transaction involves other FIs or VCCs with known deficiencies in AML/CFT controls or controls for combating proliferation financing;

(f) the transaction involves possible shell companies (e.g. companies that do not have a high level of capitalisation or display other shell company indicators);

[9] Please refer to the following link for the relevant MAS ML/TF Regulations - https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions/regulations-for-targeted-financial-sanctions

I-5 Other Sources of Guidance on Proliferation Financing

I-5-1 MAS has also published the Sound Practices to Counter Proliferation Financing on August 2018, and VCCs should also review and consider the key findings and practices noted, and incorporate them in its internal controls as appropriate.

The FATF has also provided guidance on measures to combat proliferation financing and a VCC may wish to refer to the FATF website for additional information.

II Useful Links

Financial Action Task Force ("FATF"): http://www.fatf-gafi.org/
The International Organization of Securities Commissions: http://www.iosco.org/

……

APPENDIX A – Examples of CDD Information for Customers (Including Legal Persons/ Arrangements)

Customer Type	Examples of CDD Information
Sole proprietorships	• Full registered business name • Business address or principal place of business • Information about the purpose and intended nature of the business relations with the VCC • Names of all natural persons who act on behalf of the sole proprietor (where applicable) • Name of the sole proprietor • Information about the source of funds • A report of the VCC's visit to the customer's place of business, where the VCC assesses it as necessary • Structure of the sole proprietor's business (where applicable) • Records in an independent company registry or evidence of business registration
Partnerships and unincorporated bodies	• Full Name of entity • Business Address or principal place of business • Information about the purpose and intended nature of the business relations with the VCC • Names of all natural persons who act on behalf of the entity • Names of all connected parties • Names of all beneficial owners • Information about the source of funds • A report of the VCC's visit to customer's place of business, where the VCC assesses it as necessary • Ownership and control structure • Records in an independent company registry • Partnership deed • The customer's membership with a relevant professional body • Any association the entity may have with other countries or jurisdictions (e.g. the location of the entity's headquarters, operating facilities, branches, subsidiaries)
Companies	• Full name of entity • Business address or principal place of business • Information about the purpose and intended nature of the business relations with the VCC • Names of all natural persons who act on behalf of the entity • Names of all connected parties

Customer Type	Examples of CDD Information
	• Names of all beneficial owners • Information about the source of funds • A report of the VCC's visit to the customer's place of business, where the VCC assesses it as necessary • Ownership and control structure • Records in an independent company registry • Certificate of incumbency, certificate of good standing, share register, as appropriate • Memorandum and Articles of Association • Certificate of Incorporation • Board resolution authorising the establishment of business relations with the VCC • Any association the entity may have with other countries or jurisdictions (e.g. the location of the entity's headquarters, operating facilities, branches, subsidiaries)
Public sector bodies, government, state-owned companies and supranationals (other than sovereign wealth funds)	• Full name of entity • Nature of entity (e.g. overseas government, treaty organisation) • Business address or principal place of business • Information about the purpose and intended nature of the business relations with the VCC • Name of the home state authority and nature of its relationship with its home state authority • Names of all natural persons who act on behalf of the entity • Names of all connected parties • Information about the source of funds • Ownership and control structure • A report of the VCC's visit to the customer's place of business, where the VCC assesses it as necessary • Board resolution authorising the establishment of business relations with the VCC
Clubs, Societies and Charities	• Full name of entity • Business address or principal place of business • Information about the purpose and intended nature of business relations with the VCC • Information about the nature of the entity's activities and objectives • Names of all trustees (or equivalent) • Names of all natural persons who act on behalf of the entity • Names of all connected parties • Names of all beneficial owners

Customer Type	Examples of CDD Information
	• Information about the source of funds • A report of the VCC's visit to the customer's place of business, where the VCC assesses it as necessary • Ownership and control structure • Constitutional document • Certificate of registration • Committee/Board resolution authorising the establishment of business relations with the VCC • Records in a relevant and independent registry in the country of establishment
Trusts and Other Similar Arrangements (e.g. Foundations, Fiducie, Treuhand and Fideicomiso)	• Full name of entity • Business address or principal place of business • Information about the nature, purpose and objectives of the entity (e.g. discretionary, testamentary) • Names of all natural persons who act on behalf of the entity • Names of all connected parties • Names of all beneficial owners • Information about the source of funds • A report of the VCC's visit to the customer's place of business, where the VCC assesses it as necessary • Information about the purpose and intended nature of business relations with the VCC • Records in a relevant and independent registry in the country or jurisdiction of constitution • Country or jurisdiction of constitution • Trust deed • Names of the settlors/trustees/beneficiaries or any person who has power over the disposition of any property that is subject to the trust • Declaration of trusts • Deed of retirement and appointment of trustees (where applicable)

APPENDIX B – Examples of Suspicious Transactions

B-1 General Comments

B-1-1 The list of situations given below is intended to highlight some basic ways in which money may be laundered or used for TF purposes. While each individual situation may not be sufficient to suggest that ML/TF is taking place, a combination of such situations may be indicative of a suspicious transaction. The list is not exhaustive. It is intended solely as an aid, and must not be applied as a routine instrument in place of common sense. VCCs should also be alert to changing circumstances and new ML/TF methods and typologies. VCCs may refer to STRO's website for the latest list of red flags[10].

B-1-2 A customer's explanation for its transactions should be checked for plausibility. It is not unreasonable to proceed with caution in relation to any customer who is reluctant to provide normal information and documents required routinely by the VCC in the course of the business relations. VCCs should pay attention to customers who provide minimal, false or misleading information, or information that is difficult or expensive for the VCC to verify.

B-2 Indicators of Suspicious Transactions

i) Customer evades attempts by the VCC and its EFI to establish personal contact.

ii) Customer's subscription and redemption patterns indicate some potential illicit purpose or are inconsistent with the VCC's knowledge of the customer, its business and risk profile and where appropriate, the source of funds. For example, substantial increase in the amount or frequency of, subscription or redemption of shares in the VCC, which is not aligned with the VCC's knowledge of, the source of wealth of the customer, and the purpose and intended nature of the establishment of business relations.

iii) Frequent subscriptions and redemptions in the VCC, particularly if they are loss-making after transaction fees are accounted for.

iv) Shares or units in a VCC are redeemed immediately after share subscription, without a plausible reason.

B-3 Tax Crimes Related Transactions

i) Negative tax-related reports from the media or other credible information sources.

[10] The website address as at 4 December 2020: https://www.police.gov.sg/Advisories/Crime/Commercial-Crimes/Suspicious-Transaction-Reporting-Office

ii) Inability to reasonably justify frequent and large investment and/or redemption of the shares in the VCC, where the funds for/ from the investment and/or redemption is made from or to a country or jurisdiction that presents higher risk of tax evasion.