Guideline on Anti-Money Laundering and Counter-Terrorist Financing

(For Stored Value Facility Licensees)

September 2016

CONTENTS

OVERVIEW

Introduction

1. The Guideline is published under section 54(1A)(b) of the Payment Systems and Stored Value Facilities Ordinance, Cap. 584 (the PSSVFO).

2. Terms and abbreviations used in this Guideline shall be interpreted by reference to the definitions set out in the Glossary part of this Guideline. Interpretation of other words or phrases should follow those set out in the PSSVFO.

3. This Guideline is issued by the Hong Kong Monetary Authority (HKMA) for giving guidance to a stored value facility (SVF) licensee (which is not a licensed bank[1]) or a licensed bank (hereafter referred collectively as "SVF licensee") for the issue of an SVF.

4. Chapter 1 of this Guideline provides specific guidance on SVF and covers all core requirements that are applicable to SVF licensees. However, Chapter 1 is incomplete on its own and should be read in conjunction with Chapters 2-10 which provide more detailed requirements in some specific areas.[2] It should also be noted that Chapters 2-10 of this Guideline are not significantly different from the guidance provided by other relevant authorities[3] (RAs) for financial institutions[4] (FIs) under their respective regulatory regimes.

5. The Guideline is intended for use by SVF licensees and their officers and staff. The purposes of the Guideline are to:

   (a) provide a general background on the subjects of money laundering and terrorist financing (ML/TF), including a summary of the main provisions of the applicable anti-money laundering and counter-financing of terrorism (AML/CFT) legislation in Hong Kong; and
   (b) provide practical guidance to assist SVF licensees and their

[1] A licensed bank means a bank which holds a valid banking licence granted under section 16 of the Banking Ordinance.

[2] For example, while Chapter 1 specifies the high level requirement to conduct ongoing monitoring, Chapter 5 provides more details on that particular requirement.

[3] Relevant authorities include the HKMA (in relation to an authorized institution or an SVF licensee), Securities and Futures Commission (in relation to a licensed corporation), Insurance Authority (in relation to an authorized insurer, appointed insurance agent or authorized insurance broker) and Commissioner of Customs and Excise (in relation to a licensed money service operator or the Postmaster General).

[4] Financial institutions include an SVF licensee, an authorized institution, a licensed corporation, an authorized insurer, an appointed insurance agent, an authorized insurance broker, a licensed money service operator and the Postmaster General.

senior management in designing and implementing their own policies, procedures and controls in the relevant operational areas, taking into consideration their special circumstances so as to meet the relevant AML/CFT statutory and regulatory requirements.

6. The relevance and usefulness of the Guideline will be kept under review and it may be necessary to issue amendments from time to time.

7. The contents of the Guideline are neither intended to, nor should be construed as, an exhaustive list of the means of meeting the statutory and regulatory requirements.

8. This Guideline provides guidance in relation to the operation of the criteria set out in section 6 of Part 2 of Schedule 3 to the PSSVFO. This will assist SVF licensees to meet their legal and regulatory obligations. An SVF licensee must have in place adequate and appropriate systems of control to ensure that it complies with any rules, regulations or guidelines issued by the HKMA. Departures from this Guideline, and the rationale for so doing, should be documented, and SVF licensees will have to stand prepared to justify departures to the HKMA.

The nature of money laundering and terrorist financing

9. The term "money laundering" means an act intended to have the effect of making any property:

(a) that is the proceeds obtained from the commission of an indictable offence under the laws of Hong Kong, or of any conduct which if it had occurred in Hong Kong would constitute an indictable offence under the laws of Hong Kong; or
(b) that in whole or in part, directly or indirectly, represents such proceeds,

not to appear to be or so represent such proceeds.

10. There are three common stages in the laundering of money, and they frequently involve numerous transactions. An SVF licensee should be alert to any such sign for potential criminal activities. These stages are:

(a) Placement - the physical disposal of cash proceeds derived from illegal activities;
(b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail and

provide anonymity; and

(c) Integration - creating the impression of apparent legitimacy to criminally derived wealth. In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.

11. The term "terrorist financing" means:

(a) the provision or collection, by any means, directly or indirectly, of any property –
   (i) with the intention that the property be used; or
   (ii) knowing that the property will be used,
   in whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used);
(b) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate; or
(c) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate.

12. Terrorists or terrorist organisations require financial support in order to achieve their aims. There is often a need for them to obscure or disguise links between them and their funding sources. It follows then that terrorist groups must similarly find ways to launder funds, regardless of whether the funds are from a legitimate or illegitimate source, in order to be able to use them without attracting the attention of the authorities.

Legislation concerned with money laundering and terrorist financing

13. The Financial Action Task Force (the FATF) is an inter-governmental body formed in 1989 that sets the international anti-money laundering standards. Its mandate was expanded in October 2001 to combat the financing of terrorism. In order to ensure full and effective implementation of its standards at the global level, the FATF monitors compliance by conducting evaluations on jurisdictions and undertakes stringent follow-up after the evaluations, including identifying high-risk and uncooperative jurisdictions which could be subject to enhanced scrutiny by the FATF or counter-measures by the FATF members and the international community at large. Many major economies have joined the FATF which has developed into a global network for international cooperation that facilitates exchanges between member jurisdictions. As a member of the FATF, Hong Kong is

obliged to implement the AML/CFT requirements as promulgated by the FATF, which include the revised recommendations adopted in 2012 (hereafter referred to "FATF's Recommendations")[5] and it is important that Hong Kong complies with the international AML/CFT standards in order to maintain its status as an international financial centre.

14. The five main pieces of legislation in Hong Kong in relation to SVF licensees that are concerned with ML/TF are:

(a) the PSSVFO - dealing with preventive measures that should be implemented by SVF licensees;
(b) the Drug Trafficking (Recovery of Proceeds) Ordinance (the DTROP) and the Organized and Serious Crimes Ordinance (the OSCO) - dealing with serious or organised crime; and
(c) the United Nations (Anti-Terrorism Measures) Ordinance (the UNATMO) and the United Nations Sanctions Ordinance (the UNSO) - dealing with anti-terrorism or financial sanctions.

It is important that SVF licensees and their officers and staff fully understand their respective responsibilities under the different legislation.

PSSVFO

s.6, Part 2, Sch. 3, PSSVFO

15. The PSSVFO requires an SVF licensee to have in place adequate and appropriate systems of control for preventing or combating possible money laundering or terrorist financing and ensure that it complies with:

(a) the provisions of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (the AMLO) that are applicable to the SVF licensee; and
(b) the measures promulgated by the HKMA, whether in the form of rules, regulations, guidelines or otherwise, to prevent, combat or detect money laundering or terrorist financing.

s.33Q, PSSVFO

16. The HKMA may impose sanctions on an SVF licensee for any contravention of a provision, a requirement imposed or a condition attached to a licence under the PSSVFO. The sanctions that can be taken include:

(a) ordering the SVF licensee to pay a pecuniary penalty not exceeding the greater of HK$10 million or 3 times the amount of profit gained, or costs avoided, by the SVF

[5] The FATF's Recommendations can be found on the FATF website www.fatf-gafi.org.

licensee as a result of the contravention;

(b) giving the SVF licensee a caution, warning, reprimand and/or an order to take actions remedying the contravention by a certain date; and

(c) prohibiting the SVF licensee for a period of time or until the occurrence of an event specified by the HKMA from (i) making an application for a licence; (ii) giving a written notice stating that a person has become a controller of the SVF licensee; (iii) seeking a consent for a person to become chief executive or director of the SVF licensee; (iv) seeking a consent for certain persons to become employee of the SVF licensee.

s.8G & s.6, Part 2, Sch. 3, PSSVFO

17. Under section 8G of the PSSVFO, licensed banks are regarded as being granted a licence for the issue of SVF or facilitation of the issue of SVF and they are required to have adequate and appropriate systems of control for preventing or combating possible ML/TF under section 6, Part 2 of Schedule 3 to the PSSVFO. For the avoidance of doubt, the SVF products issued by licensed banks should be complied with the PSSVFO and this Guideline.

DTROP

18. The DTROP contains provisions for the investigation of assets that are suspected to be derived from drug trafficking activities, the freezing of assets on arrest and the confiscation of the proceeds from drug trafficking activities upon conviction.

OSCO

19. The OSCO, among other things:

(a) gives officers of the Hong Kong Police and the Customs and Excise Department powers to investigate organized crime and triad activities;

(b) gives the Courts jurisdiction to confiscate the proceeds of organized and serious crimes, to issue restraint orders and charging orders in relation to the property of a defendant of an offence specified in the OSCO;

(c) creates an offence of money laundering in relation to the proceeds of indictable offences; and

(d) enables the Courts, under appropriate circumstances, to receive information about an offender and an offence in order to determine whether the imposition of a greater sentence is appropriate where the offence amounts to an organized crime/triad related offence or other serious offences.

UNATMO

20. The UNATMO is principally directed towards implementing decisions contained in Resolution 1373 dated 28 September 2001 of the United Nations Security Council (the UNSC) aimed at preventing the financing of terrorist acts. Besides the mandatory elements of the United Nations Security Council Resolution (UNSCR) 1373, the UNATMO also implements the more pressing elements of the FATF's Recommendations on terrorist financing.

s.25, DTROP & OSCO

21. Under the DTROP and the OSCO, a person commits an offence if he deals with any property knowing or having reasonable grounds to believe it to represent any person's proceeds of drug trafficking or of an indictable offence respectively. The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine of HK$5 million.

s.6, 7, 8, 13 & 14, UNATMO

22. The UNATMO, among other things, criminalizes the provision or collection of property and making any property or financial (or related) services available to terrorists or terrorist associates. The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine. The UNATMO also permits terrorist property to be frozen and subsequently forfeited.

s.25A, DTROP & OSCO, s.12 & 14, UNATMO

23. The DTROP, the OSCO and the UNATMO also make it an offence if a person fails to disclose, as soon as it is reasonable for him to do so, his knowledge or suspicion of any property that directly or indirectly, represents a person's proceeds of, was used in connection with, or is intended to be used in connection with, drug trafficking, an indictable offence or is terrorist property respectively. This offence carries a maximum term of imprisonment of 3 months and a fine of HK$50,000 upon conviction.

s.25A, DTROP & OSCO, s.12 & 14, UNATMO

24. "Tipping off" is another offence under the DTROP, the OSCO and the UNATMO. A person commits an offence if, knowing or suspecting that a disclosure has been made, he discloses to any other person any matter which is likely to prejudice any investigation which might be conducted following that first-mentioned disclosure. The maximum penalty for the offence upon conviction is imprisonment for 3 years and a fine.

UNSO

25. The UNSO provides for the implementation of sanctions in Hong Kong that are imposed by the UNSC and to specify or designate relevant persons and entities. These sanctions, usually through enactment of regulations, normally prohibit making available or

dealing with, directly or indirectly, any funds or economic resources for the benefit of or belonging to a designated party.

Chapter 1 – STORED VALUE FACILITY

1.1 General

s.2A, PSSVFO

1.1.1 Section 2A of the PSSVFO states that a facility is an SVF if:

(a) it may be used for storing the value of an amount of money that –
  (i) is paid into the facility from time to time; and
  (ii) may be stored on the facility under the rules of the facility; and

(b) it may be used for either or both of the following purposes –
  (i) as a means of making payments for goods or services under an undertaking (whether express or implied) given by the issuer.

  That means an undertaking that, if the facility is used as a means of making payments for goods or services, the issuer, or a person procured by the issuer to accept such payments, will accept the payments up to the amount of the stored value that is available for use under the rules of the facility;

  (ii) as a means of making payments to another person (other than payments mentioned in sub-paragraph (i) above) under an undertaking (whether express or implied) given by the issuer.

  That means an undertaking that, if the facility is used as a means of making payments to another person (recipient) (other than payments mentioned in sub-paragraph (i) above), the issuer, or a person procured by the issuer to make such payments, will make the payments to the recipient up to the amount of the stored value that is available for use under the rules of the facility.

s.2A & Sch. 8, PSSVFO

1.1.2 However, a single-purpose SVF is not an SVF under the PSSVFO.

Some SVFs are exempted from the SVF licensing regime. These include:

(a) SVFs used for certain cash reward schemes;
(b) SVFs used for purchasing certain digital products;
(c) SVFs used for certain bonus point schemes;
(d) SVFs used within limited group of goods or services providers; and

(e) SVFs used within certain premises.

Please refer to Schedule 8 to the PSSVFO for details.

1.1.3 An SVF covers both device-based SVF and non-device based SVF (i.e. network-based SVF).

Device-based SVF is in the form of a physical device provided by the issuer to the user and the value is stored on the device. In general, for device-based SVF, the value is stored in an electronic chip on a card or physical device such as watches and ornaments.

For network-based SVF, the value is stored on the facility by using a communication network or system (whether the internet or any other network or system). It may include prepaid cards, internet payment systems and mobile payment systems.

1.2 Management oversight and internal controls

Senior management oversight

1.2.1 The senior management of an SVF licensee is responsible for managing its business effectively. Senior management should:

(a) be satisfied that the SVF licensee's AML/CFT systems are capable of addressing the ML/TF risks identified;
(b) appoint a director or senior manager as a Compliance Officer (CO) who has overall responsibility for the establishment and maintenance of the SVF licensee's AML/CFT systems;
(c) appoint a senior member of the SVF licensee's staff as the Money Laundering Reporting Officer (MLRO) who is the central reference point for suspicious transaction reporting; and
(d) establish (or designate an existing) board-level and/or management level committee that has the responsibility of oversight AML/CFT controls.

Compliance function and audit function

1.2.2 Where practicable, an SVF licensee should establish an independent compliance function and audit function with sufficient expertise and resources, which should have a direct reporting line to the senior management of the SVF licensee.

1.2.3 The compliance function and audit function of the SVF licensee should regularly review the AML/CFT systems to ensure effectiveness. The frequency and extent of the review should be commensurate with the ML/TF risks and the size of the SVF licensee's business.

1.2.4 Further details on the role of senior management, the function and roles of both the CO and MLRO as well as the compliance function and audit function can be found in Chapter 2 of this Guideline.

1.3 Risk-based approach

1.3.1 The risk-based approach (RBA) is recognized as an effective way to combat ML/TF. The use of an RBA has the advantage of allowing resources to be allocated in the most efficient way, directed in accordance with priorities, so that the greatest risks receive the highest attention.

1.3.2 Central to the proper application of an RBA is the expectation that an SVF licensee should identify, assess and understand the ML/TF risks to which they are exposed and take measures to manage and mitigate the identified risks. The identification of risk factors, which can differ significantly from one payment product or service to another, is essential to ensure that risk mitigating measures can be tailored to address the specific risk profile. Accordingly, SVF licensees are required to conduct assessment of ML/TF risks at both the business and customer levels.

Money laundering and terrorist financing risks related to SVF

1.3.3 An SVF is a retail payment product which is mainly used for paying or transferring small value payments. Typical products and services include stored value payment cards, online stored value payment facilities, mobile payment and internet payment services.

SVF is nevertheless vulnerable to similar ML/TF risks as other retail payment products and services and unless adequate and appropriate AML/CFT systems are applied, unacceptable ML/TF risks may arise. Effective and risk-based AML/CFT systems and controls, together with appropriate product control features can help mitigate these risks.

Several factors may reduce the attractiveness of SVF for money laundering, when compared with the privacy and anonymity of cash, including:

(a) where the SVF's product design is restricted to small payments;
(b) payments made through SVF products are a more accountable means of transferring money; and
(c) SVF products generally provide an electronic trail that can

be used to locate and/or identify the user, such as the product being funded from a bank account.

Risk factors

1.3.4 The risk of an SVF product will to a significant degree depend on its design, its functions and the mitigating measures applied. In assessing the risk of an SVF product, an SVF licensee may take into account the following risk factors:

(a) maximum stored value or transaction amount of the SVF – SVF products with higher transaction value or higher maximum stored value will increase the ML/TF risk;
(b) methods of funding – SVF products that allow funding by cash offer little or no audit trail which presents a higher ML/TF risk. On the other hand, funding by unverified parties or via other payment methods without customer identification can also create an anonymous funding mechanism and hence present higher ML/TF risks;
(c) cross-border usage – in general, SVF products with cross-border usage may increase the risk as transactions may be subject to different AML/CFT requirements and oversight in other jurisdictions and also give rise to difficulties with information sharing;
(d) person-to-person fund transfer function – an SVF product that allows person-to-person fund transfers may give rise to higher ML/TF risks;
(e) cash withdrawal function – an SVF product that allows access to cash for instance through automated teller machine (ATM) networks may increase the level of ML/TF risk;
(f) holding of multiple accounts/cards – SVF products that allow a customer to hold more than one account or card may also increase the ML/TF risk as it may be utilized by a third-party user other than the customer;
(g) multiple cards linked to the same account – SVF products that permit this functionality may present higher ML/TF risks, especially where the linked card is anonymous; and
(h) payment for high risk activities – some merchant activities, for example, gaming presents higher ML/TF risks.

Risk mitigating measures

1.3.5 The ML/TF risks of an SVF product can be reduced by implementing risk mitigating measures, which may include:

(a) the application of limits on the maximum storage values, cumulative turnover or transaction amounts;
(b) disallowing higher risk funding sources;
(c) restricting the SVF product being used for higher risk

activities;
(d) restricting higher risk functions such as cash access; and
(e) implementing measures to detect multiple SVF accounts/cards held by the same customer or group of customers.

Moreover, the SVF licensee should put in place systems and controls that can detect unusual transactions and predetermined patterns of activity for further investigation. The detailed requirements are specified under Chapter 5 of this Guideline.

1.3.6 The level of ML/TF risk posed by a particular SVF product will depend on a consideration of all risk factors, the existence of risk mitigating measures and its functionality.[6]

Customer risk assessment

1.3.7 An SVF licensee should assess whether an individual customer presents a higher ML/TF risk and assign a ML/TF risk rating.

1.3.8 Generally, the customer risk assessment will be based on the information collected during the identification stage. For lower risk products, this may be comparatively simple; there is no general expectation that additional information should be obtained to fulfil this requirement. It is also worth noting that risks for some customers may become evident only when the customer has commenced using the SVF product through ongoing monitoring and an SVF licensee should adjust its risk assessment of a particular customer from time to time based upon any additional information.

1.3.9 Further details of RBA may be found in Chapter 3 of this Guideline.

1.4 Streamlined customer due diligence for SVF

1.4.1 Taking into account the lower level of ML/TF risks of some SVF products, streamlined customer due diligence (streamlined approach) is allowed which permits certain due diligence measures to be performed in a particular manner or not performed under certain scenarios. However, there is no exemption from the requirement to continuously monitor the business relationship.

1.4.2 In order to apply the streamlined approach, SVF licensees should ensure that the SVF product meets specific requirements on stored value, transaction limits and cash withdrawal function.

[6] SVF licensees may make reference to the "Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services" issued by the FATF in June 2013.

1.4.3 The limits specified under the streamlined approach from paragraphs 1.4.6 to 1.4.21 represent maximum limits which in general, SVF licensees may adopt, subject to the establishment of adequate internal controls. However, SVF licensees may choose to adopt lower limits based on their own assessment of risks. Equally, the HKMA may, based on its own assessment of the risks and adequacy of internal controls, require SVF licensees to observe lower limits as part of the licensing conditions.

1.4.4 The HKMA may also, where adequate justification exists, vary the control measure(s) which may be applicable to an SVF licensee. For examples, if higher ML/TF risks are identified, the HKMA may impose additional risk mitigating measures on the SVF licensee concerned through imposing conditions on its licence.

1.4.5 A table of limits for conducting customer due diligence (CDD) for SVF products could be found in Appendix A. The table should be read in conjunction with paragraphs 1.4.6 to 1.4.21.

Device-based SVF

1.4.6 Provided that the maximum stored value of a device-based SVF does not exceed HK$3,000, based on the low level of money laundering risk, in general there is no requirement to conduct any due diligence on the customer. However, depending on the product features (e.g. person-to-person fund transfer, cash withdrawal function), the HKMA may impose additional risk mitigating measures on the SVF licensee.

1.4.7 For a device-based SVF with maximum stored value exceeding HK$3,000, normal CDD requirements as set out in Chapter 4 of this Guideline should be applied.

Network-based SVF

Non-reloadable network-based SVF

1.4.8 Non-reloadable network-based SVF commonly take the form of prepaid cards or gift cards which may be used to make payments for goods or services. Based on the design and application of the card they may also be used to withdraw cash from ATMs. The value is stored in an account on a server and not on the card itself.

1.4.9 Provided that the maximum stored value of a non-reloadable network-based SVF does not exceed HK$8,000, in general there is no requirement to conduct any due diligence on the customer. However, depending on the product features (e.g. person-to-

person fund transfer, cash withdrawal function), the HKMA may impose additional risk mitigating measures on the SVF licensee.

1.4.10 Additionally, for non-reloadable network-based SVFs with stored value not exceeding HK$8,000, if purchases of multiple SVFs at one time are allowed and the total value of multiple SVFs purchased at one time exceeds HK$25,000, the customer should be identified and verified in accordance with paragraph 4.2.1 of Chapter 4 of this Guideline. The relevant identification information is specified in paragraph 4.8.1 for an individual customer (and that of any beneficial owner, where applicable), paragraph 4.9.7 for a corporate customer and paragraph 4.9.22 for a partnership or an unincorporated body.

1.4.11 Where the stored value of a non-reloadable network-based SVF exceeds HK$8,000, the customer should be identified and verified in accordance with paragraph 4.2.1 of Chapter 4 of this Guideline.

Reloadable network-based SVF

1.4.12 Reloadable network-based SVF includes internet-based payment platforms which provide "network-based accounts" with which users can store monetary value for making payments for online purchases or for person-to-person fund transfers.

No cash withdrawal function

1.4.13 Where the annual transaction amount for a reloadable network-based SVF does not exceed HK$25,000 and there is no ability to withdraw cash:

(a) the customer (and any beneficial owner, where applicable) should be identified on the basis of the information provided by the customer (i.e. reliance may be placed on the customer's statement). In practice, this means that the SVF licensee is required to collect the customer's identification information as specified under paragraph 4.8.1 for an individual customer (and that of any beneficial owner, where applicable), paragraph 4.9.7 for a corporate customer and paragraph 4.9.22 for a partnership or an unincorporated body;

(b) however, for SVF with low maximum stored value not exceeding HK$3,000[7], there is no requirement to collect the customer's identification information as specified under paragraph 1.4.13(a) above.

[7] The HKMA may, on an exceptional basis and based on the functionalities and related risk mitigating measures of each SVF product, impose a higher or lower maximum stored value.

1.4.14 Where the annual transaction amount for a reloadable network-based SVF exceeds HK$25,000 but does not exceed HK$100,000, the customer (and any beneficial owner, where applicable) should be identified and verified.

1.4.15 This means that if the customer's identification information has not been collected pursuant to paragraph 1.4.13(a) above, the SVF licensee is required to identify the customer (and any beneficial owner, where applicable) by collecting the customer's (and any beneficial owner's, where applicable) identification information. The SVF licensee may verify the customer's identity by (i) means of linkage with the customer's account in a licensed bank or customer's credit card issued by an authorized institution[8] (AI) or an AI's subsidiary; or (ii) obtaining a copy of the customer's identification document (whether in person or through electronic means).

1.4.16 To meet the requirement of verifying the customer's identity by means of linkage with the customer's account or credit card, an SVF licensee should have procedures in place to ensure that a payment made into the customer's SVF account is from an account or a credit card under the same name as its customer.

1.4.17 Where the SVF licensee is unable to verify that the names are the same, the SVF licensee may develop a means of establishing control over the account or the credit card using a process that is convenient and effective.

1.4.18 Where the SVF licensee verifies the customer's identity by obtaining a copy of the customer's identification document, it should verify the customer's identification information obtained under paragraph 1.4.13(a) by reference to documents, data or information provided by a reliable and independent source (as specified under paragraph 4.2.1). Paragraphs 4.8 and 4.9 provide further guidance on verifying the identity of natural persons and legal persons.

1.4.19 Where the annual transaction amount for a reloadable network-based SVF exceeds HK$100,000, normal CDD requirements as set out in Chapter 4 of this Guideline should be applied.

[8] An authorized institution means (i) a licensed bank; (ii) a restricted licence bank; or (iii) a deposit-taking company under the Banking Ordinance.

Cash withdrawal function

1.4.20 Where a reloadable network-based SVF allows cash withdrawal[9], the ML/TF risks may increase and the customer's identity should be verified, at the outset of the business relationship by (i) means of linkage with the customer's account in a licensed bank or the customer's credit card issued by an AI or an AI's subsidiary; or (ii) obtaining a copy of the customer's identification document.

1.4.21 Where the annual transaction amount of cash withdrawal for a customer exceeds HK$8,000, normal CDD requirements as set out in Chapter 4 of this Guideline should be applied.

Internal controls for applying streamlined approach

1.4.22 An SVF licensee applying the streamlined approach should have in place appropriate systems and controls to ensure compliance with the relevant limits as specified under paragraphs 1.4.6 to 1.4.21. For instance, the SVF licensee may have a system to detect when a customer is approaching the limits and alert the customer of the required CDD measures. Where there is an obligation to undertake certain CDD measures upon certain limits being exceeded and this cannot be fulfilled, the SVF licensee should freeze the account until the required CDD procedures are completed.

1.4.23 The SVF licensee should establish an appropriate system and method to calculate the annual transaction amount.

1.4.24 Where appropriate internal controls could not be implemented to ensure compliance with the limits, SVF licensees are not permitted to adopt a streamlined approach and should conduct the normal CDD requirements set out in Chapter 4 of this Guideline at the outset of the business relationship.

1.4.25 In addition, a streamlined approach should not be adopted where an SVF licensee:

(a) has knowledge or a suspicion of ML/TF;
(b) becomes aware of anything which causes doubt as to the identity or intentions of the customer or beneficial owner; or
(c) the business relationship is assessed to pose a higher ML/TF risk.

[9] Cash withdrawal function includes cash withdrawal through the ATM networks or by overpaying purchased merchandise and receiving the overpaid amount in cash (i.e. cash-back). For avoidance of doubt, the SVF licensees may allow cash redemption due to cancellation or termination of an SVF product. However, where cash redemption due to cancellation or termination of an SVF product exceeds HK$8,000, the SVF licensee should identify and verify the customer's identity and retain a copy of the customer's identification document.

Under such situations, the SVF licensee must carry out the normal CDD and enhanced customer due diligence (EDD) requirements as specified in Chapter 4 of this Guideline.

1.4.26 The risk of ML for some SVF products may not be high and therefore the requirement to implement systems to identify customers who are politically exposed persons (PEPs) should be risk-based, taking into account the ML risks presented. When a customer is identified as a PEP, EDD requirements should be applied, but SVF licensees can adjust the extent of these measures on a risk-sensitive basis[10].

Multiple accesses of SVF product

1.4.27 Based on the product design and operational need, some SVF products may allow multiple accesses, for example, two or more cards/accounts could be held by the same customer or where the customer can access an SVF account through different mobile devices. The SVF licensee should be aware that under such circumstances, the SVF product may be utilized by a third-party user other than the customer. Where the SVF licensee enables multiple accesses to the customer's SVF account, the SVF licensee should determine whether this leads to the establishment of a business relationship with each user, whether the issue of beneficial ownership arises and whether applicable CDD requirements apply.

1.4.28 Where multiple accesses do not give rise to a separate business relationship nor beneficial ownership concerns, SVF licensees should nevertheless adequately assess the risks involved, justify the reasons for allowing such function, set proper maximum numbers of cards/accounts and implement effective controls to mitigate the higher ML/TF risks which may arise. Nevertheless, the total transactions undertaken by a customer should be calculated on the basis of the aggregate of transactions conducted through all cards or accounts held by the same customer.

1.5 Ongoing monitoring

1.5.1 Effective ongoing monitoring is vital for understanding of customers' activities and is an integral part of effective AML/CFT systems. It helps an SVF licensee to know its customers and to detect unusual or suspicious activities.

1.5.2 Although the SVF licensees are allowed to apply a streamlined approach in identifying and verifying the customer's identity,

[10] Further details can be found in Chapter 4 of this Guideline.

there is no exemption from the requirement to monitor the business relationship on an ongoing basis. Appropriate and risk-based policies and procedures that are commensurate with the business size and level of ML/TF risk of the SVF licensee should therefore be maintained to monitor business relationships on an ongoing basis.

1.5.3 Further guidance on ongoing monitoring may be found in Chapter 5 of this Guideline.

1.6 Financial sanctions and terrorist financing

1.6.1 The obligations under the Hong Kong's financial sanctions regime apply to all persons including SVF licensees. Accordingly, an SVF licensee should ensure that appropriate systems and controls are in place to meet these obligations.

1.6.2 These sanctions normally prohibit making available or dealing with, directly or indirectly, any funds or economic resources for the benefit of or belonging to a designated party.

1.6.3 The HKMA will circulate the designations published in the government Gazette under the UNSO and the UNATMO to all SVF licensees.

1.6.4 An SVF licensee should ensure that the system conducts checks against the relevant lists for screening purposes based on up-to-date information concerning designated parties.

1.6.5 Further details on financial sanctions and terrorist financing can be found in Chapter 6 of this Guideline.

1.7 Suspicious transaction reports

1.7.1 Sections 25A of the DTROP and the OSCO make it an offence to fail to disclose where a person knows or suspects that property represents the proceeds of drug trafficking or of an indictable offence respectively. Likewise, section 12 of the UNATMO makes it an offence to fail to disclose knowledge or suspicion of terrorist property.

1.7.2 When an SVF licensee knows or suspects that property represents the proceeds of crime or terrorist property, a disclosure must be made to the Joint Financial Intelligence Unit (JFIU) as soon as it is reasonable to do so.

1.7.3 An SVF licensee must ensure that adequate systems and controls are in place to discharge this legal obligation, which should include internal reporting, analysis and recording processes to

manage alerts generated by the monitoring system, guidance to key staff such as the MLRO regarding the actual making of suspicious transaction reports (STRs) and the information to be included and actions which should be undertaken upon the filing of an STR with the JFIU, including escalation processes.

1.7.4 Further details on STRs can be found in Chapter 7 of this Guideline and the "Guidance Paper on Transaction Screening, Transaction Monitoring and Suspicious Transaction Reporting" issued by the HKMA on 16 December 2013.

1.8 Record-keeping

1.8.1 Record-keeping is an essential part of the audit trail for the detection, investigation and confiscation of criminal or terrorist property or funds. Record-keeping helps the investigating authorities to establish a financial profile of a suspect, trace the criminal or terrorist property or funds and assists the Court to examine all relevant past transactions to assess whether the property or funds are the proceeds of or relate to criminal or terrorist offences.

1.8.2 An SVF licensee should maintain customer records throughout the business relationship with the customers and for a period of six years after the end of the business relationship and transaction records for a period of six years after the completion of a transaction.

1.8.3 Further details on record-keeping can be found in Chapter 8 of this Guideline.

1.9 Staff training

1.9.1 An SVF licensee should provide appropriate and regular AML/CFT training to its staff. The frequency of training should be sufficient to maintain the AML/CFT knowledge and competence of the staff.

1.9.2 Further details on staff training can be found in Chapter 9 of this Guideline.

1.10 Wire transfers

1.10.1 An SVF licensee should ensure that any transaction falls within the definition of a wire transfer in an amount equal to or exceeding HK$8,000, the requirements for wire transfers in Chapter 10 of this Guideline should be complied with.

1.11 Ancillary service to an SVF licensee's principal business

1.11.1 While the principal business of an SVF licensee must be the issue of SVF or the facilitation of the issue of SVF, an SVF licensee may operate money service business (i.e. money changing service or remittance service) that are ancillary to its principal business. In conducting money service business, the SVF licensee should comply with the relevant requirements stipulated in the Guideline on Anti-Money Laundering and Counter-Terrorist Financing (For Money Service Operators) [11], and the key requirements are provided below.

Money changing service

1.11.2 An SVF licensee that operates a money changing service[12] that is ancillary to its principal business should before performing any money changing transactions equal to or exceeding an aggregate value of HK$120,000, whether carried out in a single operation or several operations that appear to the SVF licensee to be linked, conduct normal CDD as set out in Chapter 4 of this Guideline.

Remittance service

1.11.3 An SVF licensee that operates a remittance service that is ancillary to its principal business should before carrying out a remittance transaction[13], other than a wire transfer, of HK$8,000 or above or of an equivalent amount in any other currency:

(a) identify the originator;
(b) verify the identity of the originator by reference to the originator's identification document; and
(c) record (i) the originator's name; (ii) the originator's identification document number and, if the originator's identification document is a travel document, the place of issue of the travel document; (iii) the originator's address; (iv) the currency and amount involved; and (v) the date and time of receipt of the instruction, the recipient's name and address and the method of delivery.

1.11.4 An originator of a remittance transaction is:

[11] The Guideline on Anti-Money Laundering and Counter-Terrorist Financing (For Money Service Operators) can be found on the Customs and Excise Department's website (www.customs.gov.hk).

[12] Money changing service means a service for the exchanging of currencies that is operated in Hong Kong as a business, but does not include such a service that is operated by a person who manages a hotel if the service (a) is operated within the premises of the hotel primarily for the convenience of guests of the hotel; and (b) consists solely of transactions for the purchase by that person of non-Hong Kong currencies in exchange for Hong Kong currency.

[13] A remittance transaction means a transaction for sending, or arranging for the sending of, money to a place outside Hong Kong.

(a) the person from whose account with the SVF licensee the money for the remittance is paid; or
(b) in the absence of such an account, the person who instructs the SVF licensee to carry out the remittance transaction.

Chapter 2 – AML/CFT SYSTEMS AND BUSINESS CONDUCTED OUTSIDE HONG KONG

AML/CFT systems

s.6, Part 2, Sch. 3, PSSVFO

2.1 SVF licensees must put in place adequate and appropriate systems of control for preventing or combating possible ML/TF. To ensure compliance with this requirement, SVF licensees should implement appropriate internal AML/CFT policies, procedures and controls (hereafter collectively referred to as "AML/CFT systems").

Risk factors

2.2 While no system will detect and prevent all ML/TF activities, SVF licensees should establish and implement adequate and appropriate AML/CFT systems (including customer acceptance policies and procedures) taking into account factors including products and services offered, types of customers, geographical locations involved.

Product/service risk

2.3 An SVF licensee should consider the characteristics of the products and services that it offers and the extent to which these are vulnerable to ML/TF abuse. In this connection, an SVF licensee should assess the risks of any new products and services (especially those that may lead to misuse of technological developments or facilitate anonymity in ML/TF schemes) before they are introduced and ensure appropriate additional measures and controls are implemented to mitigate and manage the associated ML/TF risks.

Delivery/distribution channel risk

2.4 An SVF licensee should also consider its delivery/distribution channels and the extent to which these are vulnerable to ML/TF abuse. These may include sales through online, postal or telephone channels where a non-face-to-face account opening approach is used. Business sold through intermediaries may also increase risk as the business relationship between the customer and an SVF licensee may become indirect.

Customer risk

2.5 When assessing the customer risk, SVF licensees should consider who their customers are and any other information that may suggest the customer is of higher risk.

Country risk

2.6 An SVF licensee should pay particular attention to countries or geographical locations of operation with which its customers and intermediaries are connected where they are subject to high levels of organized crime, increased vulnerabilities to corruption and inadequate systems to prevent and detect ML/TF. When assessing which countries are more vulnerable to corruption, SVF licensees may make reference to publicly available information or relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations (an example of which is Transparency International's "Corruption Perceptions Index", which ranks countries according to their perceived level of corruption).

Effective controls

2.7 To ensure proper implementation of such policies and procedures, SVF licensees should have effective controls covering:

(a) senior management oversight;
(b) appointment of a CO and a MLRO[14];
(c) compliance function and audit function; and
(d) staff screening and training[15].

Senior management oversight

2.8 The senior management of any SVF licensee is responsible for managing its business effectively; in relation to AML/CFT this includes oversight of the functions described below.

2.9 Senior management should:

(a) be satisfied that the SVF licensee's AML/CFT systems are capable of addressing the ML/TF risks identified;
(b) appoint a director or senior manager as a CO who has overall responsibility for the establishment and maintenance of the SVF licensee's AML/CFT systems; and
(c) appoint a senior member of the SVF licensee's staff as the MLRO who is the central reference point for suspicious transaction reporting.

2.10 In order that the CO and MLRO can discharge their responsibilities effectively, senior management should, as far as practicable, ensure that the CO and MLRO are:

[14] The role and functions of an MLRO are detailed at paragraphs 7.19-7.30. For some SVF licensees, the functions of the CO and the MLRO may be performed by the same staff member.
[15] For further guidance on staff training see Chapter 9.

(a) subject to constraint of size of the SVF licensee, independent of all operational and business functions;
(b) normally based in Hong Kong;
(c) of a sufficient level of seniority and authority within the SVF licensee;
(d) provided with regular contact with, and when required, direct access to senior management to ensure that senior management is able to satisfy itself that the statutory obligations are being met and that the business is taking sufficiently robust measures to protect itself against the risks of ML/TF;
(e) fully conversant in the SVF licensee's statutory and regulatory requirements and the ML/TF risks arising from the SVF licensee's business;
(f) capable of accessing, on a timely basis, all available information (both from internal sources such as CDD records and external sources such as circulars from the HKMA); and
(g) equipped with sufficient resources, including staff and appropriate cover for the absence of the CO and MLRO (i.e. an alternate or deputy CO and MLRO who should, where practicable, have the same status).

Compliance officer and money laundering reporting officer

2.11 The principal function of the CO is to act as the focal point within an SVF licensee for the oversight of all activities relating to the prevention and detection of ML/TF and providing support and guidance to the senior management to ensure that ML/TF risks are adequately managed. In particular, the CO should assume responsibility for:

(a) developing and/or continuously reviewing the SVF licensee's AML/CFT systems to ensure they remain up-to-date and meet current statutory and regulatory requirements; and
(b) the oversight of all aspects of the SVF licensee's AML/CFT systems which include monitoring effectiveness and enhancing the controls and procedures where necessary.

2.12 In order to effectively discharge these responsibilities, a number of areas should be considered. These include:

(a) the means by which the AML/CFT systems are managed and tested;
(b) the identification and rectification of deficiencies in the AML/CFT systems;
(c) reporting numbers within the systems, both internally and disclosures to the JFIU;
(d) the mitigation of ML/TF risks arising from business

relationships and transactions with persons from countries which do not or insufficiently apply the FATF's Recommendations;

(e) the communication of key AML/CFT issues with senior management, including, where appropriate, significant compliance deficiencies;
(f) changes made or proposed in respect of new legislation, regulatory requirements or guidance;
(g) compliance with any requirement under this Guideline in overseas branches and subsidiary undertakings and any guidance issued by the HKMA in this respect; and
(h) AML/CFT staff training.

2.13 The MLRO should play an active role in the identification and reporting of suspicious transactions. Principal functions performed are expected to include:

(a) reviewing all internal disclosures and exception reports and, in light of all available relevant information, determining whether or not it is necessary to make a report to the JFIU;
(b) maintaining all records related to such internal reviews;
(c) providing guidance on how to avoid "tipping off" if any disclosure is made; and
(d) acting as the main point of contact with the JFIU, law enforcement, and any other competent authorities in relation to ML/TF prevention and detection, investigation or compliance.

Compliance function and audit function

2.14 Where practicable, an SVF licensee should establish an independent compliance function and audit function which should have a direct line of communication to the senior management of the SVF licensee.

2.15 The compliance function and audit function of the SVF licensee should regularly review the AML/CFT systems, e.g. sample testing, (in particular, the system for recognizing and reporting suspicious transactions) to ensure effectiveness. The frequency and extent of the review should be commensurate with the risks of ML/TF and the size of the SVF licensee's business. Where appropriate, the SVF licensee should seek a review from external sources.

2.16 Internal audit has an important role to play in independently evaluating on a periodic basis an SVF licensee's policies and procedures on anti-money laundering. This should include checking the effectiveness of the compliance function, the adequacy of MIS reports of large or irregular transactions and the

quality of reporting of suspicious transactions. The level of awareness of front line staff of their responsibilities in relation to the prevention of money laundering should also be reviewed. The internal audit function should have sufficient expertise and resources to enable it to carry out its responsibilities.

Staff screening

2.17 SVF licensees must establish, maintain and operate appropriate procedures in order to be satisfied of the integrity of any new employees.

Business conducted outside Hong Kong

2.18 An SVF licensee with overseas branches or subsidiary undertakings should put in place a group AML/CFT policy to ensure that all branches and subsidiary undertakings that carry on the same business as an SVF licensee in a place outside Hong Kong have procedures in place to comply with the CDD and record-keeping requirements similar to those set out in this Guideline to the extent permitted by the law of that place. The SVF licensee should communicate the group policy to its overseas branches and subsidiary undertakings.

2.19 When a branch or subsidiary undertaking of an SVF licensee outside Hong Kong is unable to comply with requirements that are similar to those set out in this Guideline because this is not permitted by local laws, the SVF licensee must:

(a) inform the HKMA of such failure; and
(b) take additional measures to effectively mitigate ML/TF risks faced by the branch or subsidiary undertaking as a result of its inability to comply with the above requirements.

s.25A, OSCO & DTROP

2.20 Suspicion that property in whole, or partly directly or indirectly represents the proceeds of an indictable offence, should normally be reported within the jurisdiction where the suspicion arises and where the records of the related transactions are held. However, in certain cases, e.g. when the account is domiciled in Hong Kong, reporting to the JFIU [16] may be required in such circumstances, but only if section 25A of OSCO/DTROP applies.

[16] Section 25(4) of the OSCO stipulates that an indictable offence includes conduct outside Hong Kong which would constitute an indictable offence if it had occurred in Hong Kong. Therefore, where an SVF licensee in Hong Kong has information regarding money laundering, irrespective of the location, it should consider seeking clarification with and making a report to the JFIU.

Chapter 3 – RISK-BASED APPROACH

Introduction

3.1 The RBA is recognized as an effective way to combat ML/TF. The general principle of an RBA is that where customers are assessed to be of higher ML/TF risks, SVF licensees should take enhanced measures to manage and mitigate those risks, and that correspondingly where the risks are lower, simplified measures may be applied.

The use of an RBA has the advantage of allowing resources to be allocated in the most efficient way directed in accordance with priorities so that the greatest risks receive the highest attention.

General requirement

3.2 SVF licensees should determine the extent of CDD measures and ongoing monitoring, using an RBA depending upon the background of the customer and the product, transaction or service used by that customer, so that preventive or mitigating measures are commensurate to the risks identified. The measures must however comply with the requirements set out in this Guideline.

The RBA will enable SVF licensees to subject customers to proportionate controls and oversight by determining:

(a) the extent of the due diligence to be performed;
(b) the level of ongoing monitoring to be applied to the relationship; and
(c) measures to mitigate any risks identified.

3.3 There are no universally accepted methodologies that prescribe the nature and extent of an RBA. However, an effective RBA does involve identifying and categorizing ML/TF risks at the customer level and establishing reasonable measures based on risks identified. An effective RBA will allow SVF licensees to exercise reasonable business judgment with respect to their customers.

An RBA should not be designed to prohibit SVF licensees from engaging in transactions with customers or establishing business relationships with potential customers, but rather it should assist SVF licensees to effectively manage potential ML/TF risks.

Institutional risk assessment

3.4 The ML/TF risk assessment forms the basis of the RBA, enabling

the SVF licensee to understand how, and to what extent it is vulnerable to ML/TF, deciding the most appropriate and effective way to mitigate the identified risks, and the way to manage any resulting residual risk according to the SVF licensee's risk appetite. The successful implementation and effective operation of an RBA to AML/CFT hinges on strong senior management leadership and oversight of the development and implementation of the RBA across the SVF licensee's business operation. Senior management should not only know about the ML/TF risks to which the SVF licensee is exposed, but also understand how its AML/CFT control framework operates to mitigate those risks.

3.5 All SVF licensees should take appropriate steps to identify, assess and understand their ML/TF risks in relation to

(a) their customers;
(b) the countries or jurisdictions their customers are from or in;
(c) the countries or jurisdictions the SVF licensees have operations in, if any; and
(d) the products, services, transactions and delivery channels of the SVF licensees.

3.6 In practice, an SVF licensee should:

(a) document the risk assessment process which includes the identification and assessment of relevant risks, supported by qualitative and quantitative analysis and information obtained from relevant internal and external sources;
(b) consider all the relevant risks factors before determining what the level of overall risk is and the appropriate level and type of mitigation to be applied;
(c) obtain the approval of senior management on the assessment results;
(d) have a process by which the risk assessment is kept up-to-date; and
(e) have appropriate mechanisms to provide its risk assessment to the HKMA when required to do so.

3.7 The complexity of the ML/TF risk assessment should be commensurate with the nature and size of the SVF licensee's business. For larger or complex SVF licensees (e.g. where SVF licensees offer different SVF products, or SVF products with various functions such as cross-border usage), a more sophisticated risk assessment may be required. For smaller or less complex SVF licensees (e.g. where SVF licensee offers the products mainly for small amount purchases and usage is limited to domestic only), a less sophisticated ML/TF risk assessment may suffice.

Customer acceptance/risk assessment

3.8 SVF licensee may assess the ML/TF risks of individual customers and assign a ML/TF risk rating to their customers.

3.9 While there is no agreed upon set of risk factors and no one single methodology to apply these risk factors in determining the ML/TF risk rating of customers, relevant factors to be considered may include the following:

1. Country risk

Customers with residence in or connection with high-risk jurisdictions[17] for example:

(a) those that have been identified by the FATF as jurisdictions with strategic AML/CFT deficiencies;
(b) countries subject to sanctions, embargos or similar measures issued by relevant organisations such as the United Nations (the UN);
(c) countries which are vulnerable to corruption; and
(d) those countries that are believed to have strong links to terrorist activities.

In assessing country risk associated with a customer, consideration may be given to local legislation (UNSO, UNATMO), data available from the UN, the International Monetary Fund, the World Bank, the FATF, etc. and the SVF licensee's own experience or the experience of other group entities (where the SVF licensee is part of a multi-national group) which may have indicated weaknesses in other jurisdictions.

2. Customer risk

Some customers, by their nature or behaviour might present a higher risk of ML/TF. Factors might include:

(a) the public profile of the customer indicating involvement with, or connection to, PEPs;
(b) nature, scope and location of business activities generating the funds/assets (e.g. merchants), having regard to sensitive or high-risk activities; and
(c) where the ownership cannot be easily verified.

[17] Guidance on jurisdictions that do not or insufficiently apply the FATF's Recommendations or otherwise pose a higher risk is provided at paragraphs 4.14.

3. Product/service risk

Factors presenting higher risk might include:

(a) high limit on the maximum stored value or maximum transaction amount of the SVF product; and
(b) using the SVF product for payments for high risk activities.

More risk factors are specified in paragraph 1.3.4.

4. Delivery/distribution channel risk

The distribution channel for products may alter the risk profile of a customer. This may include sales through online, postal or telephone channels where a non-face-to-face account opening approach is used. Business sold through intermediaries may also increase risk as the business relationship between the customer and an SVF licensee may become indirect.

Ongoing review

3.10 An SVF licensee may have to adjust its risk assessment of a particular customer from time to time or based upon information received from a competent authority, and review the extent of the CDD and ongoing monitoring to be applied to the customer.

3.11 SVF licensees should keep its policies and procedures under regular review and assess that its risk mitigation procedures and controls are working effectively.

Documenting risk assessment

3.12 An SVF licensee should keep records and relevant documents of the risk assessment covered in this Chapter so that it can demonstrate to the HKMA, among others:

(a) how it assesses the customer's ML/TF risk; and
(b) the extent of CDD and ongoing monitoring is appropriate based on that customer's ML/TF risk.

Chapter 4 – CUSTOMER DUE DILIGENCE

4.1 Introduction to CDD

4.1.1 This Chapter defines what CDD measures are (see paragraph 4.1.3) and also prescribes the circumstances in which an SVF licensee must carry out CDD (see paragraph 4.1.9). As indicated in this Chapter, SVF licensees may also need to conduct additional measures (referred to as enhanced customer due diligence (EDD) hereafter) or could conduct simplified customer due diligence (SDD) depending on specific circumstances. This Chapter sets out the expectations of the HKMA in this regard and suggests ways that these expectations may be met. Wherever possible, the guideline gives SVF licensees a degree of discretion on how they comply with the PSSVFO and put in place procedures for this purpose.

4.1.2 CDD information is a vital tool for recognising whether there are grounds for knowledge or suspicion of ML/TF.

4.1.3 The following are CDD measures applicable to an SVF licensee:

(a) identify the customer and verify the customer's identity using reliable, independent source documents, data or information (see paragraph 4.2.1);
(b) where there is a beneficial owner in relation to the customer, identify and take reasonable measures to verify the beneficial owner's identity so that the SVF licensee is satisfied that it knows who the beneficial owner is, including in the case of a legal person or trust[18], measures to enable the SVF licensee to understand the ownership and control structure of the legal person or trust (see paragraphs 4.3);
(c) obtain information on the purpose and intended nature of the business relationship (if any) established with the SVF licensee unless the purpose and intended nature are obvious (see paragraphs 4.6); and
(d) if a person purports to act on behalf of the customer:
    (i) identify the person and take reasonable measures to verify the person's identity using reliable and independent source documents, data or information; and
    (ii) verify the person's authority to act on behalf of the customer (see paragraphs 4.4).

4.1.4 The term "customer" is not defined in the PSSVFO. Its meaning should be inferred from its everyday meaning and in the context of the industry practice.

[18] For the purpose of this guideline, a trust means an express trust or any similar arrangement for which a legal-binding document (i.e. a trust deed or in any other forms) is in place.

4.1.5 In general, the term "customer" refers to the party, or parties, with whom a business relationship is established, or for whom a transaction is carried out by an SVF licensee.

4.1.6 In determining what constitutes reasonable measures to verify the identity of a beneficial owner and reasonable measures to understand the ownership and control structure of a legal person or trust, the SVF licensee should consider and give due regard to the ML/TF risks posed by a particular customer and a particular business relationship. Due consideration should also be given to the measures set out in Chapter 3.

4.1.7 SVF licensees should adopt a balanced and common sense approach with regard to customers connected with jurisdictions which do not or insufficiently apply the FATF's Recommendations (see paragraphs 4.14). While extra care may well be justified in such cases, it is not a requirement that SVF licensees should refuse to do any business with such customers or automatically classify them as high risk and subject them to EDD process. Rather, SVF licensees should weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of ML/TF.

4.1.8 "Business relationship" between a person and an SVF licensee is defined as a business, professional or commercial relationship:

(a) that has an element of duration; or
(b) that the SVF licensee, at the time the person first contacts it in the person's capacity as a potential customer of the SVF licensee, expects to have an element of duration.

4.1.9 CDD requirements should apply:

(a) at the outset of a business relationship (where the adoption of the streamlined approach does not apply) or;
(b) for the continuation of a business relationship where the limits, which apply to the use of the streamlined approach are exceeded;
(c) when the SVF licensee suspects that the customer or the customer's account is involved in ML/TF; or
(d) when the SVF licensee doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.

4.2 Identification and verification of the customer's identity

4.2.1 The SVF licensee must identify the customer and verify the

customer's identity by reference to documents, data or information provided by a reliable and independent source[19]:

(a) a governmental body;
(b) the HKMA or any other RA;
(c) an authority in a place outside Hong Kong that performs functions similar to those of the HKMA or any other RA; or
(d) any other reliable and independent source that is recognized by the HKMA.

4.3 Identification and verification of a beneficial owner

4.3.1 A beneficial owner is normally an individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. In respect of a customer who is an individual not acting in an official capacity on behalf of a legal person or trust, the customer himself is normally the beneficial owner. There is no requirement on SVF licensees to make proactive searches for beneficial owners in such a case, but they should make appropriate enquiries where there are indications that the customer is not acting on his own behalf.

4.3.2 Where an individual is identified as a beneficial owner, the SVF licensee should endeavour to obtain the same identification information as at paragraph 4.8.1.

4.3.3 The verification requirements are, however, different for a customer and a beneficial owner.

4.3.4 The obligation to verify the identity of a beneficial owner is for the SVF licensee to take reasonable measures, based on its assessment of the ML/TF risks, so that it is satisfied that it knows who the beneficial owner is.

4.3.5 SVF licensees should identify all beneficial owners of a customer. In relation to verification of beneficial owners' identities, except where a situation is assessed to be of high ML/TF risk (including those situations specified under paragraphs 4.11, 4.13, 4.14 and 4.16), SVF licensees are required to take reasonable measures to verify the identity of any beneficial owners owning or controlling 25% or more of the voting rights or shares, etc. of a corporation, partnership or trust. In high risk situations, the threshold for the requirement is 10%.[20]

[19] See Appendix B which contains a list of documents recognised by the HKMA as independent and reliable sources for identity verification purposes.

[20] In circumstances where an existing customer is reclassified as high-risk, SVF licensees may consider delaying taking reasonable measures to verify the beneficial owner's identity according to the enhanced threshold (i.e. remediate from 25% to 10%) where a risk of tipping-off exists.

4.3.6 For beneficial owners, SVF licensee should obtain the complete residential address and may adopt an RBA to determine the need to take reasonable measures to verify the address, taking account of the number of beneficial owners, the nature and distribution of the interests in the entity and the nature and extent of any business, contractual or family relationship.

4.4 Identification and verification of a person purporting to act on behalf of the customer

4.4.1 If a person purports to act on behalf of the customer, SVF licensees must:

(i) identify the person and take reasonable measures to verify the person's identity on the basis of documents, data or information provided by-
  (a) a governmental body;
  (b) the HKMA or any other RA;
  (c) an authority in a place outside Hong Kong that performs functions similar to those of the HKMA or any other RA; or
  (d) any other reliable and independent source that is recognised by the HKMA; and

(ii) verify the person's authority to act on behalf of the customer.

4.4.2 The general requirement is to obtain the same identification information as set out in paragraph 4.8.1. In taking reasonable measures to verify the identity of persons purporting to act on behalf of customers (e.g. authorized account signatories and attorneys), the SVF licensee should refer to the documents and other means listed in Appendix B wherever possible. As a general rule SVF licensees should identify and verify the identity of those authorized to give instructions for the movement of funds or assets.

4.4.3 SVF licensees should obtain written authority[21] to verify that the individual purporting to represent the customer is authorized to do so.

4.4.4 SVF licensees may on occasion encounter difficulties in identifying and verifying signatories of customers that may have long lists of account signatories, particularly if such customers are based outside Hong Kong. In such cases, SVF licensees may adopt an RBA in determining the appropriate measures to comply with these requirements; for example in respect of verification of account signatories related to a customer, such as an FI or a listed company[22], SVF licensees could adopt a simplified approach.

[21] For corporation, SVF licensees should obtain the board resolution or similar written authority.
[22] Having regard to the advice provided at paragraphs 4.14.

The provision of a signatory list[23], recording the names of the account signatories, whose identities and authority to act have been confirmed by a department or person within that customer which is independent to the persons whose identities are being verified (e.g. compliance, audit or human resources), may be sufficient to demonstrate compliance with these requirements.

Another option, mainly relevant to overseas customers and which may be considered in conjunction with or separately from reducing the signatories list, is the use of intermediaries in accordance with paragraph 4.15.

4.5 Characteristics and evidence of identity

4.5.1 No form of identification can be fully guaranteed as genuine or representing correct identity and SVF licensees should recognise that some types of documents are more easily forged than others. If suspicions are raised in relation to any document offered, SVF licensees should take whatever practical and proportionate steps are available to establish whether the document offered is genuine, or has been reported as lost or stolen. This may include searching publicly available information, approaching relevant authorities (such as the Immigration Department through its hotline) or requesting corroboratory evidence from the customer. Where suspicion cannot be eliminated, the document should not be accepted and consideration should be given to making a report to the authorities.

Where documents are in a foreign language, appropriate steps should be taken by the SVF licensee to be reasonably satisfied that the documents in fact provide evidence of the customer's identity (e.g. ensuring that staff assessing such documents are proficient in the language or obtaining a translation from a suitably qualified person).

4.6 Purpose and intended nature of business relationship

4.6.1 An SVF licensee must understand the purpose and intended nature of the business relationship. In many instances, this will be self-evident, but in some cases, the SVF licensee may have to obtain information in this regard.

4.6.2 Unless the purpose and intended nature are obvious, SVF licensees should obtain satisfactory information from all new customers as to the intended purpose and reason for opening the account or establishing the business relationship, and record the information on the account opening documentation. Depending

[23] Or equivalent.

on the SVF licensee's risk assessment of the situation, information that might be relevant may include:

(a) nature and details of the business/occupation/employment;
(b) the anticipated level and nature of the activity that is to be undertaken through the relationship (e.g. what the typical transactions are likely to be);
(c) location of customer;
(d) the expected source and origin of the funds to be used in the relationship; and
(e) initial and ongoing source(s) of wealth or income.

4.6.3 This requirement also applies in the context of non-residents. While the vast majority of non-residents seek business relationships with SVF licensees in Hong Kong for perfectly legitimate reasons, some non-residents may represent a higher risk for ML/TF. An SVF licensee should understand the rationale for a non-resident to seek to establish a business relationship in Hong Kong.

4.7 Keeping customer information up-to-date

4.7.1 Once the identity of a customer has been satisfactorily verified, there is no obligation to re-verify identity (unless doubts arise as to the veracity or adequacy of the evidence previously obtained for the purposes of customer identification); however, SVF licensees should take steps from time to time to ensure that the customer information that has been obtained for the purposes of complying with the requirements in this Chapter are up-to-date and relevant. To achieve this, an SVF licensee should undertake periodic reviews of existing records of customers.

An appropriate time to do so is upon certain trigger events. These include:

(a) when a significant transaction[24] is to take place;
(b) when a material change occurs in the way the customer's account is operated;
(c) when the SVF licensee's customer documentation standards change substantially; or
(d) when the SVF licensee is aware that it lacks sufficient information about the customer concerned.

In all cases, the factors determining the period of review or what constitutes a trigger event should be clearly defined in the SVF licensees' policies and procedures.

[24] The word "significant" is not necessarily linked to monetary value. It may include transactions that are unusual or not in line with the SVF licensee's knowledge of the customer.

4.7.2 All high-risk customers (excluding dormant accounts) should be subject to a minimum of an annual review, and more frequently if deemed necessary by the SVF licensee, of their profile to ensure the CDD information retained remains up-to-date and relevant. SVF licensees should however clearly define what constitutes a dormant account in their policies and procedures.

4.8 Natural persons

Identification

4.8.1 SVF licensees should collect the following identification information in respect of individual customers who need to be identified:

(a) full name;
(b) date of birth;
(c) nationality; and
(d) identity document type and number.

Verification (Hong Kong residents)

4.8.2 For Hong Kong residents, SVF licensees should verify an individual's name, date of birth and identity card number by reference to their Hong Kong identity card. SVF licensees should retain a copy of the individual's identity card.

4.8.3 For children born in Hong Kong who are under the age of 12 and not in possession of a valid travel document or Hong Kong identity card, the identities of children should be verified by reference to their Hong Kong birth certificates.

Whenever establishing a business relationship with a minor, the identity of the minor's parent or guardian representing or accompanying the minor should be recorded and verified in accordance with the above requirements.

Verification (non-residents)

4.8.4 For non-residents who are physically present in Hong Kong for verification purposes, SVF licensees should verify an individual's name, date of birth, nationality and travel document number and type by reference to a valid travel document (e.g. an unexpired international passport). In this respect the SVF licensee should retain a copy of the "biodata" page which contains the bearer's photograph and biographical details.

4.8.5 For non-residents who are not physically present in Hong Kong

for verification purposes, SVF licensees should verify the individual's identity, including name, date of birth, nationality, identity or travel document number and type by reference to:

(a) a valid travel document;
(b) a relevant national (i.e. government or state-issued) identity card bearing the individual's photograph;
(c) a valid national driving license bearing the individual's photograph; or
(d) any applicable alternatives mentioned in Appendix B.

4.8.6 In respect of paragraph 4.8.5 above, where a customer has not been physically present for identification purposes, an SVF licensee must also carry out the measures at paragraphs 4.12.

Address identification and verification

4.8.7 An SVF licensee should obtain the complete residential address of a customer with whom it establishes a business relationship and may adopt an RBA to determine the need to take reasonable measures to verify the residential address.

4.8.8 Where verification is undertaken, methods for verifying residential addresses may include obtaining[25]:

(a) a recent utility bill issued within the last 3 months;
(b) recent correspondence from a Government department or agency (i.e. issued within the last 3 months);
(c) a statement, issued by an AI, a licensed corporation or an authorized insurer within the last 3 months;
(d) a record of a visit to the residential address by the SVF licensee;
(e) an acknowledgement of receipt duly signed by the customer in response to a letter sent by the SVF licensee to the address provided by the customer;
(f) a letter from an immediate family member at which the individual resides confirming that the applicant lives at that address in Hong Kong, setting out the relationship between the applicant and the immediate family member, together with evidence that the immediate family member resides at the same address (for persons such as students and housewives who are unable to provide proof of address of their own name);
(g) mobile phone or pay TV statement (sent to the address provided by the customer) issued within the last 3 months;
(h) a letter from a Hong Kong nursing or residential home for the elderly or disabled, which an SVF licensee is satisfied that it

[25] The examples provided are not exhaustive.

can place reliance on, confirming the residence of the applicant;

(i) a letter from a Hong Kong university or college, which an SVF licensee is satisfied that it can place reliance on, that confirms residence at a stated address;
(j) a Hong Kong tenancy agreement which has been duly stamped by the Inland Revenue Department;
(k) a current Hong Kong domestic helper employment contract stamped by an appropriate Consulate (the name of the employer should correspond with the applicant's visa endorsement in their passport);
(l) a letter from a Hong Kong employer together with proof of employment, which an SVF licensee is satisfied that it can place reliance on and that confirms residence at a stated address in Hong Kong;
(m) a lawyer's confirmation of property purchase, or legal document recognising title to property; and
(n) for non-Hong Kong residents, a government-issued photographic driving license or national identity card containing the current residential address or bank statements issued by a bank in an equivalent jurisdiction where the SVF licensee is satisfied that the address has been verified.

4.8.9 It is conceivable that SVF licensees may not always be able to adopt any of the suggested methods in the paragraph above. Examples include countries without postal deliveries and virtually no street addresses, where residents rely upon post office boxes or their employers for the delivery of mail. Some customers may simply be unable to produce evidence of address to the standard outlined above. In such circumstances SVF licensees may, on a risk sensitive basis, adopt a common sense approach by adopting alternative methods such as obtaining a letter from a director or manager of a verified known overseas employer that confirms residence at a stated overseas address (or provides detailed directions to locate a place of residence).

There may also be circumstances where a customer's address is a temporary accommodation and where normal address verification documents are not available, for example, an expatriate on a short-term contract. SVF licensees should adopt flexible procedures to obtain verification by other means, e.g. copy of contract of employment, or bank's or employer's written confirmation. SVF licensees should exercise a degree of flexibility under special circumstances (e.g. where a customer is homeless). For the avoidance of doubt, a post office box address is not sufficient for persons residing in Hong Kong or corporate customers registered and/or operating in Hong Kong.

Other considerations

4.8.10 The standard identification requirement is likely to be sufficient for most situations. If, however, the customer, or the product or service, is assessed to present a higher ML/TF risk because of the nature of the customer, his business, his location, or because of the product features, etc., the SVF licensee should consider whether it should require additional identity information to be provided, and/or whether to verify additional aspects of identity.

4.8.11 Appendix B contains a list of documents recognised by the HKMA as independent and reliable sources for identity verification purposes.

4.9 Legal persons

General

4.9.1 For legal persons, the principal requirement is to look behind the customer to identify those who have ultimate control or ultimate beneficial ownership over the business and the customer's assets. SVF licensees would normally pay particular attention to persons who exercise ultimate control over the management of the customer.

4.9.2 In deciding who the beneficial owner is in relation to a legal person where the customer is not a natural person, the SVF licensee's objective is to know who has ownership or control over the legal person which relates to the relationship, or who constitutes the controlling mind and management of any legal entity involved in the funds. Verifying the identity of the beneficial owner(s) should be carried out using reasonable measures based on an RBA, following the guidance in Chapter 3.

4.9.3 Where the owner is another legal person or trust, the objective is to undertake reasonable measures to look behind that legal person or trust and to verify the identity of beneficial owners. What constitutes control for this purpose will depend on the nature of the institution, and may vest in those who are mandated to manage funds, accounts or investments without requiring further authorisation.

4.9.4 For a customer other than a natural person, SVF licensees should ensure that they fully understand the customer's legal form, structure and ownership, and should additionally obtain information on the nature of its business, and the reasons for seeking the product or service unless the reasons are obvious.

4.9.5 SVF licensees should conduct reviews from time to time to ensure the customer information held is up-to-date and relevant; methods by which a review could be conducted include conducting company searches, seeking copies of resolutions appointing directors, noting the resignation of directors, or by other appropriate means.

4.9.6 Many entities operate internet websites, which contain information about the entity. SVF licensees should bear in mind that this information, although helpful in providing much of the materials that an SVF licensee might need in relation to the customer, its management and business, may not be independently verified.

Corporation

Identification information

4.9.7 The information below should be obtained as a standard requirement; thereafter, on the basis of the ML/TF risk, an SVF licensee should decide whether further verification of identity is required and if so the extent of that further verification. The SVF licensee should also decide whether additional information in respect of the corporation, its operation and the individuals behind it should be obtained.

An SVF licensee should obtain and verify the following information in relation to a customer which is a corporation:

(a) full name;
(b) date and place of incorporation;
(c) registration or incorporation number; and
(d) registered office address in the place of incorporation.

If the business address of the customer is different from the registered office address in (d) above, the SVF licensee should obtain information on the business address and verify as far as practicable.

4.9.8 In the course of verifying the customer's information mentioned in paragraph 4.9.7, an SVF licensee should also obtain the following information[26]:

(a) a copy of the certificate of incorporation and business registration (where applicable);
(b) a copy of the company's memorandum and articles of association which evidence the powers that regulate and bind

[26] Examples given are not exhaustive.

the company; and
(c) details of the ownership and structure control of the company, e.g. an ownership chart.

For the avoidance of doubt, this requirement does not apply in respect of a company falling within paragraph 4.10.3.

4.9.9 An SVF licensee should[27] record the names of all directors and verify the identity of directors on an RBA.

4.9.10 SVF licensees should:

(a) confirm the company is still registered and has not been dissolved, wound up, suspended or struck off;
(b) independently identify and verify the names of the directors and shareholders recorded in the company registry in the place of incorporation; and
(c) verify the company's registered office address in the place of incorporation.

4.9.11 The SVF licensee should verify the information in paragraph 4.9.10 from:

for a locally incorporated company:

(a) a search of file at the Hong Kong Company Registry and obtain a company report[28];

for a company incorporated overseas:

(b) a similar company search enquiry of the registry in the place of incorporation and obtain a company report[28];
(c) a certificate of incumbency[29] or equivalent issued by the company's registered agent in the place of incorporation; or
(d) a similar or comparable document to a company search report or a certificate of incumbency certified by a professional third party in the relevant jurisdiction verifying that the information at paragraph 4.9.10, contained in the said document, is correct and accurate.

---

[27] The SVF licensee may, of course, already be required to identify a particular director if the director acts as a beneficial owner or a person purporting to act on behalf of the customer (e.g. account signatories). (see paragraphs 4.3 and 4.4)

[28] Alternatively, the SVF licensee may obtain from the customer a certified true copy of a company search report certified by a company registry or professional third party. The company search report should have been issued within the last 6 months. For the avoidance of doubt, it is not sufficient for the report to be self-certified by the customer.

[29] SVF licensees may accept a certified true copy of a certificate of incumbency certified by a professional third party. The certificate of incumbency should have been issued within the last 6 months. For the avoidance of doubt, it is not sufficient for the certificate to be self-certified by the customer.

For the avoidance of doubt, this requirement does not apply in respect of a company falling within paragraph 4.10.3.

4.9.12 If the SVF licensee has obtained a company search report pursuant to paragraph 4.9.11 which contains information such as certificate of incorporation, company's memorandum and articles of association, etc., the SVF licensee is not required to obtain the same information again from the customer pursuant to paragraph 4.9.8.

Beneficial owners

4.9.13 The beneficial owner in relation to a corporation is:

(i) an individual who –
  (a) owns or controls, directly or indirectly, including through a trust or bearer share holding, not less than 10% of the issued share capital of the corporation;
  (b) is, directly or indirectly, entitled to exercise or control the exercise of not less than 10% of the voting rights at general meetings of the corporation; or
  (c) exercises ultimate control over the management of the corporation; or
(ii) if the corporation is acting on behalf of another person, means the other person.

4.9.14 An SVF licensee should identify and record the identity of all beneficial owners, and take reasonable measures to verify the identity of:

(a) all shareholders holding 25% (for normal risk circumstances) / 10% (for high risk circumstances) or more of the voting rights or share capital;
(b) any individual who exercises ultimate control over the management of the corporation; and
(c) any person on whose behalf the customer is acting.

4.9.15 For companies with multiple layers in their ownership structures, an SVF licensee should ensure that it has an understanding of the ownership and control structure of the company. The intermediate layers of the company should be fully identified. The manner in which this information is collected should be determined by the SVF licensee, for example by obtaining a director's declaration incorporating or annexing an ownership chart describing the intermediate layers (the information to be included should be determined on a risk sensitive basis but at a minimum should include company name and place of incorporation, and where applicable, the rationale behind the

particular structure employed). The objective should always be to follow the chain of ownership to the individuals who are the ultimate beneficial owners of the direct customer of the SVF licensee and verify the identity of those individuals.

4.9.16 SVF licensees need not, as a matter of routine, verify the details of the intermediate companies in the ownership structure of a company. Complex ownership structures (e.g. structures involving multiple layers, different jurisdictions, trusts, etc.) without an obvious commercial purpose pose an increased risk and may require further steps to ensure that the SVF licensee is satisfied on reasonable grounds as to the identity of the beneficial owners.

4.9.17 The need to verify the intermediate corporate layers of the ownership structure of a company will therefore depend upon the SVF licensee's overall understanding of the structure, its assessment of the risks and whether the information available is adequate in the circumstances for the SVF licensee to consider if it has taken adequate measures to identify the beneficial owners.

4.9.18 Where the ownership is dispersed, the SVF licensee should concentrate on identifying and taking reasonable measures to verify the identity of those who exercise ultimate control over the management of the company.

Partnerships and unincorporated bodies

4.9.19 Partnerships and unincorporated bodies, although principally operated by individuals or groups of individuals, are different from individuals, in that there is an underlying business. This business is likely to have a different ML/TF risk profile from that of an individual.

4.9.20 The beneficial owner, in relation to a partnership, is:

(i) an individual who
  (a) is entitled to or controls, directly or indirectly, not less than a 10% share of the capital or profits of the partnership;
  (b) is, directly or indirectly, entitled to exercise or control the exercise of not less than 10% of the voting rights in the partnership; or
  (c) exercises ultimate control over the management of the partnership; or
(ii) if the partnership is acting on behalf of another person, means the other person.

4.9.21 In relation to an unincorporated body other than a partnership, beneficial owner:

(i) means an individual who ultimately owns or controls the unincorporated body; or
(ii) if the unincorporated body is acting on behalf of another person, means the other person.

4.9.22 The SVF licensee should obtain the following information in relation to the partnership or unincorporated body:

(a) the full name;
(b) the business address; and
(c) the names of all partners and individuals who exercise control over the management of the partnership or unincorporated body, and names of individuals who own or control not less than 10% of its capital or profits, or of its voting rights.

In cases where a partnership arrangement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained.

4.9.23 The SVF licensee's obligation is to verify the identity of the customer using evidence from a reliable and independent source. Where partnerships or unincorporated bodies are well-known, reputable organisations, with long histories in their industries, and with substantial public information about them, their partners and controllers, confirmation of the customer's membership of a relevant professional or trade association is likely to be sufficient to provide such reliable and independent evidence of the identity of the customer. This does not remove the need to take reasonable measures to verify the identity of the beneficial owners[30] of the partnerships or unincorporated bodies.

4.9.24 Other partnerships and unincorporated bodies have a lower profile, and generally comprise a much smaller number of partners and controllers. In verifying the identity of such customers, SVF licensees should primarily have regard to the number of partners and controllers. Where these are relatively few, the customer should be treated as a collection of individuals; where numbers are larger, the SVF licensee should decide whether it should continue to regard the customer as a collection of individuals, or whether it can be satisfied with evidence of membership of a relevant professional or trade association. In either case, SVF licensees should obtain the partnership deed (or other evidence in the case of sole traders or other unincorporated

[30] Reference should be made to paragraph 4.3.5.

bodies), to satisfy themselves that the entity exists, unless an entry in an appropriate national register may be checked.

4.9.25 In the case of associations, clubs, societies, charities, religious bodies, institutes, mutual and friendly societies, co-operative and provident societies, an SVF licensee should satisfy itself as to the legitimate purpose of the organisation, e.g. by requesting sight of the constitution.

Other considerations

4.9.26 Appendix B contains a list of documents recognised by the HKMA as independent and reliable sources for identity verification purposes.

4.10 Simplified customer due diligence

General

4.10.1 This Guideline specifies what CDD measures are and also prescribes the circumstances in which an SVF licensee must carry out CDD. SDD means that application of full CDD measures is not required. In practice, this means that SVF licensees are not required to identify and verify the beneficial owner. However, other aspects of CDD must be undertaken and it is still necessary to conduct ongoing monitoring of the business relationship. SVF licensees must have reasonable grounds to support the use of SDD and may have to demonstrate these grounds to the HKMA.

4.10.2 Nonetheless, SDD must not be applied when the SVF licensee suspects that the customer, the customer's account or the transaction is involved in ML/TF, or when the SVF licensee doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or verifying the customer's identity, notwithstanding when the customer falls within paragraph 4.10.3 below.

4.10.3 Customers to whom SDD may be applied are as follows:

(a) an FI including an SVF licensee, an AI, a licensed corporation, an authorized insurer, an appointed insurance agent, an authorized insurance broker, a licensed money service operator and the Postmaster General;
(b) an institution that-
  (i) is incorporated or established in an equivalent jurisdiction (see paragraphs 4.17);
  (ii) carries on a business similar to that carried on by an FI;
  (iii) has measures in place to ensure compliance with requirements relating to CDD and record-keeping similar

to those imposed under this Guideline; and

(iv) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the RAs;

(c) a corporation listed on any stock exchange ("listed company");

(d) an investment vehicle where the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle is-

(i) an FI;

(ii) an institution incorporated or established in Hong Kong, or in an equivalent jurisdiction that-

i. has measures in place to ensure compliance with requirements relating to CDD and record-keeping similar to those imposed under this Guideline; and

ii. is supervised for compliance with those requirements.

(e) the Government or any public body in Hong Kong; or

(f) the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.

4.10.4 If a customer not falling within paragraph 4.10.3 has in its ownership chain an entity that falls within that paragraph, the SVF licensee is not required to identify or verify the beneficial owners of that entity in that chain when establishing a business relationship with for the customer. However, SVF licensees should still identify and take reasonable measures to verify the identity of beneficial owners in the ownership chain that are not connected with that entity.

4.10.5 For the avoidance of doubt, the SVF licensee must still:

(a) identify the customer and verify[31] the customer's identity;

(b) if a business relationship is to be established and its purpose and intended nature are not obvious, obtain information on the purpose and intended nature of the business relationship with the SVF licensee; and

(c) if a person purports to act on behalf of the customer,

(i) identify the person and take reasonable measures to verify the person's identity; and

(ii) verify the person's authority to act on behalf of the customer,

in accordance with the relevant requirements stipulated in this Guideline.

[31] For FIs and listed companies, please refer to paragraphs 4.10.7 and 4.10.8 respectively.

Local and foreign financial institution

4.10.6 SVF licensees may apply SDD to a customer that is an FI as defined in paragraph 4.10.3(a), or an institution that carries on a business similar to that carried on by an FI and meets the criteria set out in paragraph 4.10.3(b). If the customer does not meet the criteria, the SVF licensee must carry out all the CDD measures set out in paragraph 4.1.3.

4.10.7 For ascertaining whether the institution meets the criteria set out in paragraph 4.10.3(a) and (b), it will generally be sufficient for an SVF licensee to verify that the institution is on the list of authorized (and supervised) FIs in the jurisdiction concerned.

Listed company

4.10.8 SVF licensees may perform SDD in respect of a corporate customer listed on a stock exchange[32]. This means SVF licensees need not identify the beneficial owners of the listed company. In such cases, it will be generally sufficient for an SVF licensee to obtain proof of listed status on a stock exchange. In all other cases, SVF licensees should follow the CDD requirements for a legal person set out in paragraphs 4.9 of this Guideline.

Government and public body

4.10.9 SVF licensees may apply SDD to a customer that is the Hong Kong government, any public bodies in Hong Kong, the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.

4.10.10 Public body includes:

(a) any executive, legislative, municipal or urban council;
(b) any Government department or undertaking;
(c) any local or public authority or undertaking;
(d) any board, commission, committee or other body, whether paid or unpaid, appointed by the Chief Executive or the Government; and
(e) any board, commission, committee or other body that has power to act in a public capacity under or for the purposes of any enactment.

[32] Reference should be made to paragraphs 4.14.

4.11 High-risk situations

4.11.1 An SVF licensee must, in any situation that by its nature presents a higher risk of ML/TF, take additional measures to mitigate the risk of ML/TF.

Additional measures[33] or EDD should be taken to mitigate the ML/TF risk involved, which for illustration purposes, may include:

(a) obtaining additional information on the customer (e.g. connected parties[34], accounts or relationships) and updating more regularly the customer profile including the identification data;
(b) obtaining additional information on the intended nature of the business relationship (e.g. anticipated account activity);
(c) obtaining the approval of senior management to commence or continue the relationship; and
(d) conducting enhanced monitoring of the business relationship, by increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination.

For the avoidance of doubt, all high-risk customers should be subject to a minimum annual review with reference to paragraph 4.7.2.

4.12 Customer not physically present for identification purposes

4.12.1 SVF licensees must apply equally effective customer identification procedures and ongoing monitoring standards for customers not physically present for identification purposes as for those where the customer is available for interview[35]. In case a business relationship is established where the customer is not physically present for identification purposes (e.g. through internet), it may pose additional ML/TF risks as well as increased risk of impersonation.

4.12.2 An SVF licensee is required to take additional measures to compensate for any risk associated with customers not physically present for identification purposes. In determining the additional measures to be taken, the SVF licensee should take into account the nature and characteristic of products or service provided and the risk of customer and carry out at least one of the following

[33] Additional measures should be documented in the SVF licensee's policies and procedures.
[34] Consideration might be given to obtaining, and taking reasonable measures to verify, the addresses of directors and account signatories.
[35] For the avoidance of doubt, this is not restricted to being physically present in Hong Kong; the face-to-face meeting could take place outside Hong Kong.

measures to mitigate the risks posed:

(a) further verifying the customer's identity on the basis of documents, data or information referred to in paragraph 4.2.1 but not previously used for the purposes of verification of the customer's identity under that paragraph;
(b) taking supplementary measures to verify all the information provided by the customer;
(c) ensuring that the first payment made into the customer's account is received from an account in the customer's name with an AI or a bank operating in an equivalent jurisdiction that has measures in place to ensure compliance with requirements relating to CDD and record-keeping similar to those imposed under this Guideline and is supervised for compliance with those requirements by a banking regulator in that jurisdiction; or
(d) taking additional measures to mitigate the risks involved.

Consideration should be given on the basis of the ML/TF risk to obtaining copies of documents that have been certified by a suitable certifier.

Suitable certifiers and the certification procedure

4.12.3 Use of an independent suitable certifier guards against the risk that documentation provided does not correspond to the customer whose identity is being verified. However, for certification to be effective, the certifier will need to have seen the original documentation.

4.12.4 Suitable persons to certify verification of identity documents may include:

(a) an intermediary specified in paragraphs 4.15.8, 4.15.9 and 4.15.10;
(b) a member of the judiciary in an equivalent jurisdiction;
(c) an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity; and
(d) a Justice of the Peace.

4.12.5 The certifier must sign and date the copy document (printing his/her name clearly in capitals underneath) and clearly indicate his/her position or capacity on it. The certifier must state that it is a true copy of the original (or words to similar effect).

4.12.6 SVF licensees remain liable for failure to carry out prescribed CDD and therefore must exercise caution when considering accepting certified copy documents, especially where such

documents originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction.

In any circumstances where an SVF licensee is unsure of the authenticity of certified documents, or that the documents relate to the customer, SVF licensees should take additional measures to mitigate the ML/TF risk.

4.13 Politically exposed persons

General

4.13.1 Much international attention has been paid in recent years to the risk associated with providing financial and business services to those with a prominent political profile or holding senior public office. However, PEP status itself does not automatically mean that the individuals are corrupt or that they have been incriminated in any corruption.

4.13.2 However, their office and position may render PEPs vulnerable to corruption. The risks increase when the person concerned is from a foreign country with widely-known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have adequate AML/CFT standards.

4.13.3 While the definition of PEPs in paragraph 4.13.5 below only includes individuals entrusted with prominent public function in a place outside the People's Republic of China[36], domestic PEPs may also present, by virtue of the positions they hold, a high risk situation where EDD should be applied. SVF licensees should therefore adopt an RBA to determining whether to apply the measures in paragraph 4.13.13 below in respect of domestic PEPs.

4.13.4 The definition of PEPs does not automatically exclude sub-national political figures. Corruption by heads of regional governments, regional government ministers and large city mayors is no less serious as sub-national figures in some jurisdictions may have access to substantial funds. Where SVF licensees identify a customer as a sub-national figure holding a prominent public function, they should apply appropriate EDD. This also applies to domestic sub-national figures assessed by the SVF licensee to pose a higher risk. In determining what constitutes a prominent public function, SVF licensees should consider factors such as persons with significant influence in general, significant influence over or control of public

[36] Reference should be made to the definition of the People's Republic of China in the Interpretation and General Clauses Ordinance (Cap. 1).

procurement or state owned enterprises, etc.

(Foreign) Politically exposed person

4.13.5 A politically exposed person is:

(a) an individual who is or has been entrusted with a prominent public function in a place outside the People's Republic of China and
  (i) includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official;
  (ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i);
(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or
(c) a close associate of an individual falling within paragraph (a) (see paragraph 4.13.6).

4.13.6 A close associate is:

(a) an individual who has close business relations with a person falling under paragraph 4.13.5(a) above, including an individual who is a beneficial owner of a legal person or trust of which the person falling under paragraph 4.13.5(a) is also a beneficial owner; or
(b) an individual who is the beneficial owner of a legal person or trust that is set up for the benefit of a person falling under paragraph 4.13.5(a) above.

4.13.7 SVF licensees that handle the proceeds of corruption, or handle illegally diverted government, supranational or aid funds, face reputational and legal risks, including the possibility of criminal charges for having assisted in laundering the proceeds of crime.

4.13.8 SVF licensees can reduce risk by conducting EDD at the outset of the business relationship and ongoing monitoring where they know or suspect that the business relationship is with a PEP.

4.13.9 SVF licensees must establish and maintain effective procedures (for example making reference to publicly available information and/or screening against commercially available databases) for determining whether a customer or a beneficial owner of a customer is a PEP. These procedures should extend to the connected parties of the customer using an RBA.

4.13.10 SVF licensees may use publicly available information or refer to relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations to assess which countries are most vulnerable to corruption (an example of which is Transparency International's "Corruption Perceptions Index", which ranks countries according to their perceived level of corruption).

SVF licensees should be vigilant where either the country to which the customer has business connections or the business/industrial sector is more vulnerable to corruption.

4.13.11 SVF licensees may demonstrate compliance with the requirement set out at paragraph 4.13.9 (this also applies to domestic PEPs), for example, by implementing policies and procedures to screen the name of the customer and the beneficial owner against publicly available information or a commercial electronic database to determine, as far as practicable, whether the individual is politically exposed, before establishing a business relationship, and on a periodic basis thereafter. These procedures should extend to the connected parties of the customer using an RBA.

SVF licensees may rely on its overseas office to undertake the screening process.

4.13.12 Having regard to Chapter 3, specific risk factors the SVF licensees should consider in handling a business relationship (or potential relationship) with a PEP include:

(a) any particular concern over the country where the PEP holds his public office or has been entrusted with his public functions, taking into account his position;
(b) any unexplained sources of wealth or income (i.e. value of assets owned not in line with the PEP's income level);
(c) expected receipts of large sums from governmental bodies or state-owned entities;
(d) source of wealth described as commission earned on government contracts;
(e) request by the PEP to associate any form of secrecy with a transaction; and
(f) use of accounts at a government-owned bank or of government accounts as the source of funds in a transaction.

4.13.13 When SVF licensees know that a particular customer or beneficial owner is a PEP, it should, before (i) establishing a business relationship or (ii) continuing an existing business relationship where the customer or the beneficial owner is subsequently found to be a PEP, apply all the following EDD measures:

(a) obtaining approval from its senior management;
(b) taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds; and
(c) applying enhanced monitoring to the relationship in accordance with the assessed risks.

4.13.14 It is for an SVF licensee to decide which measures it deems reasonable, in accordance with its assessment of the risks, to establish the source of funds and source of wealth. In practical terms, this will often amount to obtaining information from the PEP and verifying it against publicly available 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. SVF licensees should however note that not all declarations are publicly available and that a PEP customer may have legitimate reasons for not providing a copy. SVF licensees should also be aware that some jurisdictions impose restrictions on their PEP's ability to hold foreign bank accounts or to hold other office or paid employment.

Senior management approval

4.13.15 While the Guideline is silent on the level of senior management who may approve the establishment or continuation of the relationship, the approval process should take into account the advice of the SVF licensee's CO. The more potentially sensitive the PEP, the higher the approval process should be escalated.

Domestic politically exposed persons

4.13.16 For the purposes of this Guideline, a domestic PEP is defined as:

(a) an individual who is or has been entrusted with a prominent public function in a place within the People's Republic of China and
    (i) includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official;
    (ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i);
(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or
(c) a close associate of an individual falling within paragraph (a)

(see paragraph 4.13.6).

4.13.17 SVF licensees should take reasonable measures to determine whether an individual is a domestic PEP.

4.13.18 If an individual is known to be a domestic PEP, the SVF licensee should perform a risk assessment to determine whether the individual poses a higher risk of ML/TF. Domestic PEPs status in itself does not automatically confer higher risk. In any situation that the SVF licensee assesses to present a higher risk of ML/TF, it should apply the EDD and monitoring specified in paragraph 4.11.1.

4.13.19 SVF licensees should retain a copy of the assessment for the HKMA, other authorities and auditors and should review the assessment whenever concerns as to the activities of the individual arise.

Periodic reviews

4.13.20 For domestic PEPs assessed to present a higher risk and foreign PEPs, they should be subject to a minimum annual review. SVF licensees should review CDD information to ensure that it remains up-to-date and relevant.

4.14 Jurisdictions that do not or insufficiently apply the FATF's Recommendations or otherwise posing higher risk

4.14.1 SVF licensees should give particular attention to, and exercise extra care in respect of:

(a) business relationships and transactions with persons (including legal persons and other FIs) from or in jurisdictions that do not or insufficiently apply the FATF's Recommendations; and
(b) transactions and business connected with jurisdictions assessed as higher risk.

Based on the SVF licensee's assessment of the risk in either case, the special requirements of paragraph 4.11.1 may apply. In addition to ascertaining and documenting the business rationale for establishing a relationship, an SVF licensee should take reasonable measures to establish the source of funds of such customers.

4.14.2 In determining which jurisdictions do not apply, or insufficiently apply the FATF's Recommendations, or may otherwise pose a higher risk, SVF licensees should consider, among other things:

(a) circulars issued to SVF licensees by the HKMA;
(b) whether the jurisdiction is subject to sanctions, embargoes or similar measures issued by relevant organisations such as the UN. In addition, in some circumstances where a jurisdiction is subject to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized, the sanctions or measures may still be given credence by an SVF licensee because of the standing of the issuer and the nature of the measures;
(c) whether the jurisdiction is identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures;
(d) whether the jurisdiction is identified by credible sources as providing funding or support for terrorist activities and has designated terrorist organisations operating within it; and
(e) whether the jurisdiction is identified by credible sources as having significant levels of corruption, or other criminal activity.

"Credible sources" refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-government organisations. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

An SVF licensee should be aware of the potential reputation risk of conducting business in jurisdictions which do not or insufficiently apply the FATF's Recommendations or other jurisdictions known to apply inferior standards for the prevention of ML/TF.

If an SVF licensee incorporated in Hong Kong has operating units in such jurisdictions, care should be taken to ensure that effective controls on prevention of ML/TF are implemented in these units. In particular, the SVF licensee should ensure that the policies and procedures adopted in such overseas units are similar to those adopted in Hong Kong. There should also be compliance and internal audit checks by staff from the head office in Hong Kong.

4.15 Reliance on CDD performed by intermediaries

General

4.15.1 SVF licensees may rely upon an intermediary to perform any part of the CDD measures specified in paragraph 4.1.3, subject to fulfilment of certain criteria. However, the ultimate responsibility for ensuring that CDD requirements are met remains with the SVF licensee.

For the avoidance of doubt, reliance on intermediaries does not apply to:

(a) outsourcing or agency relationships, i.e. where the agent is acting under a contractual arrangement with the SVF licensee to carry out its CDD function. In such a situation the outsource or agent is to be regarded as synonymous with the SVF licensee (i.e. the processes and documentation are those of the SVF licensee itself); and
(b) business relationships, accounts or transactions between SVF licensees for their clients.

In practice, this reliance on third parties often occurs through introductions made by another member of the same financial services group, or in some jurisdictions from another FI or third party.

4.15.2 The SVF licensee must obtain written confirmation from the intermediary that:

(a) it agrees to perform the role; and
(b) it will provide without delay a copy of any document or record obtained in the course of carrying out the CDD measures on behalf of the SVF licensee upon request.

The SVF licensee must ensure that the intermediary will, if requested by the SVF licensee within the period specified in the record-keeping requirements under Chapter 8, provide to the SVF licensee a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out that measure as soon as reasonably practicable after receiving the request.

4.15.3 SVF licensees should obtain satisfactory evidence to confirm the status and eligibility of the intermediary. Such evidence may comprise corroboration from the intermediary's regulatory authority, or evidence from the intermediary of its status, regulation, policies and procedures.

4.15.4 An SVF licensee that carries out a CDD measure by means of an intermediary must immediately after the intermediary has carried out that measure, obtain from the intermediary the data or information that the intermediary has obtained in the course of carrying out that measure, but nothing in this paragraph requires the SVF licensee to obtain at the same time from the intermediary a copy of the document, or a record of the data or information, that is obtained by the intermediary in the course of carrying out that measure.

4.15.5 Where these documents and records are kept by the intermediary, the SVF licensee should obtain an undertaking from the intermediary to keep all underlying CDD information throughout the continuance of the SVF licensee's business relationship with the customer and for at least six years beginning on the date on which the business relationship of a customer with the SVF licensee ends or until such time as may be specified by the HKMA. SVF licensees should also obtain an undertaking from the intermediary to supply copies of all underlying CDD information in circumstances where the intermediary is about to cease trading or does not act as an intermediary for the SVF licensee anymore.

4.15.6 SVF licensees should conduct sample tests from time to time to ensure CDD information and documentation is produced by the intermediary upon demand and without undue delay.

4.15.7 Whenever an SVF licensee has doubts as to the reliability of the intermediary, it should take reasonable steps to review the intermediary's ability to perform its CDD duties. If the SVF licensee intends to terminate its relationship with the intermediary, it should immediately obtain all CDD information from the intermediary. If the SVF licensee has any doubts regarding the CDD measures carried out by the intermediary previously, the SVF licensee should perform the required CDD as soon as reasonably practicable.

Domestic intermediaries

4.15.8 SVF licensees may rely upon an AI, a licensed corporation, an authorized insurer, an appointed insurance agent or an authorized insurance broker, to perform any part of the CDD measures.

4.15.9 SVF licensees may also rely upon the following categories of domestic intermediaries:

(a) a solicitor practising in Hong Kong;
(b) a certified public accountant practising in Hong Kong;
(c) a current member of The Hong Kong Institute of Chartered

Secretaries practising in Hong Kong; and

(d) a trust company registered under Part VIII of the Trustees Ordinance carrying on trust business in Hong Kong,

provided that the intermediary is able to satisfy the SVF licensee that they have adequate procedures in place to prevent ML/TF.[37]

Overseas intermediaries

4.15.10 SVF licensees may only rely upon an overseas intermediary carrying on business or practising in an equivalent jurisdiction where the intermediary:

(a) falls into one of the following categories of businesses or professions:
  (i) an institution that carries on a business similar to that carried on by an FI mentioned in paragraph 4.15.8;
  (ii) a lawyer or a notary public;
  (iii) an auditor, a professional accountant, or a tax advisor;
  (iv) a trust or company service provider; and
  (v) a trust company carrying on trust business;
(b) is required under the law of the jurisdiction concerned to be registered or licensed or is regulated under the law of that jurisdiction;
(c) has measures in place to ensure compliance with requirements relating to CDD and record-keeping similar to those imposed under this Guideline; and
(d) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the RAs.

4.15.11 Compliance with the requirements set out above for both domestic or overseas intermediaries may entail the SVF licensee:

(a) reviewing the intermediary's AML/CFT policies and procedures; or
(b) making enquiries concerning the intermediary's stature and regulatory track record and the extent to which any group's AML/CFT standards are applied and audited.

4.16 Prohibition on anonymous accounts

4.16.1 Other than the low risk SVF products which are permitted under the streamlined approach as specified under paragraphs 1.4.6 to 1.4.21, SVF licensees must not maintain anonymous accounts or

[37] Based on a similar provision under the AMLO, the arrangement for allowing SVF licensees to rely on these intermediaries will expire in March 2018. This arrangement will be reviewed again at the same time.

accounts in fictitious names for any new or existing customer. Where numbered accounts exist, SVF licensees must maintain them in such a way that full compliance can be achieved with this Guideline. SVF licensees must properly identify and verify the identity of the customer in accordance with the Guideline. In all cases, whether the relationship involves numbered accounts or not, the customer identification and verification records must be available to the CO, other appropriate staff, the HKMA, other authorities and auditors upon appropriate authority.

4.17 Jurisdictional equivalence

General

4.17.1 Jurisdictional equivalence and the determination of equivalence may be a consideration in the application of CDD measures under this Guideline. For example, paragraph 4.10.3 restricts the application of SDD to overseas institutions that carry on a business similar to that carried on by an FI and are incorporated or established in an equivalent jurisdiction. Paragraph 4.15.10 restricts reliance upon intermediaries outside Hong Kong for CDD measures to those practising or carrying on business in an equivalent jurisdiction.

4.17.2 Equivalent jurisdiction means:

(a) a jurisdiction that is a member of the FATF, other than Hong Kong; or
(b) a jurisdiction that imposes requirements relating to CDD and record-keeping similar to those imposed to FIs in Hong Kong.

Determination of jurisdictional equivalence

4.17.3 SVF licensees may therefore be required to evaluate and determine for themselves which jurisdictions other than FATF members apply requirements relating to CDD and record-keeping similar to those imposed to FIs in Hong Kong for jurisdictional equivalence purposes. When doing so an SVF licensee should document its assessment of the jurisdiction, which may include consideration of the following factors:

(a) membership of a regional group of jurisdictions that admit as members only jurisdictions that have demonstrated a commitment to the fight against ML/TF, and which have an appropriate legal and regulatory regime to back up this commitment. Where a jurisdiction is a member of such a group, this may be taken into account as a supporting factor in the SVF licensee's assessment of whether the jurisdiction

is likely to be "equivalent";

(b) mutual evaluation reports. Particular attention should be paid to assessments that have been undertaken by the FATF, FATF-style regional bodies, the International Monetary Fund and the World Bank. SVF licensees should bear in mind that mutual evaluation reports are at a "point in time", and should be interpreted as such;

(c) lists of jurisdictions published by the FATF with strategic AML/CFT deficiencies through the International Co-operation Review Group processes;

(d) advisory circulars issued by the HKMA from time to time alerting SVF licensees to such jurisdictions with poor AML/CFT controls;

(e) lists of jurisdictions, entities and individuals that are involved, or that are alleged to be involved, in activities that cast doubt on their integrity in the AML/CFT area that are published by specialised national, international, non-governmental and commercial organisations. An example of such is Transparency International's "Corruption Perceptions Index", which ranks countries according to their perceived level of corruption; and

(f) guidance provided at paragraphs 4.14 "Jurisdictions that do not or insufficiently apply the FATF's Recommendations or otherwise posing a higher risk".

4.17.4 The judgment on equivalence is one to be made by each SVF licensee in the light of the particular circumstances and senior management is accountable for this judgment. It is therefore important that the reasons for concluding that a particular jurisdiction is equivalent (other than those jurisdictions that are FATF members) are documented at the time the decision is made, and that the decision is made on up-to-date and relevant information. A record of the assessment performed and factors considered should be retained for regulatory scrutiny and periodically reviewed to ensure it remains up-to-date and valid.

Chapter 5 – ONGOING MONITORING

General

5.1 Effective ongoing monitoring is vital for understanding of customers' activities and an integral part of effective AML/CFT systems. It helps SVF licensees to know their customers and to detect unusual or suspicious activities.

An SVF licensee must continuously monitor its business relationship with a customer by:

(a) reviewing from time to time documents, data and information relating to the customer and obtained for the purpose of complying with the requirements imposed under this Guideline to ensure that they are up-to-date and relevant[38];
(b) monitoring the activities (including cash and non-cash transactions) of the customer to ensure that they are consistent with the nature of business, the risk profile and source of funds. An unusual transaction may be in the form of activity that is inconsistent with the expected pattern for that customer, or with the normal business activities for the type of product or service that is being delivered; and
(c) identifying transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose and which may indicate ML/TF.

5.2 Failure to conduct ongoing monitoring could expose an SVF licensee to potential abuse by criminals, and may call into question the adequacy of systems and controls, or the prudence and integrity or fitness and properness of the SVF licensee's management.

5.3 Possible characteristics that SVF licensees should consider monitoring include:

(a) the nature and type of transactions (e.g. abnormal size or frequency);
(b) the nature of a series of transactions (e.g. a number of cash top-up);
(c) the amount of any transactions, paying particular attention to particularly substantial transactions;
(d) the geographical origin/destination of a payment or receipt; and
(e) the customer's normal activity or turnover.

5.4 SVF licensees should be vigilant for changes on the basis of the

[38] See paragraphs 4.7.1 and 4.7.2.

business relationship with the customer over time. These may include where:

(a) new products or services that pose higher risk are entered into;
(b) new corporate structures are created;
(c) the stated activity or turnover of a customer changes or increases; or
(d) the nature of transactions changes or their volume or size increases, etc.

5.5 Where the basis of the business relationship changes significantly, SVF licensees should carry out further CDD procedures to ensure that the ML/TF risk involved and basis of the relationship are fully understood. Ongoing monitoring procedures must take account of the above changes.

5.6 SVF licensees should conduct an appropriate review of a business relationship upon the filing of a report to the JFIU and should update the CDD information where appropriate; this will enable SVF licensees to assess appropriate levels of ongoing review and monitoring.

RBA to monitoring

5.7 The extent of monitoring should be linked to the risk profile of the customer which has been determined through the risk assessment required in Chapter 3. To be most effective, resources should be targeted towards business relationships presenting a higher risk of ML/TF.

5.8 SVF licensees must take additional measures when monitoring business relationships that pose a higher risk. High-risk relationships, for example those involving PEPs, will require more frequent and intensive monitoring. In monitoring high-risk situations, relevant considerations may include:

(a) whether adequate procedures or management information systems are in place to provide relevant staff (e.g. CO, MLRO, front line staff and relationship managers) with timely information that might include, as a result of EDD or other additional measures undertaken, any information on any connected accounts or relationships; and
(b) how to monitor the sources of funds, wealth and income for higher risk customers and how any changes in circumstances will be recorded.

Methods and procedures

5.9 When considering how best to monitor customer transactions and activities, an SVF licensee should take into account the following factors:

(a) the size and complexity of its business;
(b) its assessment of the ML/TF risks arising from its business;
(c) the nature of its systems and controls;
(d) the monitoring procedures that already exist to satisfy other business needs; and
(e) the nature of the products and services (which includes the means of delivery or communication).

There are various methods by which these objectives can be met including exception reports (e.g. large transactions exception report) and transaction monitoring systems. Exception reports will help SVF licensee's stay apprised of operational activities.

5.10 Where transactions that are complex, large or unusual, or patterns of transactions which have no apparent economic or lawful purpose are noted, SVF licensees should examine the background and purpose, including where appropriate the circumstances, of the transactions. The findings and outcomes of these examinations should be properly documented in writing and be available to assist the HKMA, other competent authorities and auditors. Proper records of decisions made, by whom, and the rationale for them will help an SVF licensee demonstrate that it is handling unusual or suspicious activities appropriately.

s. 25A(5), DTROP & OSCO, s.12(5), UNATMO

5.11 Such examinations may include asking the customer questions, based on common sense, that a reasonable person would ask in the circumstances. Such enquiries, when conducted properly and in good faith, do not constitute tipping off *(see: <www.jfiu.gov.hk>)*. These enquiries are directly linked to the CDD requirements, and reflect the importance of "knowing your customer" in detecting unusual or suspicious activities. Such enquiries and their results should be properly documented and be available to assist the HKMA, other authorities and auditors. Where there is any suspicion, a report must be made to the JFIU.

5.12 Where cash transactions (including cash top-up and withdrawals) and transfers to third parties are not in accordance with the customer's known reasonable practice, SVF licensees must approach such situations with caution and make relevant further enquiries. Where the SVF licensee has been unable to satisfy itself that any cash transaction or third party transfer is reasonable, and therefore considers it suspicious, it should make an STR to the JFIU.

Chapter 6 – FINANCIAL SANCTIONS AND TERRORIST FINANCING

Financial sanctions and proliferation financing

6.1 The obligations under the Hong Kong's financial sanctions regime apply to all persons, including SVF licensees.

s.3(1), UNSO

6.2 UNSO gives the Chief Executive the authority to make regulations to implement sanctions decided by the UNSC and to specify or designate relevant persons and entities.

6.3 These sanctions normally prohibit making available or dealing with, directly or indirectly, any funds or economic resources for the benefit of or belonging to a designated party.

6.4 The HKMA circulates to all SVF licensees designations published in the government Gazette under the UNSO.

6.5 While SVF licensees will not normally have any obligation under Hong Kong law to have regard to lists issued by other organisations or authorities in other jurisdictions, an SVF licensee operating internationally will need to be aware of the scope and focus of relevant financial/trade sanctions regimes in those jurisdictions. Where these sanctions may affect their operations, SVF licensees should consider what implications exist for their procedures, such as the consideration to monitor the parties concerned with a view to ensuring that there are no payments to or from a person on a sanctions list issued by an overseas jurisdiction.

Applicable UNSO Regulation

6.6 The Chief Executive can licence exceptions to the prohibitions on making funds and economic resources available to a designated party under the UNSO. An SVF licensee seeking such a licence should write to the Commerce and Economic Development Bureau.

Terrorist financing

6.7 Terrorist financing generally refers to the carrying out of transactions involving property that are owned by terrorists, or that have been, or are intended to be, used to assist the commission of terrorist acts. This has not previously been explicitly covered under the money laundering regime where the focus is on the handling of criminal proceeds, i.e. the source of property is what matters. In terrorist financing, the focus is on the destination or use of property, which may have derived from legitimate sources.

UNSCR 1373 (2001)

6.8 The UNSC has passed UNSCR 1373 (2001), which calls on all member states to act to prevent and suppress the financing of

terrorist acts. Guidance issued by the UNSC Counter Terrorism Committee in relation to the implementation of UNSCRs regarding terrorism can be found at: www.un.org/en/sc/.

UNSCR 1267 (1999); 1390 (2002); 1617 (2005)

6.9 The UN has also published the names of individuals and organisations subject to UN financial sanctions in relation to involvement with Usama bin Laden, Al-Qa'ida, and the Taliban under relevant UNSCRs (e.g. UNSCR 1267 (1999), 1390 (2002) and 1617 (2005)). All UN member states are required under international law to freeze the funds and economic resources of any legal person(s) named in this list and to report any suspected name matches to the relevant authorities.

6.10 The UNATMO was enacted in 2002 to give effect to the mandatory elements of UNSCR 1373 and the FATF's Recommendations.

s.6, UNATMO

6.11 The Secretary for Security (S for S) has the power to freeze suspected terrorist property and may direct that a person shall not deal with the frozen property except under the authority of a licence. Contraventions are subject to a maximum penalty of 7 years imprisonment and an unspecified fine.

6.12 Section 6 of the UNATMO essentially confers the S for S an administrative power to freeze suspected terrorist property for a period of up to two years, during which time the authorities may apply to the court for an order to forfeit the property. This administrative freezing mechanism will enable the S for S to take freezing action upon receiving intelligence of suspected terrorist property in Hong Kong.

s.8 & 14, UNATMO

6.13 It is an offence for any person to make any property or financial services available, by any means, directly or indirectly, to or for the benefit of a terrorist or terrorist associate except under the authority of a licence granted by S for S. It is also an offence for any person to collect property or solicit financial (or related) services, by any means, directly or indirectly, for the benefit of a terrorist or terrorist associate. Contraventions are subject to a maximum sentence of 14 years imprisonment and an unspecified fine.

6.14 Section 8 of the UNATMO does not affect a freeze per se; it prohibits a person from (i) making available, by any means, directly or indirectly, any property or financial services to or for the benefit of a person he knows or has reasonable grounds to suspect is a terrorist or terrorist associate, in the absence of a licence granted by S for S; and (ii) collecting property or soliciting financial (or related) services, by any means, directly or indirectly, for the benefit of a person he knows or has reasonable

grounds to suspect is a terrorist or terrorist associate.

s.6(1), UNATMO

6.15 The S for S can licence exceptions to the prohibitions to enable frozen property and economic resources to be unfrozen and to allow payments to be made to or for the benefit of a designated party under the UNATMO. An SVF licensee seeking such a licence should write to the Security Bureau.

s.4(1), UNATMO

6.16 Where a person is designated by a Committee of the UNSC as a terrorist and his details are subsequently published in a notice under section 4 of the UNATMO in the Government gazette, the HKMA will circulate the designations to all SVF licensees.

s.4, WMD(CPS)O

6.17 It is an offence under section 4 of the Weapons of Mass Destruction (Control of Provision of Services) Ordinance (WMD(CPS)O), Cap. 526, for a person to provide any services where he believes or suspects, on reasonable grounds, that those services may be connected to WMD proliferation. The provision of services is widely defined and includes the lending of money or other provision of financial assistance.

6.18 SVF licensees may draw reference from a number of sources including relevant designation by overseas authorities, such as the designations made by the US Government under relevant Executive Orders. The HKMA may draw the SVF licensee's attention to such designations from time to time.

All SVF licensees will therefore need to ensure that they should have appropriate system to conduct checks against the relevant list for screening purposes and that this list is up-to-date.

Database maintenance and screening (customers and payments)

6.19 SVF licensees should take measures to ensure compliance with the relevant regulations and legislation on terrorist financing. The legal obligations of SVF licensees and those of its staff should be well understood and adequate guidance and training should be provided to the latter. SVF licensees are required to establish policies and procedures for combating terrorist financing. The systems and mechanisms for identification of suspicious transactions should cover terrorist financing as well as money laundering.

6.20 It is particularly vital that an SVF licensee should be able to identify and report transactions with terrorist suspects and designated parties. To this end, the SVF licensee should ensure that it maintains a database of names and particulars of terrorist suspects and designated parties which consolidates the various lists that have been made known to it. Alternatively, an SVF

licensee may make arrangements to access to such a database maintained by third party service providers.

6.21 SVF licensees should ensure that the relevant designations are included in the database. Such database should, in particular, include the lists published in the Gazette and those designated under the US Executive Order 13224. The database should also be subject to timely update whenever there are changes, and should be made easily accessible by staff for the purpose of identifying suspicious transactions.

6.22 Comprehensive ongoing screening of an SVF licensee's complete customer base is a fundamental internal control to prevent terrorist financing and sanction violations, and should be achieved by:

(a) screening customers against current terrorist and sanction designations at the establishment of the relationship; and
(b) thereafter, as soon as practicable after new terrorist and sanction designations are published by the HKMA that these new designations, screening against their entire client base.

6.23 The screening procedures should extend to the connected parties of the customer using an RBA. SVF licensees may rely on its overseas office to undertake the screening process.

6.24 SVF licensees need to have some means of screening payment instructions to ensure that proposed payments to designated parties are not made. SVF licensees should be particularly alert for suspicious wire transfers.

6.25 Enhanced checks should be conducted before establishing a business relationship or processing a transaction, where possible, if there are circumstances giving rise to suspicion.

6.26 In order to demonstrate compliance with the provisions of paragraphs 6.22 to 6.25 above, the screening and any results should be documented, or recorded electronically.

6.27 If an SVF licensee suspects that a transaction is terrorist-related, it should make a report to the JFIU. Even if there is no evidence of a direct terrorist connection, the transaction should still be reported to the JFIU if it looks suspicious for other reasons, as it may emerge subsequently that there is a terrorist link.

6.28 In case of any suspicions of terrorist financing or sanction violations, SVF licensees should also make a report to the HKMA.

Chapter 7 – SUSPICIOUS TRANSACTION REPORTS

General issues

s.25A(1), DTROP & OSCO, s.12(1), UNATMO

7.1 Sections 25A of the DTROP and the OSCO make it an offence to fail to disclose where a person knows or suspects that property represents the proceeds of drug trafficking or of an indictable offence respectively. Likewise, section 12 of the UNATMO makes it an offence to fail to disclose knowledge or suspicion of terrorist property. Under the DTROP and the OSCO, failure to report knowledge or suspicion carries a maximum penalty of three months imprisonment and a fine of HK$50,000.

s.25A(2), DTROP & OSCO, s.12(2), UNATMO

7.2 Filing a report to the JFIU provides SVF licensees with a statutory defence to the offence of ML/TF in respect of the acts disclosed in the report, provided:

(a) the report is made before the SVF licensee undertakes the disclosed acts and the acts (transaction(s)) are undertaken with the consent of the JFIU; or
(b) the report is made after the SVF licensee has performed the disclosed acts (transaction(s)) and the report is made on the SVF licensee's own initiative and as soon as it is reasonable for the SVF licensee to do so.

s.25A(4), DTROP & OSCO, s.12(4), UNATMO

7.3 Once an employee has reported his suspicion to the appropriate person in accordance with the procedure established by his employer for the making of such disclosures, he has fully satisfied the statutory obligation.

s.25A(5), DTROP & OSCO, s.12(5), UNATMO

7.4 It is an offence ("tipping off") to reveal to any person any information which might prejudice an investigation; if a client is told that a report has been made, this would prejudice the investigation and an offence would be committed.

7.5 Once knowledge or suspicion has been formed the following general principles should be applied:

(a) in the event of suspicion of ML/TF, a disclosure should be made even where no transaction has been conducted by or through the SVF licensee[39];
(b) disclosures must be made as soon as is reasonably practical after the suspicion was first identified; and
(c) SVF licensees must ensure that they put in place internal

[39] The reporting obligations require a person to report suspicions of ML/TF, irrespective of the amount involved. The reporting obligations of section 25A(1) DTROP and OSCO and section 12(1) UNATMO apply to "any property". These provisions establish a reporting obligation whenever a suspicion arises, without reference to transactions *per se.* Thus, the obligation to report applies whether or not a transaction was actually conducted and also covers attempted transactions.

controls and systems to prevent any directors, officers and employees committing the offence of tipping off the customer or any other person who is the subject of the disclosure. SVF licensees should also take care that their line of enquiry with customers is such that tipping off cannot be construed to have taken place.

7.6 CDD and ongoing monitoring provide the basis for recognising unusual and suspicious transactions and events. An effective way of recognising suspicious activity is knowing enough about customers, their circumstances and their normal expected activities to recognise when a transaction or instruction, or a series of transactions or instructions, is unusual.

7.7 SVF licensees must ensure sufficient guidance is given to staff to enable them to form suspicion or to recognise when ML/TF is taking place, taking account of the nature of the transactions and instructions that staff is likely to encounter, the type of product or service and the means of delivery, i.e. whether face to face or remote. This will also enable staff to identify and assess the information that is relevant for judging whether a transaction or instruction is suspicious in the circumstances.

Knowledge vs. suspicion

7.8 SVF licensees have an obligation to report where there is knowledge or suspicion of ML/TF. Generally speaking, knowledge is likely to include:

(a) actual knowledge;
(b) knowledge of circumstances which would indicate facts to a reasonable person; and
(c) knowledge of circumstances which would put a reasonable person on inquiry.

7.9 Suspicion is more subjective. Suspicion is personal and falls short of proof based on firm evidence.

7.10 As the types of transactions which may be used for criminal activity are almost unlimited, it is difficult to determine what will constitute a suspicious transaction.

7.11 The key is knowing enough about the customer's business to recognise that a transaction, or a series of transactions, is unusual and, from an examination of the unusual, whether there is a suspicion of ML/TF. Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, etc., the transaction should be considered as unusual and the SVF licensee should be

put on alert.

JFIU "SAFE" Approach

7.12 Where the SVF licensee conducts enquiries and obtains what it considers to be a satisfactory explanation of the activity or transaction, it may conclude that there are no grounds for suspicion, and therefore take no further action. However, where the SVF licensee's enquiries do not provide a satisfactory explanation of the activity or transaction, it may conclude that there are grounds for suspicion, and must make a disclosure (*see: <www.jfiu.gov.hk/>)*.

7.13 For a person to have knowledge or suspicion, he does not need to know the nature of the criminal activity underlying the money laundering, or that the funds themselves definitely arose from the criminal offence.

7.14 The following is a (non-exhaustive) list of examples of situations that might give rise to suspicion in certain circumstances:

(a) discrepancies between the information submitted by the customer and information detected by monitoring systems;
(b) individuals who hold an unusual volume of SVF accounts with the same provider;
(c) a large and diverse source of funds (i.e. bank transfers, credit card and cash funding from different locations) used to fund the same SVF account(s);
(d) multiple reference bank accounts from banks located in different jurisdictions used to fund the same SVF account;
(e) loading or funding of an SVF account always done by third parties;
(f) multiple third party funding activities of an SVF account, followed by the immediate transfer of funds to unrelated bank account(s);
(g) multiple loading or funding of the same SVF account, followed by ATM withdrawals shortly afterwards, over a short period of time;
(h) multiple withdrawals conducted at different ATMs (sometimes located in various countries different from jurisdiction where the SVF account was funded);
(i) an SVF account only used for withdrawals, and not for making payments for goods or services;
(j) an SVF account being used in multiple jurisdictions within days of issuance;
(k) atypical use of the SVF product (including unexpected and frequent cross-border access or transactions);
(l) customers who load or fund SVF accounts containing counterfeit notes or forged instruments;
(m) a substantial increase in turnover on an SVF account;
(n) reluctance to provide normal information when opening an

SVF account, providing minimal or fictitious information or, when applying to open an SVF account, providing information that is difficult or expensive for the institution to verify;

(o) large cash withdrawals from a previously dormant/inactive SVF account; and

(p) structured the transactions to avoid reaching the limits for conducting normal CDD (e.g. a few transactions within a short period of time with an amount just below the limit for conducting normal CDD, purchase of multiple non-reloadable prepaid cards just below the limit for conducting normal CDD by a single customer over a short period of time).

These are not intended to be exhaustive and only provide examples of the most basic ways in which money may be laundered. However, identification of any of the types of transactions listed above should prompt further investigations and be a catalyst towards making at least initial enquiries about the source of funds.

SVF licensees should also be aware of elements of individual transactions that could indicate property involved in terrorist financing. The FATF has issued guidance in detecting terrorist financing [40] and SVF licensees should be familiar with the characteristics in that guidance.

7.15 The OSCO, DTROP and UNATMO prohibit disclosure by the SVF licensee or its staff that an STR has been made which is likely to prejudice any investigation that might be conducted following that disclosure. A risk exists that customers could be unintentionally tipped off when the SVF licensee is seeking to perform its CDD obligations during the establishment or course of the business relationship.

The customer's awareness of a possible STR or investigation could prejudice future efforts to investigate the suspected ML/TF operation. Therefore, if SVF licensees form a suspicion that transactions relate to ML/TF, they should take into account the risk of tipping off when performing the CDD process. SVF licensees should ensure that their employees are aware of and sensitive to these issues when conducting CDD.

Timing and manner of reports

7.16 When an SVF licensee knows or suspects that property represents

[40] Reference could be made to the "Terrorist Financing" and "Guidance for Financial Institutions in Detecting Terrorist Financing" issued by the FATF in February 2008 and April 2002 respectively.

the proceeds of crime or terrorist property, a disclosure must be made to the JFIU as soon as it is reasonable to do so[41]. The use of a standard form or the use of the e-channel "STREAMS"[42] is strongly encouraged. Further details of reporting methods and advice may be found at www.jfiu.gov.hk. In the event that an urgent disclosure is required, particularly when the account is part of an ongoing investigation, it should be indicated in the disclosure. Where exceptional circumstances exist in relation to an urgent disclosure, an initial notification by telephone may be considered.

7.17 Dependent on when knowledge or suspicion arises, disclosures may be made either before a suspicious transaction or activity occurs (whether the intended transaction ultimately takes place or not), or after a transaction or activity has been completed.

s.25A(1), DTROP & OSCO, s.12(1), UNATMO

7.18 The law requires the disclosure to be made together with any matter on which the knowledge or suspicion is based. The need for prompt disclosures is especially important where a customer has instructed the SVF licensee to move funds or other property, close the account, make cash available for collection, or carry out significant changes to the business relationship. In such circumstances, consideration may be given to contact the JFIU urgently.

Internal reporting

7.19 An SVF licensee should appoint a MLRO as a central reference point for reporting suspicious transactions. The SVF licensee should have measures in place to check, on an ongoing basis that it has policies and procedures to ensure compliance with legal and regulatory requirements and of testing such compliance. The type and extent of the measures to be taken in this respect should be appropriate having regard to the risk of ML/TF and the size of the business.

7.20 The SVF licensee should ensure that the MLRO is of sufficient status within the organisation, and has adequate resources, to enable him to perform his functions.

s.25A(4), DTROP & OSCO, s12(4), UNATMO

7.21 It is the responsibility of the MLRO to consider all internal disclosures he receives in the light of full access to all relevant documentation and other parties. However, the MLRO should not simply be that of a passive recipient of ad hoc reports of

[41] The purpose of disclosure is to fulfil the legal obligations set out in paragraph 7.1. Where SVF licensees want to make a crime report, a report should be made directly to the Hong Kong Police.

[42] STREAMS (Suspicion Transaction Report and Management System) is a web-based platform to assist in the receipt, analysis and dissemination of STRs. Use of STREAMS is recommended, especially for FIs who make frequent reports. Further details may be obtained from the JFIU.

suspicious transactions. Rather, the MLRO should play an active role in the identification and reporting of suspicious transactions. This may also involve regular review of exception reports or large or irregular transaction reports as well as ad hoc reports made by staff. To fulfil these functions all SVF licensees must ensure that the MLRO receives full co-operation from all staff and full access to all relevant documentation so that he is in a position to decide whether attempted or actual ML/TF is suspected or known.

7.22 Failure by the MLRO to diligently consider all relevant material may lead to vital information being overlooked and the suspicious transaction or activity or suspicious attempted transaction or activity not being disclosed to the JFIU in accordance with the requirements of the legislation. Alternatively, it may also lead to vital information being overlooked which may have made it clear that a disclosure would have been unnecessary.

7.23 SVF licensees should establish and maintain procedures to ensure that:

(a) all staff are made aware of the identity of the MLRO and of the procedures to follow when making an internal disclosure report; and
(b) all disclosure reports must reach the MLRO without undue delay.

7.24 While SVF licensees may wish to set up internal systems that allow staff to consult with supervisors or managers before sending a report to the MLRO, under no circumstances should reports raised by staff be filtered out by supervisors or managers who have no responsibility for the money laundering reporting/compliance function. The legal obligation is to report as soon as it is reasonable to do so, so reporting lines should be as short as possible with the minimum number of people between the staff with the suspicion and the MLRO. This ensures speed, confidentiality and accessibility to the MLRO.

7.25 All suspicious activity reported to the MLRO must be documented (in urgent cases this may follow an initial discussion by telephone). The report must include the full details of the customer and as full a statement as possible of the information giving rise to the suspicion.

s.25A(5), DTROP & OSCO, s.12(5), UNATMO

7.26 The MLRO must acknowledge receipt of the report and at the same time provide a reminder of the obligation regarding tipping off. The tipping-off provision includes circumstances where a suspicion has been raised internally, but has not yet been reported to the JFIU.

7.27 The reporting of a suspicion in respect of a transaction or event does not remove the need to report further suspicious transactions or events in respect of the same customer. Further suspicious transactions or events, whether of the same nature or different to the previous suspicion, must continue to be reported to the MLRO who should make further reports to the JFIU if appropriate.

7.28 When evaluating an internal disclosure, the MLRO must take reasonable steps to consider all relevant information, including CDD and ongoing monitoring information available within or to the SVF licensee concerning the entities to which the report relates. This may include:

(a) making a review of other transaction patterns and volumes through connected accounts;
(b) any previous patterns of instructions, the length of the business relationship and reference to CDD and ongoing monitoring information and documentation; and
(c) appropriate questioning of the customer per the systematic approach to identifying suspicious transactions recommended by the JFIU[43].

7.29 As part of the review, other connected accounts or relationships may need to be examined. The need to search for information concerning connected accounts or relationships should strike an appropriate balance between the statutory requirement to make a timely disclosure to the JFIU and any delays that might arise in searching for more relevant information concerning connected accounts or relationships. The evaluation process should be documented, together with any conclusions drawn.

7.30 If after completing the evaluation, the MLRO decides that there are grounds for knowledge or suspicion, he should disclose the information to the JFIU as soon as it is reasonable to do so after his evaluation is complete together with the information on which that knowledge or suspicion is based. Providing they act in good faith in deciding not to file an STR with the JFIU, it is unlikely that there will be any criminal liability for failing to report if a MLRO concludes that there is no suspicion after taking into account all available information. It is however vital for MLROs to keep proper records of their deliberations and actions taken to demonstrate they have acted in reasonable manner.

Recording internal reports

7.31 SVF licensees must establish and maintain a record of all ML/TF reports made to the MLRO. The record should include details of

[43] For details, please see www.jfiu.gov.hk.

the date the report was made, the staff members subsequently handling the report, the results of the assessment, whether the report resulted in a disclosure to the JFIU, and information to allow the papers relevant to the report to be located.

Records of reports to the JFIU

7.32 SVF licensees must establish and maintain a record of all disclosures made to the JFIU. The record must include details of the date of the disclosure, the person who made the disclosure, and information to allow the papers relevant to the disclosure to be located. This register may be combined with the register of internal reports, if considered appropriate.

Post reporting matters

7.33 SVF licensees should note that:

(a) filing a report to the JFIU only provides a statutory defence to ML/TF in relation to the acts disclosed in that particular report. It does not absolve an SVF licensee from the legal, reputational or regulatory risks associated with the account's continued operation;
(b) a "consent" response from the JFIU to a pre-transaction report should not be construed as a "clean bill of health" for the continued operation of the account or an indication that the account does not pose a risk to the SVF licensee;
(c) SVF licensees should conduct an appropriate review of a business relationship upon the filing of a report to the JFIU, irrespective of any subsequent feedback provided by the JFIU;
(d) once an SVF licensee has concerns over the operation of a customer's account or a particular business relationship, it should take appropriate action to mitigate the risks. Filing a report with the JFIU and continuing to operate the relationship without any further consideration of the risks and the imposition of appropriate controls to mitigate the risks identified is not acceptable;
(e) relationships reported to the JFIU should be subject to an appropriate review by the MLRO and if necessary the issue should be escalated to the SVF licensee's senior management to determine how to handle the relationship to mitigate any potential legal or reputational risks posed by the relationship in line with the SVF licensee's business objectives, and its capacity to mitigate the risks identified; and
(f) SVF licensees are not obliged to continue business relationships with customers if such action would place them at risk. It is recommended that SVF licensees indicate any intention to terminate a relationship in the initial disclosure to

the JFIU, thereby allowing the JFIU to comment, at an early stage, on such a course of action.

s.25A(1)(c) & (2)(a), DTROP & OSCO, s.1 & 12(2)(a), UNATMO

7.34 The JFIU will acknowledge receipt of a disclosure made by an institution under section 25A of both the DTROP and the OSCO, and section 12 of the UNATMO. If there is no need for imminent action e.g. the issue of a restraint order on an account, consent will usually be given for the institution to operate the account under the provisions of section 25A(2) of both the DTROP and the OSCO. An example of such a letter is given at Appendix C to this guideline. For disclosures submitted via e-channel "STREAM", e-receipt will be issued via the same channel. The JFIU may, on occasion, seek additional information or clarification with an SVF licensee of any matter on which the knowledge or suspicion is based.

7.35 Whilst there are no statutory requirements to provide feedback arising from investigations, the Hong Kong Police and Customs and Excise Department recognise the importance of having effective feedback procedures in place. The JFIU provides feedback both in its quarterly report[44] and upon request, to a disclosing SVF licensee in relation to the current status of an investigation.

7.36 After initial analysis by the JFIU, reports that are to be developed are allocated to financial investigation officers for further investigation. SVF licensees must ensure that they respond to all production orders within the required time limit and provide all of the information or material that falls within the scope of such orders. Where an SVF licensee encounters difficulty in complying with the timeframes stipulated, the MLRO should at the earliest opportunity contact the officer-in-charge of the investigation for further guidance.

[44] The purpose of the quarterly report, which is relevant to all financial sectors, is to raise AML/CFT awareness. It consists of two parts, (i) analysis of STRs and (ii) matters of interest and feedback. The report is available through the JFIU's website at www.jfiu.gov.hk. A password is required, details may be found under the typologies and feedback section of the website or by contacting the JFIU directly.

Chapter 8 – RECORD-KEEPING

General legal and regulatory requirements

8.1 Record-keeping is an essential part of the audit trail for the detection, investigation and confiscation of criminal or terrorist property or funds. Record-keeping helps the investigating authorities to establish a financial profile of a suspect, trace the criminal or terrorist property or funds and assists the Court to examine all relevant past transactions to assess whether the property or funds are the proceeds of or relate to criminal or terrorist offences.

8.2 SVF licensees should maintain customer, transaction and other records that are necessary and sufficient to meet the record-keeping requirements under this Guideline and other regulatory requirements that are appropriate to the scale, nature and complexity of their businesses. This is to ensure that:

(a) the audit trail for funds moving through an SVF licensee that relate to any customer and, where appropriate, the beneficial owner of the customer, account or transaction is clear and complete;
(b) any customer and, where appropriate, the beneficial owner of the customer can be properly identified and verified;
(c) all customer and transaction records and information are available on a timely basis to the HKMA, other authorities and auditors upon appropriate authority; and
(d) SVF licensees are able to comply with any relevant requirements specified in other sections of this Guideline and other guidelines issued by the HKMA, including, among others, records of customer risk assessment (see paragraph 3.12), registers of STRs (see paragraph 7.32) and training records (see paragraph 9.9).

Retention of records relating to customer identity and transactions

8.3 SVF licensees should keep:

(a) the original or a copy of the documents, and a record of the data and information, obtained in the course of identifying and verifying the identity of the customer and/or beneficial owner of the customer and/or beneficiary and/or persons who purport to act on behalf of the customer and/or other connected parties to the customer;
(b) any additional information in respect of a customer and/or beneficial owner of the customer that may be obtained for the purposes of EDD or ongoing monitoring;
(c) where applicable, the original or a copy of the documents,

and a record of the data and information, on the purpose and intended nature of the business relationship;

(d) the original or a copy of the records and documents relating to the customer's account (e.g. account opening form; risk assessment form) and business correspondence[45] with the customer and any beneficial owner of the customer (which at a minimum should include business correspondence material to CDD measures or significant changes to the operation of the account).

8.4 All documents and records mentioned in paragraph 8.3 should be kept throughout the business relationship with the customer and for a period of six years after the end of the business relationship.

8.5 SVF licensees should maintain the original or a copy of the documents, and a record of the data and information, obtained in connection with the transaction, which should be sufficient to permit reconstruction of individual transactions and establish a financial profile of any suspect account or customer. These records may include the following:

(a) the identity of the parties to the transaction;
(b) the nature and date of the transaction;
(c) the type and amount of currency involved;
(d) the origin of the funds (if known);
(e) the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.;
(f) the destination of the funds;
(g) the form of instruction and authority; and
(h) the type and identifying number of any account involved in the transaction (where applicable).

8.6 All documents and records mentioned in paragraph 8.5 should be kept for a period of six years after the completion of a transaction, regardless of whether the business relationship ends during the period.

8.7 If the record consists of a document, either the original of the document should be retained or a copy of the document should be kept on microfilm or in the database of a computer. If the record consists of data or information, such record should be kept either on microfilm or in the database of a computer.

8.8 The HKMA may write to an SVF licensee and require it to keep the records relating to a specified transaction or customer for a

[45] SVF licensees are not expected to keep each and every correspondence, such as a series of emails with the customer; the expectation is that sufficient correspondence is kept to demonstrate compliance with this Guideline.

period specified by the HKMA that is longer than those referred to in paragraphs 8.4 and 8.6, where the records are relevant to an ongoing criminal or other investigation, or to any other purposes as specified in the notice.

Records kept by intermediaries

8.9 Where customer identification and verification documents are held by an intermediary on which the SVF licensee is relying to carry out CDD measures, the SVF licensee concerned remains responsible for compliance with all record-keeping requirements. SVF licensees should ensure that the intermediaries being relied on have systems in place to comply with all the record-keeping requirements under this Guideline (including the requirements of paragraphs 8.3 to 8.8), and that documents and records will be provided by the intermediaries as soon as reasonably practicable after the intermediaries receive the request from the SVF licensees.

8.10 For the avoidance of doubt, SVF licensees that rely on intermediaries for carrying out a CDD measure should immediately obtain the information that the intermediary has obtained in the course of carrying out that measure, for example, name and address.

8.11 An SVF licensee should ensure that an intermediary will pass the documents and records to the SVF licensee, upon termination of the services provided by the intermediary.

8.12 Irrespective of where identification and transaction records are held, SVF licensees are required to comply with all legal and regulatory requirements in Hong Kong, including the requirements specified under this Guideline.

Chapter 9 – STAFF TRAINING

9.1 Staff training is an important element of an effective system to prevent and detect ML/TF activities. The effective implementation of even a well-designed internal control system can be compromised if staff using the system is not adequately trained.

9.2 Staff should be trained in what they need to do to carry out their particular roles in the SVF licensee with respect to AML/CFT. This is particularly important before new staff commence work.

9.3 SVF licensees should implement a clear and well articulated policy for ensuring that relevant staff receive adequate AML/CFT training.

9.4 The timing and content of training packages for different groups of staff will need to be adapted by individual SVF licensees for their own needs, with due consideration given to the size and complexity of their business and the type and level of ML/TF risk.

9.5 SVF licensees should provide appropriate AML/CFT training to their staff. The frequency of training should be sufficient to maintain the AML/CFT knowledge and competence of the staff.

9.6 Staff should be made aware of:

(a) their SVF licensee's and their own personal statutory obligations and the possible consequences for failure to report suspicious transactions under the DTROP, the OSCO and the UNATMO;
(b) any other statutory and regulatory obligations that concern their SVF licensees and themselves under the DTROP, the OSCO, the UNATMO, the UNSO and the PSSVFO, and the possible consequences of breaches of these obligations;
(c) the SVF licensee's policies and procedures relating to AML/CFT, including suspicious transaction identification and reporting; and
(d) any new and emerging techniques, methods and trends in ML/TF to the extent that such information is needed by the staff to carry out their particular roles in the SVF licensee with respect to AML/CFT.

9.7 In addition, the following areas of training may be appropriate for certain groups of staff:

(a) all new staff, irrespective of seniority:
    (i) an introduction to the background to ML/TF and the importance placed on ML/TF by the SVF licensee; and

(ii) the need for identifying and reporting of any suspicious transactions to the MLRO, and the offence of "tipping-off";

(b) members of staff who are dealing directly with the public (e.g. front-line personnel):
   (i) the importance of their role in the SVF licensee's ML/TF strategy, as the first point of contact with potential money launderers;
   (ii) the SVF licensee's policies and procedures in relation to CDD and record-keeping requirements that are relevant to their job responsibilities; and
   (iii) training in circumstances that may give rise to suspicion, and relevant policies and procedures, including, for example, lines of reporting and when extra vigilance might be required;

(c) back-office staff, depending on their roles:
   (i) appropriate training on customer verification and relevant processing procedures; and
   (ii) how to recognise unusual activities including abnormal settlements, payments or delivery instructions;

(d) managerial staff including internal audit officers and COs:
   (i) higher level training covering all aspects of the SVF licensee's AML/CFT regime; and
   (ii) specific training in relation to their responsibilities for supervising or managing staff, auditing the system and performing random checks as well as reporting of suspicious transactions to the JFIU; and

(e) MLROs:
   (i) specific training in relation to their responsibilities for assessing internal disclosure reports submitted to them and reporting of suspicious transactions to the JFIU; and
   (ii) training to keep abreast of AML/CFT requirements/developments generally.

9.8 SVF licensees are encouraged to consider using a mix of training techniques and tools in delivering training, depending on the available resources and learning needs of their staff. These techniques and tools may include on-line learning systems, focused classroom training, relevant videos as well as paper- or intranet-based procedures manuals. SVF licensees may consider including available FATF papers and typologies as part of the training materials. All materials should be up-to-date and in line with current requirements and standards.

9.9 No matter which training approach is adopted, SVF licensees should monitor and maintain records of who have been trained, when the staff received the training and the type of the training provided. Records should be maintained for a minimum of 3 years.

9.10 SVF licensees should monitor the effectiveness of the training. This may be achieved by:

(a) testing staff's understanding of the SVF licensee's policies and procedures to combat ML/TF, the understanding of their statutory and regulatory obligations, and also their ability to recognise suspicious transactions; and
(b) monitoring the compliance of staff with the SVF licensee's AML/CFT systems as well as the quality and quantity of internal reports so that further training needs may be identified and appropriate action can be taken.

Chapter 10 – WIRE TRANSFERS

General requirements

10.1 SVF licensees should comply with the requirements set out in this Chapter if they act as an ordering institution or beneficiary institution as specified in this Guideline. Where an SVF licensee is the originator or recipient/beneficiary of a wire transfer, it is not acting as an ordering institution or beneficiary institution and thus is not required to comply with the requirements in this Chapter in respect of that transaction.

10.2 A wire transfer is a transaction carried out by an institution (the ordering institution) on behalf of a person (the originator) by electronic means with a view to making an amount of money available to that person or another person (the recipient/beneficiary) at another institution (the beneficiary institution), which may be the ordering institution or another institution, whether or not one or more other institutions (intermediary institutions) participate in completion of the transfer of the money.

10.3 This Chapter does not apply to the following wire transfers:

(a) a wire transfer between an SVF licensee and an FI if each of them acts on its own behalf;
(b) a wire transfer between an SVF licensee and a foreign institution if each of them acts on its own behalf;
(c) a wire transfer if:
    (i) it arises from a transaction that is carried out using a credit card or debit card (such as withdrawing money from a bank account through an automated teller machine with a debit card, obtaining a cash advance on a credit card, or paying for goods or services with a credit or debit card), except when the card is used to effect a transfer of money; and
    (ii) the credit card or debit card number is included in the message or payment form accompanying the transfer.

10.4 FATF's Recommendations on wire transfers was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds, and for detecting such misuse when it occurs.

Ordering institutions

10.5 Ordering institutions must ensure that all wire transfers of amount equal to or exceeding HK$8,000 (or an equivalent amount in any other currency) are accompanied by complete and verified

originator information which includes:

(a) the originator's name;
(b) the number of the originator's account maintained with the SVF licensee and from which the money for the wire transfer is paid, or a unique reference number[46] (for non-account holders); and
(c) the originator's address or, in the absence of an address, the originator's customer identification number or identification document number (e.g. Hong Kong identity card number for a customer who is a natural person, or business registration number for a customer who is a legal person), or, if the originator is an individual, the originator's date and place of birth.

There is also a concession for domestic wire transfers set out below (see paragraph 10.16 below).

10.6 It is acceptable for an ordering institution to include the "correspondence address" of the originator in the wire transfer message provided that the ordering institution is satisfied that the address has been verified.

10.7 Ordering institutions must ensure that all the originator information accompanying the payment has been verified. The verification requirement is deemed to be met for account holding customers of the SVF licensee whose identity has been verified in compliance with Chapter 4 of this Guideline. No further verification of such account holder's information is normally required, although ordering institutions may exercise their discretion to do so in individual cases.

10.8 For transactions with non-account holders, the ordering institution must verify the identity of the customer and all originator information to accompany the wire transfer involving an amount equal to or exceeding the equivalent of HK$8,000, in compliance with Chapter 4 of this Guideline. For an occasional wire transfer below HK$8,000 (or the equivalent), ordering institutions are in general not required to verify the originator's identity, except when several transactions are carried out which appear to the ordering institution to be linked and are equal to or exceed the equivalent of HK$8,000. Evidence of verification must be retained with the customer information in accordance with the record-keeping requirements of Chapter 8 of this Guideline.

10.9 Ordering institutions may choose not to include all the required

[46] The unique reference number assigned by the ordering institution should permit the wire transfer to be traced back to the originator.

information in the wire transfer message accompanying a wire transfer of less than HK$8,000 or equivalent in foreign currencies. However, the relevant information about the originator should be recorded and retained by the ordering institution and should be made available within three business days on request by the beneficiary institution or the appropriate authorities. In considering whether to apply the threshold of HK$8,000, ordering institutions should take into account the business and operational characteristics of their wire transfer activities. Ordering institutions are encouraged to include, as far as practicable, the relevant originator information in the messages accompanying all wire transfer transactions.

10.10 For wire transfers conducted by an account holder as the originator, the originator's name and address (or permitted alternative) should generally correspond to the account holder. Any request to override customer information should not be entertained and any suspicion of improper motive by a customer should be reported to the ordering institution's MLRO.

10.11 In particular, an ordering institution should exercise care if there is suspicion that a customer may be effecting a wire transfer on behalf of a third party. If a wire transfer carries the name of a third party as the ordering person or otherwise does not appear to be consistent with the usual business/activity of the customer, the customer should be asked to provide further explanation of the nature of the wire transfer.

10.12 The relevant originator information should be recorded and retained in respect of both account holders and non-account holders.

10.13 Ordering institutions should adopt an RBA to check whether certain wire transfers may be suspicious taking into account such factors as the name of the beneficiary, the destination and amount of the wire transfer, etc.

10.14 Ordering institutions should establish clear policies on the processing of cross-border and domestic wire transfers. The policies should address the following:

(a) record-keeping;
(b) the verification of originator's identity information[47]; and
(c) the information to be included in messages.

[47] Where an originator is a non-account holder, SVF licensees should follow the customer identification, verification and record-keeping requirements prescribed for wire transfers in this Chapter.

10.15 Ordering institutions should include wire transfers in their ongoing due diligence on the business relationship with the originator and in their scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with their knowledge of the customer, its business and risk profile. Ordering institutions may adopt an RBA in their ongoing due diligence process. The process should be subject to regular audits to ensure its effectiveness.

Domestic wire transfers

10.16 Where both the ordering and beneficiary institutions are located within Hong Kong, the originator's information accompanying the wire transfer can simply be the originator's account number or a unique reference number which permits the transaction to be traced back to the originator.

10.17 However, if requested by the beneficiary institution or the HKMA, complete originator information (see paragraph 10.5) must be provided by the ordering institution within 3 business days after the request is received.

Beneficiary institutions

10.18 In respect of a wire transfer of any value for a beneficiary who is not an account holder, the beneficiary institution should record the identity and address of the recipient. For wire transfers equal to or exceeding HK$8,000, the beneficiary institution should verify the recipient's identity by reference to his identity card or travel document.

Batch file transfers

10.19 An ordering institution may bundle a number of transfers into a batch file for transmission to an overseas beneficiary institution. In such cases, the individual transfers within the batch file need only carry the originator's customer account number (or unique reference number if there is no account number), provided that the batch file itself contains complete originator information.

Intermediary institutions

10.20 If an SVF licensee acts as an intermediary institution in a wire transfer, it must ensure that all originator information which accompanies the wire transfer is retained with the transfer and is passed to the next institution in the payment chain.

10.21 The requirement to detect the lack of complete originator information applies to intermediaries in the same way as for transfers of funds received directly by the beneficiary institution.

10.22 It is preferable for an intermediary institution to forward payments through a system which is capable of carrying all the information received with the transfer. However, where an intermediary institution is technically unable to onward transmit originator information with transfers originating outside Hong Kong, it must advise the beneficiary institution of the originator information by another form of communication, whether within a payment or messaging system or otherwise.

Missing, incomplete or meaningless originator information[48]

10.23 SVF licensees must establish and maintain effective procedures for identifying and handling incoming wire transfers in compliance with the relevant originator information requirements.

10.24 If the domestic or cross border wire transfer is not accompanied by the originator's information, the SVF licensee must as soon as reasonably practicable, obtain the information from the institution from which it receives the transfer instruction. If the information cannot be obtained, the SVF licensee should either consider restricting or terminating its business relationship with that institution, or take reasonable measures to mitigate the ML/TF risk involved.

10.25 If the SVF licensee is aware that the accompanying information that purports to be the originator's information is incomplete or meaningless, it must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved.

SVF licensees may demonstrate compliance by implementing effective risk-based procedures and systems to subject incoming payment traffic to an appropriate level of post-event random sampling to identify wire transfers that contain incomplete or meaningless originator's information. This sampling may be weighted towards transfers:

(a) from institutions that are not located in equivalent jurisdictions, particularly those that are known to have failed to adequately implement international messaging standards (i.e. FATF's Recommendations on wire transfers);
(b) from institutions located in high-risk jurisdictions;
(c) that are higher value transfers; and
(d) from institutions that are identified by such sampling as

[48] This section is only applicable to an SVF licensee acting as a beneficiary institution.

having previously failed to comply with the relevant information requirement.

10.26 If a beneficiary institution becomes aware that a payment message contains meaningless or incomplete information, it must request complete originator information. Beneficiary institutions should set appropriate deadlines for the remediation of deficient transfers.

10.27 If the complete and meaningful information cannot be obtained by the beneficiary institution within the deadline set, it must either consider restricting or terminating its business relationship with the institution from which it receives the transfer instruction or take reasonable measures to mitigate the ML/TF risk posed, taking into account such factors as the name of the beneficiary, the origin and amount of the transfer, etc.

10.28 Other specific measures should also be considered by the beneficiary institutions, for example, checking, at the point of payment delivery, that originator information is complete and meaningful on all transfers that are collected in cash by recipients/beneficiaries on a "pay on application and identification" basis.

10.29 SVF licensees should also consider whether incomplete or meaningless information of which it becomes aware on a funds transfer constitutes grounds for suspicion and a report to the JFIU is appropriate.

10.30 If an ordering institution in Hong Kong regularly fails to supply the required originator information for a wire transfer involving an amount equal to or exceeding the equivalent of HK$8,000, the beneficiary institution should report the matter to the HKMA. Where an ordering institution is identified as having regularly failed to comply with these information requirements, the beneficiary institution should consider taking steps, which may initially include issuing warnings and setting deadlines, prior to either refusing to accept further transfers from that institution or deciding whether to restrict or terminate its relationship with that institution either completely or in respect of funds transfers.

10.31 For incoming wire transfers below HK$8,000 containing incomplete payment information (i.e. below the threshold where the requirement becomes mandatory), SVF licensees are not precluded from requesting the complete information; however, an RBA is suggested in such circumstances.

10.32 Records of all electronic payments and messages must be retained in accordance with this Guideline.

Cover payment messages related to cross-border wire transfers

10.33 The processing of cross-border wire transfers usually involves several institutions. In addition to the ordering institution and the beneficiary institution, additional institutions (cover intermediary institutions) which provide correspondent banking services to the originating institution or the beneficiary institution are often involved in the settlement of cross-border wire transfers. Cover payment messages are messages used by these institutions for the purpose of arranging funding to settle the interbank payment obligations created by cross-border wire transfers.

10.34 For wire transfers involving cover payment messages, ordering institutions should ensure that the message they send to cover intermediary institutions contains originator and beneficiary information. The originator and beneficiary information included in the cover payment message should be identical to that contained in the corresponding direct cross-border wire transfer message sent to the beneficiary institution. Ordering institutions are encouraged, where possible, to include other identity information about the beneficiary in cover payment messages, where this is necessary to limit the risk of customer assets being incorrectly frozen, blocked or rejected, or of the cover payment being unduly delayed.

10.35 Cover intermediary institutions should establish clear policies and procedures to ensure, in real time, that the relevant fields for storing originator and beneficiary information in cross-border cover payment messages are not blank. In addition, they should develop and implement policies and procedures to monitor if the originator and beneficiary information in the cross-border cover payment messages is manifestly meaningless or incomplete. The monitoring may be done on a risk sensitive basis, subsequent to the processing of the transactions. Cover intermediary institutions should also implement other measures including screening the originator and beneficiary names against their database of terrorists and terrorist suspects.

10.36 Beneficiary institutions should identify and verify the beneficiary. They should also have effective risk-based procedures in place to identify and handle wire transfers lacking complete originator information.

APPENDIX A

Limits for conducting CDD for SVF products

1. Device-based SVF

Maximum Stored Value (in HK$)	CDD Requirement
≤ 3,000	No CDD required[49]
> 3,000	Normal CDD under Chapter 4 of this Guideline

2. Network-based SVF

(i) Non-reloadable (e.g. non-reloadable prepaid card, gift card)

Maximum Stored Value (in HK$)	CDD Requirement
≤ 8,000	No CDD required[49]
> 8,000	Identify and verify the customer's identity by obtaining a copy of the customer's identification document

[49] Depending on the product features (e.g. person-to-person fund transfer and cash withdrawal functions), the HKMA may impose additional risk mitigating measures on the SVF licensee.

(ii) Reloadable (e.g. reloadable prepaid card, internet-based payment platform)

<table>
<tr><th>Annual Transaction Amount (in HK$)</th><th>Payments for Goods or Services / Person-to-Person Fund Transfers</th><th>Cash Withdrawal Function</th></tr>
<tr><td>≤ 8,000</td><td rowspan="2">No CDD required[50] / Collect the customer's identification information</td><td>Identify and verify the customer's identity by:
(i) means of linkage with the customer's account in a licensed bank or the customer's credit card issued by an AI or an AI's subsidiary; or
(ii) obtaining a copy of the customer's identification document</td></tr>
<tr><td>> 8,000
to
≤ 25,000</td><td rowspan="3">Normal CDD under Chapter 4 of this Guideline</td></tr>
<tr><td>> 25,000
to
≤ 100,000</td><td>Identify and verify the customer's identity by:
(i) means of linkage with the customer's account in a licensed bank or the customer's credit card issued by an AI or an AI's subsidiary; or
(ii) obtaining a copy of the customer's identification document</td></tr>
<tr><td>> 100,000</td><td>Normal CDD under Chapter 4 of this Guideline</td></tr>
</table>

[50] The maximum stored value should not exceed HK$3,000. However, the HKMA may, on an exceptional basis and based on the functionalities and related risk mitigating measures of each SVF product, impose a higher or lower maximum stored value.

APPENDIX B

Examples of reliable and independent sources for customer identification purposes

1 The identity of an individual physically present in Hong Kong should be verified by reference to their Hong Kong identify card or travel document. SVF licensees should always identify and/or verify a Hong Kong resident's identity by reference to their Hong Kong identity card, certificate of identity or document of identity. The identity of a non-resident should be verified by reference to their valid travel document.

2 For non-resident individuals who are not physically present in Hong Kong, SVF licensees may identify and / or verify their identity by reference to the following documents:

(a) a valid international passport or other travel document;
(b) a current national (i.e. Government or State-issued) identity card bearing the photograph of the individual; or
(c) current valid national (i.e. Government or State-issued) driving licence[51] incorporating photographic evidence of the identity of the applicant, issued by a competent national or state authority.

3 Travel document means a passport or some other document furnished with a photograph of the holder establishing the identity and nationality, domicile or place of permanent residence of the holder. The following documents constitute travel documents for the purpose of identity verification:

(a) Permanent Resident Identity Card of Macau Special Administrative Region;
(b) Mainland Travel Permit for Taiwan Residents;
(c) Seaman's Identity Document (issued under and in accordance with the International Labour Organisation Convention/Seafarers Identity Document Convention 1958);
(d) Taiwan Travel Permit for Mainland Residents;
(e) Permit for residents of Macau issued by Director of Immigration;
(f) Exit-entry Permit for Travelling to and from Hong Kong and Macau for Official Purposes; and
(g) Exit-entry Permit for Travelling to and from Hong Kong and Macau.

[51] For the avoidance of doubt, international driving permits and licences are not acceptable for this purpose.

4 For minors born in Hong Kong who are not in possession of a valid travel document or Hong Kong identity card[52], their identity should be verified by reference to the minors' Hong Kong birth certificates. Whenever establishing a business relationship with a minor, the identity of the minor's parent or guardian representing or accompanying the minor should also be recorded and verified in accordance with the above requirements.

5 An SVF licensee may identify and/or verify a corporate customer by performing a company registry search in the place of incorporation and obtaining a full company search report, which confirms the current reference to a full company particulars search (or overseas equivalent).

6 For jurisdictions that do not have national identity cards and where customers do not have a travel document or driving licence with a photograph, SVF licensees may, exceptionally and applying an RBA, accept other documents as evidence of identity. Wherever possible such documents should have a photograph of the individual.

[52] All residents of Hong Kong who are aged 11 and above are required to register for an identity card. Hong Kong permanent residents will have a Hong Kong Permanent Identity Card. The identity card of a permanent resident (i.e. a Hong Kong Permanent Identity Card) will have on the front of the card a capital letter "A" underneath the individual's date of birth.

APPENDIX C

CONFIDENTIAL 機密

Joint Financial Intelligence Unit

G.P.O. Box No. 6555, General Post Office, Hong Kong

Tel : 2866 3366 Fax : 2529 4013
Email : jfiu@police.gov.hk

Date: 2012-XX-XX

Money Laundering Reporting Officer,
XXXXXXX.

Fax No. : XXXX XXXX

Dear Sir/Madam,

Suspicious Transaction Report ("STR")

JFIU No.	Your Reference	Date Received
XX	XX	XX

I acknowledge receipt of the above mentioned STR made in accordance with the provisions of section 25A(1) of the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap 405) / Organized and Serious Crimes Ordinance (Cap 455) and section 12(1) of the United Nations (Anti-Terrorism Measures) Ordinance (Cap 575).

Based upon the information currently in hand, consent is given in accordance with the provisions of section 25A(2) of the Drug Trafficking (Recovery of Proceeds) Ordinance and Organized and Serious Crimes Ordinance, and section 12(2) of United Nations (Anti-Terrorism Measures) Ordinance.

Should you have any queries, please feel free to contact Senior Inspector Mr. XXXXX on (852) 2860 XXXX.

Yours faithfully,

(XXXXX)
for Head, Joint Financial Intelligence Unit

PERSONAL DATA

CONFIDENTIAL 機密

Joint Financial Intelligence Unit

G.P.O. Box No. 6555, General Post Office, Hong Kong
Tel : 2866 3366 Fax : 2529 4013
Email : jfiu@police.gov.hk

Our Ref. :
Your Ref :

2012-XX-XX

Money Laundering Reporting Officer,
XXXXXX
Fax No. : XXXX XXXX

Dear Sir/Madam,

Drug Trafficking (Recovery of Proceeds) Ordinance/
Organized and Serious Crimes Ordinance

I refer to your disclosure made to JFIU under the following reference:

JFIU No.	Your Reference	Dated
XX	XX	XX

Your disclosure is related to an investigation of 'XXXXX' by officers of XXXXX under reference XXXXX.

In my capacity as an Authorized Officer under the provisions of section 25A(2) of the Organized and Serious Crimes Ordinance, Cap. 455 ("OSCO"), I wish to inform you that you do NOT have my consent to further deal with the funds in the account listed in Annex A since the funds in the account are believed to be crime proceeds.

As you should know, dealing with money known or reasonably believed to represent the proceeds of an indictable offence is an offence under section 25 of OSCO. This information should be treated in strict confidence and disclosure of the contents of this letter to any unauthorized person, including the subject under investigation which is likely to prejudice the police investigation, may be an offence under section 25A(5) OSCO. Neither the accounts holder nor any other person should be notified about this correspondence.

CONFIDENTIAL 機密

If any person approaches your institution and attempts to make a transaction involving the account, please ask your staff to immediately contact the officer-in-charge of the case, and decline the transaction. Should the account holder or a third party question the bank as to why he cannot access the funds in the accounts he should be directed to the officer-in-charge of the case, without any further information being revealed.

Please contact the officer-in-charge, Inspector XXXXX on XXXX XXXX or the undersigned should you have any other query or seek clarification of the contents of this letter.

Yours faithfully,

(XXXXXXX)
Superintendent of Police
Head, Joint Financial Intelligence Unit

c.c. OC Case

Annex A

S/N	Account holder	Account Number
1.		

GLOSSARY OF KEY TERMS AND ABBREVIATIONS	
Terms / abbreviations	**Meaning**
AI(s)	Authorized institution(s)
AMLO	Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615)
AML/CFT	Anti-money laundering and counter financing of terrorism
CDD	Customer due diligence
CO	Compliance officer
Connected parties	Connected parties to a customer include the beneficial owner and any natural person having the power to direct the activities of the customer. For the avoidance of doubt the term connected party will include any director, shareholder, beneficial owner, signatory, trustee, settlor/grantor/founder, protector(s), or defined beneficiary of a legal arrangement.
DTROP	Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405)
EDD	Enhanced customer due diligence
FATF	Financial Action Task Force
FI(s)	Financial institution(s)
HKMA	Hong Kong Monetary Authority
Individual	Individual means a natural person, other than a deceased natural person.
JFIU	Joint Financial Intelligence Unit
Minor	Minor means a person who has not attained the age of 18 years [Interpretation and General Clauses Ordinance (Cap. 1) - section 3].
MLRO	Money laundering reporting officer
ML/TF	Money laundering and/or terrorist financing
OSCO	Organized and Serious Crimes Ordinance (Cap. 455)
PEP(s)	Politically exposed person(s)

PSSVFO	Payment Systems and Stored Value Facilities Ordinance (Cap. 584)
RA(s)	Relevant authority (authorities)
RBA	Risk-based approach
SDD	Simplified customer due diligence
Senior management	Senior management means directors (or board) and senior managers (or equivalent) of a firm who are responsible, either individually or collectively, for management and supervision of the firm's business. This may include a firm's Chief Executive Officer, Managing Director, or other senior operating management personnel (as the case may be).
STR(s)	Suspicious transaction report(s); also referred to as reports or disclosures
Streamlined approach	Streamlined customer due diligence
SVF	Stored value facility
Trust	For the purposes of the guideline, a trust means an express trust or any similar arrangement for which a legal-binding document (i.e. a trust deed or in any other form) is in place.
UNATMO	United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575)
UN	United Nations
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution
UNSO	United Nations Sanctions Ordinance (Cap. 537)