Guideline on Anti-Money Laundering and Counter-Financing of Terrorism

(For Stored Value Facility Licensees)

Revised September 2020

CONTENTS

OVERVIEW		
Introduction		
	1.	This Guideline is published under section 54(1A)(b) of the Payment Systems and Stored Value Facilities Ordinance (PSSVFO) and takes effect on 2 July 2021.
	2.	Terms and abbreviations used in this Guideline should be interpreted by reference to the definitions set out in the Glossary part of this Guideline. Where applicable, 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) and sets out the relevant anti-money laundering and counter-financing of terrorism (AML/CFT) statutory and regulatory requirements, and the AML/CFT standards which stored value facility (SVF) licensees (which are not licensed banks[1]) or licensed banks (hereafter referred collectively as "SVF licensees") for the issue of SVF, should meet in order to comply with the statutory requirements under the PSSVFO. Compliance with this Guideline is enforced through the PSSVFO. SVF licensees which fail to comply with this Guideline may be subject to disciplinary or other actions under the PSSVFO for non-compliance with the relevant requirements.
	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]
	5.	This Guideline is intended for use by SVF licensees and their officers and staff. This Guideline also: (a) provides a general background on the subjects of money laundering and terrorist financing (ML/TF), including a summary of the main provisions of the applicable AML/CFT legislation in Hong Kong; and (b) provides practical guidance to assist SVF licensees and their 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.

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.

	6.	The relevance and usefulness of this Guideline will be kept under review and it may be necessary to issue amendments from time to time.
	7.	For the avoidance of doubt, the use of the word "must" or "should" in relation to an action, consideration or measure referred to in this Guideline indicates that it is a mandatory requirement. The content of this Guideline is not intended to be an exhaustive list of the means of meeting the statutory and regulatory requirements. SVF licensees should therefore use this Guideline as a basis to develop measures appropriate to their structure and business activities.
	8.	This Guideline also 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.
	9.	A failure to comply with any provision of this Guideline may reflect adversely on whether an SVF licensee continues to comply with the minimum criteria for licence granted set out in section 6 of Part 2 of Schedule 3 to the PSSVFO, which requires an SVF licensee to have in place adequate and appropriate systems of control for preventing or combating possible money laundering or terrorist financing. The HKMA is empowered to exercise various provisions under the PSSVFO in case of non-compliance with the requirements set out in this Guideline.
The nature of money laundering and terrorist financing		
	10.	The term "money laundering" (ML) 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.
	11.	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.
	12.	The term "terrorist financing" (TF) 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.
	13.	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, terrorist financing, financing of proliferation of weapons of mass destruction and financial sanctions		
	14.	The Financial Action Task Force (FATF) is an inter-governmental body formed in 1989. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating of ML, TF, the financing of proliferation of weapons of mass destruction (PF), and other related threats to the integrity of the international financial system. The FATF has developed a series of Recommendations that are recognised as the international standards for combating of ML, TF and PF. They form the basis for a co-ordinated response

		to these threats to the integrity of the financial system and help ensure a level playing field. 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 other monitored 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 latest FATF Recommendations[3] 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.
	15.	The main pieces of legislation in Hong Kong in relation to SVF licensees that are concerned with ML, TF, PF and financial sanctions are: (a) the PSSVFO - dealing with preventive measures that should be implemented by SVF licensees; (b) the Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP) and the Organized and Serious Crimes Ordinance (OSCO) - dealing with serious or organised crime; and (c) the United Nations (Anti-Terrorism Measures) Ordinance (UNATMO), the United Nations Sanctions Ordinance (UNSO) and the Weapons of Mass Destruction (Control of Provision of Services) Ordinance (WMD(CPS)O) - dealing with anti-terrorism, financial sanctions and PF. It is very important that SVF licensees and their officers and staff fully understand their respective responsibilities under the different legislation.
<u>PSSVFO</u>		
s.6, Part 2, Sch. 3, PSSVFO	16.	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 Ordinance (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.

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

s.33Q, PSSVFO	17.	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 loss avoided, by the SVF 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	18.	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 in compliance with the PSSVFO and this Guideline.
<u>DTROP</u>		
	19.	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.
<u>OSCO</u>		
	20.	The OSCO, among other things: (a) gives officers of the Hong Kong Police and the Customs and Excise Department powers to investigate organised crime and triad activities; (b) gives the Courts jurisdiction to confiscate the proceeds of organised 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 organised crime/triad related offence or other serious offences.
UNATMO		
	21.	The UNATMO is principally directed towards implementing decisions contained in relevant United Nations Security Council Resolutions (UNSCRs) aimed at preventing the financing of terrorist acts and combating the threats posed by foreign terrorist fighters. Besides the mandatory elements of the relevant UNSCRs, the UNATMO also implements the more pressing elements of the FATF Recommendations specifically related to TF.
s.25, DTROP & OSCO	22.	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, 8A, 13 & 14, UNATMO	23.	The UNATMO, among other things, criminalises 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	24.	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	25.	"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		
	26.	The UNSO provides for the imposition of sanctions against persons and against places outside the People's Republic of China arising

		from Chapter 7 of the Charter of the United Nations (UN). Most UNSCRs are implemented in Hong Kong under the UNSO.
WMD(CPS)O		
s.4, WMD(CPS)O	27.	The WMD(CPS)O controls the provision of services that will or may assist the development, production, acquisition or stockpiling of weapons capable of causing mass destruction or that will or may assist the means of delivery of such weapons. Section 4 of WMD(CPS)O prohibits a person from providing any services where he believes or suspects, on reasonable grounds, that those services may be connected to PF. The provision of services is widely defined and includes the lending of money or other provision of financial assistance.

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 Risk-based approach		
	1.2.1	The risk-based approach (RBA) is central to the effective implementation of an AML/CFT regime. RBA allows an SVF licensee to allocate its resources more effectively and apply preventive measures that are commensurate with the nature and level of risks, in order to focus its AML/CFT efforts in the most effective way.
	1.2.2	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 institutional and customer levels.
<u>Money laundering and terrorist financing risks related to SVF</u>		
	1.2.3	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 policies, procedures and controls (hereafter collectively referred to as "AML/CFT Systems") are applied, unacceptable ML/TF risks may arise. Effective and risk-based AML/CFT Systems and 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		
	1.2.4	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		
	1.2.5	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.
	1.2.6	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.[4]
Customer risk assessment		
	1.2.7	An SVF licensee should assess whether a business relationship presents a higher ML/TF risk and assign a ML/TF risk rating.
	1.2.8	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.
	1.2.9	Further details of RBA may be found in Chapter 2 of this Guideline.

[4] 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.

1.3 Compliance management arrangements and independent audit function		
Compliance management arrangements		
	1.3.1	An SVF licensee should have appropriate compliance management arrangements that facilitate the SVF licensee to implement AML/CFT Systems to comply with relevant legal and regulatory obligations as well as to manage ML/TF risks effectively. Compliance management arrangements should, at a minimum, include oversight by the SVF licensee's senior management, and appointment of a Compliance Officer (CO) and a Money Laundering Reporting Officer (MLRO).
Senior management oversight		
	1.3.2	The senior management of an SVF licensee is responsible for implementing effective AML/CFT Systems that can adequately manage the ML/TF risks identified. In particular, the senior management should: (a) appoint a CO at the management level to have the overall responsibility for the establishment and maintenance of the SVF licensee's AML/CFT Systems; (b) appoint a senior staff as the MLRO to act as the central reference point for suspicious transaction reporting; and (c) establish a (or designate an existing) board-level and/or management level committee to have the responsibility of oversight AML/CFT controls.
Independent audit function		
	1.3.3	An SVF licensee should establish an independent audit function with sufficient expertise and resources, which should have a direct reporting line to the senior management of the SVF licensee.
	1.3.4	The audit function should regularly review the AML/CFT Systems to ensure effectiveness. The frequency and extent of the review should be commensurate with the nature, size and complexity of its businesses and the ML/TF risks arising from those businesses.
	1.3.5	Further details on compliance management arrangements, the role of senior management, the function and roles of both the CO and MLRO as well as the independent audit function can be found in Chapter 3 of this Guideline.
1.4 Tiered approach to customer due diligence for SVF		
	1.4.1	In general, an SVF licensee should carry out customer due diligence (CDD) measures as set out in Chapter 4 of this Guideline in relation to a customer at the outset of a business relationship. Taking into account the lower level of ML/TF risks of some SVF products as determined by limitations to value stored and functionality and predominant use for low-value retail

		transactions[5], a tiered approach to customer due diligence (tiered approach) is allowed which permits certain due diligence measures to be performed in a particular manner or not performed under certain scenarios. For the avoidance of doubt, there is no exemption from the requirement to continuously monitor the business relationship in all cases.
	1.4.2	In order to apply the tiered approach, SVF licensees should ensure that the SVF product meets specific requirements on stored value, transaction limits and functions of payments for goods or services, person-to-person fund transfer[6] and cash withdrawal[7].
	1.4.3	The limits specified under the tiered 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 assessment of risks. Equally, the HKMA may, based on its assessment of 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 example, 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 CDD for SVF products could be found in the Appendix. The table should be read in conjunction with paragraphs 1.4.6 to 1.4.21.
Device-based SVF		
	1.4.6	Provided that a device-based SVF is used exclusively for domestic payments for goods or services[8] and its maximum stored value 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

5 SVF licensees may make reference to the "Stored Value Facility Sector: Money Laundering and Terrorist Financing Risk Assessment Report" published by the HKMA.

6 For the avoidance of doubt, an SVF licensee should also comply with the relevant requirements for remittance or wire transfers.

7 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 the avoidance of doubt, 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 any SVF product(s) 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.

8 For the purpose of this Guideline, a domestic payment for goods or services means a point-of-sale in or online payment to a merchant who carries on a business in Hong Kong. For the avoidance of doubt, an SVF product, including device-based and network-based SVF, used exclusively for domestic payments for goods or services is allowed to receive top-up payments from cash, person-to-person fund transfer and bank transfer.

		on the customer. These customers are regarded as unverified customers.
	1.4.7	Where a device-based SVF offered to an unverified customer is limited to funding from identifiable sources[9] only, its functions could also include cross-border payments for goods or services[10], subject to the maximum stored value not exceeding HK$3,000. SVF licensees should notify the HKMA in advance (e.g. 6 months) of other proposals involving cross-border payments for goods and services, supported by risk assessment and effective risk mitigating measures.
	1.4.8	CDD requirements for verified customers as set out in Chapter 4 of this Guideline should be applied if a device-based SVF has any of the following product features: (a) maximum stored value exceeding HK$3,000; (b) function of cross-border payments for goods or services and could be funded from unidentifiable sources; (c) person-to-person fund transfers function; or (d) cash withdrawal function.
Network-based SVF		
Non-reloadable network-based SVF		
	1.4.9	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.
	1.4.10	Provided that a non-reloadable network-based SVF is used exclusively for domestic payments for goods or services and its maximum stored value does not exceed HK$8,000, in general there is no requirement to conduct any due diligence on the customer. These customers are regarded as unverified customers.
	1.4.11	Where a non-reloadable network-based SVF offered to an unverified customer is limited to funding from an identifiable source only, its functions could also include cross-border payments

[9] For the purpose of this and other related paragraphs in this Guideline, an identifiable source may include (i) an account in a licensed bank, (ii) a credit card issued by an authorized institution or an authorized institution's subsidiary, (iii) an account of a verified customer or a pre-existing customer in an SVF licensee, or (iv) an account in 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. For the avoidance of doubt, any anonymous funding source, including cash, anonymous prepaid card or anonymous financial instrument would not be considered as an identifiable source.

[10] For the purpose of this Guideline, a cross-border payment for goods or services means a point-of-sale in or online payment to a merchant who carries on a business outside Hong Kong.

		for goods or services, subject to the maximum stored value not exceeding HK$8,000.[11]
	1.4.12	Additionally, for non-reloadable network-based SVFs with stored value not exceeding HK$8,000 and used exclusively for payments for goods or services, 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, CDD requirements for verified customers as set out in Chapter 4 of this Guideline should be applied.
	1.4.13	CDD requirements for verified customers as set out in Chapter 4 of this Guideline should be applied if a non-reloadable network-based SVF has any of the following product features: (a) maximum stored value exceeding HK$8,000; (b) function of cross-border payments for goods or services and could be funded from unidentifiable sources; (c) person-to-person fund transfers function; or (d) cash withdrawal function.
Reloadable network-based SVF		
	1.4.14	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.
	1.4.15	Provided that a reloadable network-based SVF (i) is used exclusively for domestic payments for goods or services; (ii) its maximum stored value does not exceed HK$3,000[12]; and (iii) the annual transaction amount does not exceed HK$25,000, in general there is no requirement to conduct any due diligence on the customer. These customers are regarded as unverified customers.
	1.4.16	Where a reloadable network-based SVF offered to an unverified customer is limited to funding from identifiable sources only, it could also include the following functions, subject to the maximum stored value not exceeding HK$3,000 and annual transaction amount not exceeding HK$25,000: (a) cross-border payments for goods or services; and/or (b) person-to-person fund transfers to other accounts of the same SVF licensee.
	1.4.17	CDD requirements for verified customers as set out in Chapter 4 of this Guideline should be applied if a reloadable network-based SVF

[11] For a non-reloadable network-based SVF issued before the publication date of this revised Guideline, SVF licensees may allow the customer to use the remaining stored value for existing functions.

[12] 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.

		has any of the following product features: (a) maximum stored value exceeding HK$3,000; (b) annual transaction amount exceeding HK$25,000; (c) function of cross-border payments for goods or services and could be funded from unidentifiable sources; (d) person-to-person fund transfers function and could be funded from unidentifiable sources; or (e) cash withdrawal function.
Pre-existing customers		
	1.4.18	For customers of reloadable network-based SVFs with the business relationships established before the commencement date of this revised Guideline and where the SVF licensee had collected the customer's identification information, as well as (i) obtained a copy / copies of the customer's identification document(s); and/or (ii) established a linkage with the customer's account in a licensed bank or customer's credit card issued by an authorized institution[13] (AI) or an AI's subsidiary, the SVF licensee may complete measures as specified in paragraph 1.4.19 and continue to provide existing functions to these customers[14].
	1.4.19	Customers mentioned in paragraph 1.4.18 are regarded as pre-existing customers if the SVF licensee completed the following measures (in case the relevant measures were not previously conducted): (a) obtaining a copy of the customer's identification document; and (b) requiring the customer to make a transfer to the customer's SVF account from the customer's account in a licensed bank, provided that the SVF licensee is able to confirm that the name of bank account holder concerned matches the name of its customer.
	1.4.20	Where the pre-existing customer's annual transaction amount exceeds HK$100,000 or annual transaction amount of cash withdrawal exceeds HK$8,000, CDD requirements for verified customers as set out in Chapter 4 of this Guideline should be applied.
	1.4.21	For a customer mentioned in paragraph 1.4.18 who has not completed the measures as specified in paragraph 1.4.19 before the

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

[14] The SVF licensee should give adequate advance notice to the customers about the key differences in services offered by the SVF licensee to its unverified and verified customers, so that the customers can make informed decisions to subscribe or otherwise the most suitable services of the SVF licensee in all circumstances.

		date of commencement of this revised Guideline, the customer is regarded as an unverified customer[15] and the SVF licensee should follow relevant requirements as set out in paragraphs 1.4.15 to 1.4.17 above.
Internal controls for applying tiered approach		
	1.4.22	An SVF licensee applying the tiered 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 take appropriate risk mitigating measures 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 must not adopt the tiered approach and should conduct the CDD requirements for verified customers, as set out in Chapter 4 of this Guideline, at the outset of the business relationship.
	1.4.25	In addition, the tiered 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. Under such situations, the SVF licensee should carry out the CDD and enhanced 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[16].

[15] The SVF licensee may still conduct the measures as specified in paragraph 1.4.19 for relevant customers not later than 6 months after commencement of this revised Guideline.

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

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	Ongoing monitoring is an essential component of effective AML/CFT Systems. An SVF licensee should continuously monitor its business relationship with a customer through ongoing CDD and transaction monitoring.
	1.5.2	Although the SVF licensees are allowed to apply the tiered approach in identifying and verifying the customer's identity, 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 Terrorist financing, financial sanctions and proliferation financing		
	1.6.1	UNATMO is an ordinance to further implement a decision under UNSCR 1373 (2001) relating to measures for prevention of terrorist acts and a decision under UNSCR 2178 (2014) relating to the prevention of travel for the purpose of terrorist acts or terrorist training; as well as to implement certain terrorism-related multilateral conventions and certain FATF Recommendations.

	1.6.2	The UNSO empowers the Chief Executive to make regulations to implement sanctions decided by the United Nations Security Council (UNSC), including targeted financial sanctions against individuals and entities designated by the UNSC or its Committees. Designated persons and entities are specified by notice published in the Gazette or on the website of the Commerce and Economic Development Bureau. It is an offence to make available, directly or indirectly, any funds, or other financial assets, or economic resources, to, or for the benefit of, a designated person or entity, as well as those acting on their behalf, at their direction, or owned or controlled by them; or to deal with any funds, other financial assets or economic resources belonging to, or owned or controlled by, such persons and entities, except under the authority of a licence granted by the Chief Executive.
	1.6.3	The counter proliferation financing regime in Hong Kong is implemented through legislation, including the regulations made under the UNSO which are specific to Democratic People's Republic of Korea (DPRK) and the Islamic Republic of Iran (Iran), and the WMD(CPS)O.
	1.6.4	An SVF licensee should establish and maintain effective policies, procedures and controls to ensure compliance with the relevant regulations and legislation on TF, financial sanctions and PF.
	1.6.5	To avoid establishing business relationship or conducting transactions with any terrorist suspects and possible designated parties, an SVF licensee should implement an effective screening mechanism.
	1.6.6	Further details on TF, financial sanctions and PF can be found in Chapter 6 of this Guideline.
1.7 Suspicious transaction reports		
	1.7.1	It is a statutory obligation under sections 25A(1) of the DTROP and the OSCO, as well as section 12(1) of the UNATMO, that where a person knows or suspects that any property: (a) in whole or in part directly or indirectly represents any person's proceeds of, (b) was used in connection with, or (c) is intended to be used in connection with drug trafficking or an indictable offence; or that any property is terrorist property, the person shall as soon as it is reasonable for him to do so, file a suspicious transaction report (STR) with the Joint Financial Intelligence Unit (JFIU).
	1.7.2	An SVF licensee should 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 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.
	1.7.3	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.
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 CDD information throughout the business relationship with the customers and for a period of at least five years after the end of the business relationship and transaction records for a period of at least five 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	For any transaction falls within the definition of a wire transfer, an SVF licensee should comply with the requirements for wire transfers in Chapter 10 of this Guideline.
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-Financing of Terrorism (For Money Service Operators)[17]. By virtue of the nature of the SVF licensee's business, an SVF licensee should also comply with the requirements under paragraphs 1.11.2 to 1.11.5. Depending on the features of the money service business, the HKMA may impose additional risk mitigating measures on the SVF licensee.
Money changing service		
	1.11.2	An SVF licensee that operates a money changing service[18] 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 CDD for verified customers 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[19], other than a wire transfer, of HK$8,000 or above or of an equivalent amount in any other currency, whether carried out in a single operation or several operations that appear to the SVF licensee to be linked: (a) identify the originator; (b) verify the identity of the originator by reference to the originator's identification document in compliance with Chapter 4 of this Guideline; 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 SVF licensee that operates a remittance service that is ancillary to its principal business should before carrying out a remittance transaction, other than a wire transfer, of amount below HK$8,000 or of an equivalent amount in any other currency, record (i) the

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

[18] 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.

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

		originator's name; (ii) the currency and amount involved; and (iii) the date and time of receipt of the instruction, the recipient's name and address[20] and the method of delivery.
	1.11.5	An originator of a remittance transaction is: (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.

[20] Other than the recipient's address, an SVF licensee may record the recipient's account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

Chapter 2 – RISK-BASED APPROACH		
Introduction		
	2.1	The risk-based approach (RBA) is central to the effective implementation of an AML/CFT regime. An RBA to AML/CFT means that jurisdictions, competent authorities, and SVF licensees are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate with those risks in order to manage and mitigate them effectively. RBA allows an SVF licensee to allocate its resources more effectively and apply preventive measures that are commensurate with the nature and level of risks, in order to focus its AML/CFT efforts in the most effective way. Therefore, an SVF licensee should adopt an RBA in the design and implementation of its AML/CFT Systems with a view to managing and mitigating ML/TF risks.
Institutional ML/TF risk assessment		
	2.2	The institutional ML/TF risk assessment forms the basis of the RBA, enabling an SVF licensee to understand how and to what extent it is vulnerable to ML/TF. The SVF licensee should conduct an institutional ML/TF risk assessment to identify, assess and understand its ML/TF risks in relation to: (a) its customers; (b) the countries or jurisdictions its customers are from or in; (c) the countries or jurisdictions the SVF licensee has operations in; and (d) the products, services, transactions and delivery channels of the SVF licensee.
	2.3	The appropriate steps to conduct the institutional ML/TF risk assessment should include: (a) documenting 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) considering all the relevant risk factors before determining what the level of overall risk is, and the appropriate level and type of mitigation to be applied; (c) obtaining the approval of senior management on the risk assessment results; (d) having a process by which the risk assessment is kept up-to-date; and (e) having appropriate mechanisms to provide the risk assessment to the HKMA when required to do so.

	2.4	In conducting the institutional ML/TF risk assessment, an SVF licensee should cover a range of factors, including: (a) customer risk factors, for example: (i) its target market and customer segments; (ii) the number and proportion of customers identified as high risk; (b) country risk factors, for example: (i) the countries or jurisdictions it is exposed to, either through its own activities or the activities of customers, especially countries or jurisdictions identified by credible sources, with relatively higher level of corruption or organised crime, and/or not having effective AML/CFT regimes; (c) product, service, transaction or delivery channel risk factors, for example: (i) the nature, scale, diversity and complexity of its business; (ii) the characteristics of products and services offered, and the extent to which they are vulnerable to ML/TF abuse; (iii) the volume and size of its transactions; (iv) the delivery channels, including the extent to which the SVF licensee deals directly with the customer, the extent to which the SVF licensee relies on (or is allowed to rely on) third party to conduct CDD, the extent to which the SVF licensee uses technology, and the extent to which these channels are vulnerable to ML/TF abuse; (d) other risk factors, for example: (i) the nature, scale and quality of available ML/FT risk management resources, including appropriately qualified staff with access to ongoing AML/CFT training and development; (ii) compliance and regulatory findings; (iii) results of internal or external audits.
	2.5	The scale and scope of the institutional ML/TF risk assessment should be commensurate with the nature, size and complexity 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.
	2.6	The institutional ML/TF risk assessment should consider any higher risks identified in other relevant risk assessments which may be issued from time to time, such as Hong Kong's jurisdiction-wide

		ML/TF risk assessment and any higher risks notified to the SVF licensees by the HKMA.
	2.7	A locally-incorporated SVF licensee with branches or subsidiaries, including those located outside Hong Kong, should perform a group-wide ML/TF risk assessment.
	2.8	For the purpose of paragraphs 2.2 and 2.7, if an SVF licensee is a part of a financial group and a group-wide or regional ML/TF risk assessment has been conducted, it may make reference to or rely on those assessments provided that the assessments adequately reflect ML/TF risks posed to the SVF licensee in the local context.
	2.9	To keep the institutional ML/TF risk assessment up-to-date, an SVF licensee should conduct its assessment every two years and upon trigger events which are material to the SVF licensee's business and risk exposure.
New products, new business practices and use of new technologies		
	2.10	An SVF licensee should identify and assess the ML/TF risks that may arise in relation to: (a) the development of new products and new business practices, including new delivery mechanisms; and (b) the use of new or developing technologies for both new and pre-existing products.
	2.11	An SVF licensee should undertake the risk assessment prior to the launch of the new products, new business practices, or the use of new or developing technologies, and should take appropriate measures to manage and mitigate the risks identified.
Customer risk assessment		
	2.12	An SVF licensee should assess the ML/TF risks associated with a proposed business relationship, which usually referred as a customer risk assessment. The assessment conducted would determine the extent of CDD measures to be applied[21]. This means that the amount and type of information obtained, and the extent to which this information is verified, should be increased where the ML/TF risks associated with the business relationship are higher. It may also be simplified where the ML/TF risks associated with the business relationship is lower. The risk assessment conducted will also assist the SVF licensee to differentiate between the risks

[21] For the avoidance of doubt, except for certain situations specified in paragraph 1.4 and Chapter 4, an SVF licensee should always apply all the CDD measures set out in paragraph 4.1.3 and conduct ongoing monitoring of its customers.

		of individual customers and business relationships, as well as apply appropriate and proportionate CDD and risk mitigating measures[22].
	2.13	Based on a holistic view of the information obtained in the context of the application of CDD measures, an SVF licensee should be able to finalise the customer risk assessment[23], which determines the level and type of ongoing monitoring (including ongoing CDD and transaction monitoring), and support the SVF licensee's decision whether to enter into, continue or terminate, the business relationship. As the customer risk profile will change over time, an SVF licensee should review and update the risk assessment of a customer from time to time, particularly during ongoing monitoring.
	2.14	Similar to other parts of the AML/CFT Systems, an SVF licensee should adopt an RBA in the design and implementation of its customer risk assessment framework, and the complexity of the framework should be commensurate with the nature and size of the SVF licensee's business, and should be designed based on the results of SVF licensee's institutional ML/TF risk assessment. In general, the customer risk assessment framework will include customer risk factors; country risk factors; and product, service, transaction or delivery channel risk factors[24].
	2.15	An SVF licensee should keep records and relevant documents of its customer risk assessments so that it can demonstrate to the HKMA, among others: (a) how it assesses the customer's ML/TF risks; and (b) the extent of CDD measures and ongoing monitoring is appropriate based on that customer's ML/TF risks.

[22] An SVF licensee should adopt a balanced and common sense approach when conducting a customer risk assessment and applying CDD measures, which should not pose an unreasonable barrier to bona fide businesses and individuals accessing services offered by the SVF licensee.

[23] This is sometimes also called a "customer risk profile".

[24] Further guidance can be found in Chapter 4.

Chapter 3 – AML/CFT SYSTEMS		
AML/CFT Systems		
s.6, Part 2, Sch. 3, PSSVFO	3.1	An SVF licensee must put in place adequate and appropriate systems of control for preventing or combating possible ML/TF. To ensure compliance with this requirement, the SVF licensee should implement appropriate AML/CFT Systems following the RBA as stated in paragraph 2.1.
	3.2	An SVF licensee should: (a) have AML/CFT Systems, which are approved by senior management, to enable the SVF licensee to effectively manage and mitigate the risks that are relevant to the SVF licensee; (b) monitor the implementation of those AML/CFT Systems referred to in (a), and to enhance them if necessary; and (c) take enhanced measures to manage and mitigate the risks where higher risks are identified.
	3.3	The nature, scale and complexity of AML/CFT Systems may be simplified provided that: (a) the SVF licensee complies with the requirements set out in this Guideline, in particular the requirements set out in paragraphs 2.2, 2.3 and 3.2; and; (b) the lower ML/TF risks which form the basis for doing so have been identified through an appropriate risk assessment (e.g. institutional ML/TF risk assessment); and (c) simplified AML/CFT Systems, which are approved by senior management, are subject to review from time to time. However, AML/CFT Systems are not permitted to be simplified whenever there is a suspicion of ML/TF.
	3.4	An SVF licensee should implement AML/CFT Systems having regard to the nature, size and complexity of its businesses and the ML/TF risks arising from those businesses, and which should include: (a) compliance management arrangements; (b) an independent audit function; (c) employee screening procedures; and (d) an ongoing employee training programme (see Chapter 9).

Compliance management arrangements		
	3.5	An SVF licensee should have appropriate compliance management arrangements that facilitate the SVF licensee to implement AML/CFT Systems to comply with relevant legal and regulatory obligations as well as to manage ML/TF risks effectively. Compliance management arrangements should, at a minimum, include oversight by the SVF licensee's senior management, and appointment of a CO and a MLRO[25].
Senior management oversight		
	3.6	Effective ML/TF risk management requires adequate governance arrangements. The board of directors or its delegated committee (where applicable), and senior management of an SVF licensee should have a clear understanding of its ML/TF risks and ensure that the risks are adequately managed. Management information regarding ML/TF risks and the AML/CFT Systems should be communicated to them in a timely, complete, understandable and accurate manner so that they are equipped to make informed decisions.
	3.7	The senior management of an SVF licensee is responsible for implementing effective AML/CFT Systems that can adequately manage the ML/TF risks identified. In particular, the senior management should appoint a CO at the management level to have the overall responsibility for the establishment and maintenance of the SVF licensee's AML/CFT Systems; and a senior staff as the MLRO to act as the central reference point for suspicious transaction reporting.
	3.8	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: (a) appropriately qualified with sufficient AML/CFT knowledge; (b) subject to constraint of size of the SVF licensee, independent of all operational and business functions; (c) normally based in Hong Kong; (d) of a sufficient level of seniority and authority within the SVF licensee; (e) 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 effective measures to protect itself against the risks of ML/TF;

[25] Depending on the size of an SVF licensee, the functions of CO and MLRO may be performed by the same person.

		(f) fully conversant with the SVF licensee's statutory and regulatory requirements and the ML/TF risks arising from the SVF licensee's business; (g) 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 (h) 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		
	3.9	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 identified, understood and managed. In particular, the CO should assume responsibility for: (a) developing and/or continuously reviewing the SVF licensee's AML/CFT Systems, including any group-wide AML/CFT Systems in the case of a Hong Kong-incorporated SVF licensee, to ensure they remain up-to-date, meet current statutory and regulatory requirements, and are effective in managing ML/TF risks arising from the SVF licensee's business; (b) overseeing all aspects of the SVF licensee's AML/CFT Systems which include monitoring effectiveness and enhancing the controls and procedures where necessary; (c) communicating key AML/CFT issues with senior management, including, where appropriate, significant compliance deficiencies; and (d) ensuring AML/CFT staff training is adequate, appropriate and effective.
	3.10	An SVF licensee should appoint an MLRO as a central reference point for reporting suspicious transactions and also as the main point of contact with the JFIU and law enforcement agencies. The MLRO should play an active role in the identification and reporting of suspicious transactions. Principal functions of the MLRO should include having oversight of: (a) review of 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) maintenance of all records related to such internal reviews; and (c) provision of guidance on how to avoid tipping off.

Independent audit function		
	3.11	An SVF licensee should establish an independent audit function[26] which should have a direct line of communication to the senior management of the SVF licensee. The function should have sufficient expertise and resources to enable it to carry out its responsibilities, including independent reviews of the SVF licensee's AML/CFT Systems.
	3.12	The audit function should regularly review the AML/CFT Systems to ensure effectiveness. The review should include, but not be limited to: (a) adequacy of the SVF licensee's AML/CFT Systems, ML/TF risk assessment framework and application of RBA; (b) effectiveness of suspicious transaction reporting systems; (c) effectiveness of the compliance function; and (d) level of awareness of staff having AML/CFT responsibilities.
	3.13	The frequency and extent of the review should be commensurate with the nature, size and complexity of its businesses and the ML/TF risks arising from those businesses. Where appropriate, the SVF licensee should also seek a review from external parties.
Employee screening		
	3.14	An SVF licensee should have adequate and appropriate screening procedures in order to ensure high standards when hiring employees.
Group-wide AML/CFT Systems		
	3.15	Subject to paragraphs 3.18 and 3.19, a Hong Kong-incorporated SVF licensee with overseas branches or subsidiary undertakings[27] that carry on the same business as a financial institution (FI) as defined in the AMLO should implement group-wide AML/CFT Systems to apply the requirements set out in this Guideline[28] to all of its overseas branches and subsidiary undertakings in its financial group, wherever the requirements in this Guideline are relevant and applicable to the overseas branches and subsidiary undertakings concerned.

[26] Reference should be made to relevant parts of "Guideline on Supervision of Stored Value Facility Licensees".

[27] An SVF licensee should contact the HKMA at an early stage to discuss its intention to establish an overseas branch or subsidiary undertaking.

[28] For the avoidance of doubt, these include, but not limited to, the requirements set out in paragraph 3.4.

	3.16	In particular, a Hong Kong-incorporated SVF licensee should, through its group-wide AML/CFT Systems, ensure that all of its overseas branches, and subsidiary undertakings that carry on the same business as an FI as defined in the AMLO, have procedures in place to ensure compliance with the CDD and record-keeping requirements similar to those set out in this Guideline, to the extent permitted by the laws and regulations of that place.
	3.17	To the extent permitted by the laws and regulations of the jurisdictions involved and subject to adequate safeguards on the protection of confidentiality and use of information being shared, including safeguards to prevent tipping off, a Hong Kong-incorporated SVF licensee should also implement, through its group-wide AML/CFT Systems, for: (a) sharing information required for the purposes of CDD and ML/TF risk management; and (b) provision to the SVF licensee's group-level compliance, audit and/or AML/CFT functions, of customer, account, and transaction information from its overseas branches and subsidiary undertakings that carry on the same business as an FI as defined in the AMLO, when necessary for AML/CFT purposes[29].
	3.18	If the AML/CFT requirements in the jurisdiction where the overseas branch or subsidiary undertaking of a Hong Kong-incorporated SVF licensee is located (host jurisdiction) differ from those relevant requirements referred to in paragraph 3.15, the SVF licensee should require that branch or subsidiary undertaking to apply the higher of the two sets of requirements, to the extent that host jurisdiction's laws and regulations permit.
	3.19	If the host jurisdiction's laws and regulations do not permit the branch or subsidiary undertaking of a Hong Kong-incorporated SVF licensee to apply the higher AML/CFT requirements, particularly the CDD and record-keeping requirements set out in this Guideline, the SVF licensee should: (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 requirements.

[29] This should include information and analysis of transactions or activities which appear unusual (if such analysis was done); and could include an STR, its underlying information, or the fact that an STR has been submitted. Similarly, branches and subsidiary undertakings should receive such information from these group-level functions when relevant and appropriate to risk management.

Chapter 4 – CUSTOMER DUE DILIGENCE		
4.1 What CDD measures are		
	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 should carry out CDD (see paragraph 4.2). Wherever possible, this Guideline gives SVF licensees a degree of discretion in how they comply with the PSSVFO and put in place procedures for this purpose. In addition, an SVF licensee should, in respect of each kind of customer, business relationship, product and transaction, establish and maintain effective AML/CFT Systems for complying with the CDD requirements set out in this Chapter.
	4.1.2	An SVF licensee should apply an RBA when conducting CDD measures and the extent of CDD measures should be commensurate with the ML/TF risks associated with a business relationship. Where the ML/TF risks are high, the SVF licensee should conduct EDD measures (see paragraph 4.8). In low risk situations, the SVF licensee may apply simplified due diligence (SDD) measures (see paragraph 4.7).
	4.1.3	The following are CDD measures applicable to an SVF licensee: (a) identify the customer and verify the customer's identity using documents, data or information provided by a reliable and independent source (see paragraph 4.3); (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[30], measures to enable the SVF licensee to understand the ownership and control structure of the legal person or trust (see paragraph 4.4); (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 paragraph 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 documents, data or information provided by a reliable and independent source; and (ii) verify the person's authority to act on behalf of the customer (see paragraph 4.5).

[30] 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.

	4.1.4	The meaning of "customer"[31] should be inferred from its everyday meaning and in the context of the industry practice.
	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.
4.2 When CDD measures should be carried out		
	4.2.1	An SVF licensee should carry out CDD measures in relation to a customer: (a) at the outset of a business relationship (where the adoption of the tiered approach does not apply); (b) for the continuation of a business relationship where the limits, which apply to the use of the tiered 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.
	4.2.2	"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.
4.3 Identification and verification of identity – customer		
	4.3.1	An SVF licensee should identify the customer and verify the customer's identity by reference to documents, data or information provided by a reliable and independent source: (a) a governmental body; (b) the HKMA or any other relevant authority (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.
<u>Customer that is a natural person</u>[32]		
	4.3.2	For a customer that is a natural person, an SVF licensee should identify the customer by obtaining at least the following identification information:

[31] The term "customer" includes a client.
[32] For the purpose of this Guideline, the terms "natural person" and "individual" are used interchangeably.

		(a) full name; (b) date of birth; (c) nationality; and (d) unique identification number (e.g. identity card number or passport number) and document type.
	4.3.3	In verifying the identity of a customer that is a natural person, an SVF licensee should verify the name, date of birth, unique identification number and document type of the customer by reference to documents, data or information provided by a reliable and independent source, examples of which include: (a) Hong Kong identity card or other national identity card; (b) valid travel document (e.g. unexpired passport); or (c) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).
	4.3.4	The identification document obtained by an SVF licensee should contain a photograph of the customer. In exceptional circumstances where an SVF licensee is unable to obtain an identification document with a photograph, the SVF licensee may accept an identification document without a photograph if the associated risks have been properly assessed and mitigated.
	4.3.5	An SVF licensee should obtain the residential address information of a customer that is a natural person[33].
Customer that is a legal person[34]		
	4.3.6	For a customer that is a legal person, an SVF licensee should identify the customer by obtaining at least the following identification information: (a) full name; (b) date of incorporation, establishment or registration; (c) place of incorporation, establishment or registration (including address of registered office); (d) unique identification number (e.g. incorporation number or business registration number) and document type; and (e) principal place of business (if different from the address of

[33] For the avoidance of doubt, an SVF licensee may, under certain circumstances, require verification (on top of collection) of residential address from a customer for other purposes (e.g. group requirements, other local or overseas legal and regulatory requirements). In such circumstances, the SVF licensee should communicate clearly to the customer the reasons of requiring verification of address.

[34] Legal person refers to any entities other than natural person that can establish a permanent customer relationship with an SVF licensee or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, associations or other relevantly similar entities.

		registered office).
	4.3.7	In verifying the identity of a customer that is a legal person, an SVF licensee should normally verify its name, legal form, current existence (at the time of verification) and powers that regulate and bind the legal person by reference to documents, data or information provided by a reliable and independent source, examples of which include[35]: (a) certificate of incorporation; (b) record in an independent company registry; (c) certificate of incumbency; (d) certificate of good standing; (e) record of registration; (f) partnership agreement or deed; (g) constitutional document; or (h) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).
	4.3.8	For a customer that is a partnership or an unincorporated body, confirmation of the customer's membership of a relevant professional or trade association is likely to be sufficient to verify the identity of the customer as required in paragraph 4.3.7 provided that: (a) the customer is a well-known, reputable organisation; (b) the customer has a long history in its industry; and (c) there is substantial public information about the customer, its partners and controllers.
	4.3.9	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.
Customer that is a trust or other similar legal arrangement[36]		
	4.3.10	In respect of trusts, an SVF licensee should identify and verify the trust as a customer in accordance with the requirements set out in paragraphs 4.3.11 and 4.3.12. The SVF licensee should also regard the trustee as its customer if the trustee enters into a business relationship on behalf of the trust, which is generally the case if the trust does not possess a separate legal personality. In such a case, the SVF licensee should identify and verify the identity of the

[35] In some instances, an SVF licensee may need to obtain more than one document to meet this requirement. For example, a certificate of incorporation can only verify the name and legal form of the legal person in most circumstances but cannot act as a proof of current existence.

[36] Examples of legal arrangement include fiducie, treuhand and fideicomiso.

		trustee in line with the identification and verification requirements for a customer that is a natural person or a legal person, where applicable.
	4.3.11	For a customer that is a trust or other similar legal arrangement, an SVF licensee should identify the customer by obtaining at least the following identification information: (a) name of the trust or legal arrangement; (b) date of establishment or settlement; (c) the jurisdiction whose laws govern the trust or legal arrangement; (d) unique identification number (if any) granted by any applicable official bodies and document type (e.g. tax identification number or registered charity or non-profit organisation number); and (e) address of registered office (if applicable).
	4.3.12	In verifying the identity of a customer that is a trust or other similar legal arrangement, an SVF licensee should normally verify its name, legal form, current existence (at the time of verification) and powers that regulate and bind the trust or other similar legal arrangement by reference to documents, data or information provided by a reliable and independent source, examples of which include: (a) trust deed or similar instrument[37]; (b) record of an appropriate register[38] in the relevant country of establishment; (c) written confirmation from a trustee acting in a professional capacity[39]; (d) written confirmation from a lawyer who has reviewed the relevant instrument; or (e) written confirmation from a trust company which is within the same financial group as the SVF licensee, if the trust concerned is managed by that trust company.
<u>Reliability of documents, data or information</u>		
	4.3.13	In verifying the identity of a customer, an SVF licensee needs not establish accuracy of every piece of identification information collected in paragraphs 4.3.2, 4.3.6 and 4.3.11.

[37] Under exceptional circumstance, the SVF licensee may choose to retain a redacted copy.

[38] In determining whether a register is appropriate, the SVF licensee should have regard to adequate transparency (e.g. a system of central registration where a national registry records details on trusts and other legal arrangements registered in that country). Changes in ownership and control information would need to be kept up-to-date.

[39] "Trustees acting in their professional capacity" in this context means that they act in the course of a profession or business which consists of or includes the provision of services in connection with the administration or management of trusts (or a particular aspect of the administration or management of trusts).

	4.3.14	An SVF licensee should ensure that documents, data or information obtained for the purpose of verifying the identity of a customer as required in paragraphs 4.3.3, 4.3.7 and 4.3.12 is current at the time they are provided to or obtained by the SVF licensee.
	4.3.15	When using documents for verification, an SVF licensee should be aware that some types of documents are more easily forged than others, or can be reported as lost or stolen. Therefore, the SVF licensee should consider applying anti-fraud procedures that are commensurate with the risk profile of the person being verified.
	4.3.16	If a natural person customer or a person representing a legal person, a trust or other similar legal arrangement to establish a business relationship with an SVF licensee is physically present during the CDD process, the SVF licensee should generally have sight of original identification document by its staff and retain a copy of the document. However, there are a number of occasions where an original identification document cannot be produced by the customers (e.g. the original document is in electronic form). In such an occasion, the SVF licensee should take appropriate measures to ensure the reliability of identification documents obtained.
	4.3.17	If the business relationship with a natural person customer is established through remote on-boarding [40], an SVF licensee should employ technology solutions appropriate to mitigate the risks, particularly for impersonation risks, when identifying and verifying the identity of a natural person customer [41]. The technology solutions adopted by the SVF licensee should cover the following two aspects: (a) identity authentication – where the natural person customer's identity is obtained through electronic channels, the SVF licensee should take appropriate technology measures to ensure reliability of the document, data or information obtained for the purpose of verifying the customer's identity; and (b) identity matching – SVF licensees should use appropriate technology to link the natural person customer incontrovertibly to the identity provided in (a).
	4.3.18	Where the documents, data or information being used for the purposes of identification are in a foreign language, appropriate steps should be taken by the SVF licensee to be reasonably satisfied that the documents, data or information in fact provide evidence of

[40] For the purpose of this Guideline, remote on-boarding refers to the process of establishing a business relationship with a customer solely through an electronic channel such as mobile applications or internet.

[41] For the avoidance of doubt, an SVF licensee should also comply with the relevant requirements for customer not physically present for identification purposes as specified in paragraph 4.9.

		the customer's identity.
Connected parties		
	4.3.19	Where a customer is a legal person, a trust or other similar legal arrangement, an SVF licensee should identify all the connected parties[42] of the customer by obtaining their names.
	4.3.20	A connected party of a customer that is a legal person, a trust or other similar legal arrangement: (a) in relation to a corporation, means a director of the customer; (b) in relation to a partnership, means a partner of the customer; (c) in relation to a trust or other similar legal arrangement, means a trustee (or equivalent) of the customer; and (d) in other cases not falling within subsection (a), (b) or (c), means a natural person holding a senior management position or having executive authority in the customer.
4.4 Identification and verification of identity – beneficial owner		
	4.4.1	A beneficial owner is normally a natural person who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. An SVF licensee should identify any beneficial owner in relation to a customer, 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.
	4.4.2	The verification requirements for a customer and a beneficial owner are different. In determining what constitutes reasonable measures to verify the identity of a beneficial owner of a customer, an SVF licensee should consider and give due regard to the ML/TF risks posed by the customer and the business relationship.
	4.4.3	Where a natural person is identified as a beneficial owner, the SVF licensee should endeavour to obtain the same identification information as at paragraph 4.3.2 as far as possible.
Beneficial owner in relation to a natural person		
	4.4.4	In respect of a customer that is a natural person, there is no requirement on an SVF licensee to make proactive searches for beneficial owners of the customer in such a case, but the SVF licensee should make appropriate enquiries where there are indications that the customer is not acting on his own behalf.
Beneficial owner in relation to a legal person		
	4.4.5	The beneficial owner in relation to a corporation is:

[42] For the avoidance of doubt, if a connected party also satisfies the definition of a customer, a beneficial owner of the customer or a person purporting to act on behalf of the customer, the SVF licensee has to identify and verify the identity of that person with reference to relevant requirements set out in this Guideline.

		(a) an individual who – (i) owns or controls, directly or indirectly, including through a trust or bearer share holding, more than 25% of the issued share capital of the corporation; (ii) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights at general meetings of the corporation; or (iii) exercises ultimate control over the management of the corporation; or (b) if the corporation is acting on behalf of another person, means the other person.
	4.4.6	The beneficial owner in relation to a partnership is: (a) an individual who – (i) is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership; (ii) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights in the partnership; or (iii) exercises ultimate control over the management of the partnership; or (b) if the partnership is acting on behalf of another person, means the other person.
	4.4.7	In relation to an unincorporated body other than a partnership, beneficial owner: (a) means an individual who ultimately owns or controls the unincorporated body; or (b) if the unincorporated body is acting on behalf of another person, means the other person.
	4.4.8	For a customer that is a legal person, an SVF licensee should identify any natural person who ultimately has a controlling ownership interest (i.e. more than 25%) in the legal person and any natural person exercising control of the legal person or its management, and take reasonable measures to verify their identities. If there is no such natural person (i.e. no natural person falls within the definition of beneficial owners set out in paragraphs 4.4.5 to 4.4.7), the SVF licensee should identify the relevant natural persons who hold the position of senior managing official, and take reasonable measures to verify their identities.
	4.4.9	While an SVF licensee usually can identify who the beneficial owner of a customer is in the course of understanding the ownership and control structure of the customer, the SVF licensee

		may obtain an undertaking or declaration[43] from the customer on the identity of, and the information relating to, its beneficial owner. Nevertheless, in addition to the undertaking or declaration obtained, the SVF licensee should take reasonable measures to verify the identity of the beneficial owner (e.g. corroborating the undertaking or declaration with publicly available information).
	4.4.10	If the ownership structure of a customer involves different types of legal persons or legal arrangements, in determining who the beneficial owner is, an SVF licensee should pay attention to who has ultimate ownership or control over the customer, or who constitutes the controlling mind and management of the customer.
Beneficial owner in relation to a trust or other similar legal arrangement		
	4.4.11	The beneficial owner in relation to a trust is: (a) an individual who is entitled to a vested interest in more than 25% of the capital of the trust property, whether the interest is in possession or in remainder or reversion and whether it is defeasible or not; (b) the settlor of the trust; (c) a protector or enforcer of the trust; or (d) an individual who has ultimate control over the trust.
	4.4.12	Similar to a corporation, a trust or other similar legal arrangement can also be part of an intermediate layer in an ownership structure, and should be dealt with in similar manner to a corporation being part of an intermediate layer. For trusts, an SVF licensee should identify the settlor, the protector (if any), the enforcer (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate control over the trust (including through a chain of control or ownership), and take reasonable measures to verify their identities. For other similar legal arrangements, an SVF licensee should identify any natural person in equivalent or similar positions to a beneficial owner of a trust as stated above and take reasonable measures to verify the identity of such person. If a trust or other similar legal arrangement is involved in a business relationship and an SVF licensee does not regard the trustee (or equivalent in other similar legal arrangement) as its customer pursuant to paragraph 4.3.10 (e.g. when a trust appears as part of an intermediate layer), the SVF licensee should also identify the trustee and take reasonable measures to verify the identity of the trustee so that the SVF licensee is satisfied that it knows who the trustee is.

[43] In some jurisdictions, corporations are required to maintain registers of their beneficial owners (e.g. the significant controllers registers maintained in accordance with the Companies Ordinance of Hong Kong). An SVF licensee may refer to those registers to assist in identifying the beneficial owners of its customers. Where a register of the beneficial owners is not made publicly available, the SVF licensee may obtain the record directly from its customers.

	4.4.13	For a beneficiary of a trust designated by characteristics or by class, an SVF licensee should obtain sufficient information[44] concerning the beneficiary to satisfy the SVF licensee that it will be able to establish the identity of the beneficiary at the time of payout or when the beneficiary intends to exercise vested rights.
Ownership and control structure		
	4.4.14	Where a customer is not a natural person, an SVF licensee should understand its ownership and control structure, including identification of any intermediate layers (e.g. by reviewing an ownership chart of the customer). The objective is to follow the chain of ownerships to the beneficial owners of the customer.
	4.4.15	Where a customer has a complex ownership or control structure, an SVF licensee should obtain sufficient information for the SVF licensee to satisfy itself that there is a legitimate reason behind the particular structure employed.
Bearer shares		
	4.4.16	Bearer shares refer to negotiable instruments that accord ownership in a legal person to the person who possesses the bearer share certificate. Therefore, it is more difficult to establish the beneficial ownership of a company with bearer shares. An SVF licensee should adopt procedures to establish the identities of the beneficial owners of such shares and ensure that the SVF licensee is notified whenever there is a change of beneficial owner of such shares.
	4.4.17	Where bearer shares have been deposited with an authorised/registered custodian, an SVF licensee should seek independent evidence of this, for example confirmation from the registered agent that an authorised/registered custodian holds the bearer shares, together with the identities of the authorised/registered custodian and the person who has the right to those entitlements carried by the share. As part of the SVF licensee's ongoing periodic review, it should obtain evidence to confirm the authorised/registered custodian of the bearer shares.
	4.4.18	Where the shares are not deposited with an authorised/registered custodian, an SVF licensee should obtain declarations prior to account opening and annually thereafter from each beneficial owner of such shares. The SVF licensee should also require the customer to notify it immediately of any changes in the ownership of the shares.

[44] For example, an SVF licensee may ascertain and name the scope of the class of beneficiaries (e.g. children of a named individual).

Nominee shareholders		
	4.4.19	For a customer identified to have nominee shareholders in its ownership structure, an SVF licensee should obtain satisfactory evidence of the identities of the nominees, and the persons on whose behalf they are acting, as well as the details of arrangements in place, in order to determine who the beneficial owner is.
4.5 Identification and verification of identity – person purporting to act on behalf of the customer		
	4.5.1	A person may be appointed to act on behalf of a customer to establish business relationships, or may be authorised to give instructions to an SVF licensee to conduct various activities through the account or the business relationship established. Whether the person is considered to be a person purporting to act on behalf of the customer (PPTA) should be determined based on the nature of that person's roles and the activities which the person is authorised to conduct, as well as the ML/TF risks associated with these roles and activities. An SVF licensee should implement clear policies and procedures for determining who is considered to be a PPTA.
	4.5.2	If a person is a PPTA, an SVF licensee should: (a) identify the person and take reasonable measures to verify the person's identity on the basis of documents, data or information provided by- (i) a governmental body; (ii) the HKMA or any other RA; (iii) an authority in a place outside Hong Kong that performs functions similar to those of the HKMA or any other RA; or (iv) any other reliable and independent source that is recognised by the HKMA; and (b) verify the person's authority to act on behalf of the customer.
	4.5.3	An SVF licensee should identify and verify the identity of the PPTA in line with the identification and verification requirements for a customer that is a natural person or a legal person, where applicable.
	4.5.4	An SVF licensee should verify the authority of each PPTA by appropriate documentary evidence (e.g. board resolution or similar written authorisation).
4.6 Purpose and intended nature of business relationship		
	4.6.1	An SVF licensee should 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. The information obtained by the

		SVF licensee to understand the purpose and intended nature should be commensurate with the risk profile of the customer and the nature of the business relationship. In addition, where a customer is not a natural person, an SVF licensee should also understand the nature of the customer's business.
4.7 Simplified due diligence		
General		
	4.7.1	In general, an SVF licensee should carry out all four CDD measures set out in paragraph 4.1.3 and continuously monitor its business relationship (i.e. ongoing CDD and transaction monitoring). As stated in Chapter 2, the extent of four CDD measures and ongoing monitoring should be determined using an RBA.
	4.7.2	An SVF licensee may apply SDD measures in relation to a business relationship or transaction if it determines that, taking into account its risk assessment, the business relationship or transaction presents a low ML/TF risk.
	4.7.3	SDD measures should not be applied or continue to be applied, where: (a) the SVF licensee's risk assessment changes and it no longer considers that there is a low degree of ML/TF risk; (b) where the SVF licensee suspects ML or TF; or (c) where there are doubts about the veracity or accuracy of documents or information previously obtained for the purposes of identification or verification.
	4.7.4	The assessment of low risks should be supported by an adequate analysis of ML/TF risks by the SVF licensee.
	4.7.5	The SDD measures applied should be commensurate with the nature and level of ML/TF risk, based on the lower ML/TF risk factors identified by the SVF licensee.
	4.7.6	When an SVF licensee applies SDD measures, it is still required to continuously monitor its business relationship (i.e. ongoing CDD and transaction monitoring) in accordance with Chapter 5 of this Guideline.
	4.7.7	Examples of potentially lower risk factors[45] include: (a) customer risk factors:

[45] In assessing ML/TF risk of a business relationship, an SVF licensee should consider a range of factors in a holistic approach.

		(i) a government entity or a public body[46] in Hong Kong or in an equivalent jurisdiction; (ii) a corporation listed on a stock exchange and subject to disclosure requirements (e.g. either by stock exchange rules, or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership; or (iii) an FI as defined in the AMLO, or other FI incorporated or established in an equivalent jurisdiction and is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF. (b) product, service, transaction or delivery channel risk factors: (i) an SVF product with low maximum stored value or transaction limits; (ii) an SVF product without higher risk functions (e.g. cash access or cross-border usage); or (iii) an SVF product that provides appropriately defined and limited services or exposures to certain types of customers. (c) country risk factors: (i) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT Systems; or (ii) countries or jurisdictions identified by credible sources as having a lower level of corruption or other criminal activity.
	4.7.8	Examples of possible SDD measures include: (a) accepting other documents, data or information (e.g. proof of FI's license, listed status or authorization status etc.), other than examples provided in paragraphs 4.3.7 and 4.3.12, for a customer falling within any category specified in paragraph 4.7.7(a); (b) adopting simplified customer due diligence in relation to beneficial owners as specified in paragraphs 4.7.9 to 4.7.12 if a customer falls within paragraph 4.7.10; (c) reducing the frequency of updates of customer identification information; (d) reducing the degree of ongoing monitoring and scrutiny of transactions based on a reasonable monetary threshold; or (e) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the

[46] Public body, for the purpose of this Guideline, 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.

		business relationship, but inferring the purpose and intended nature from the type of transactions or business relationship established.
Simplified customer due diligence in relation to beneficial owners		
General		
	4.7.9	An SVF licensee may choose not to identify and take reasonable measures to verify the beneficial owner in relation to a customer that is listed in paragraph 4.7.10.
Specific customers		
	4.7.10	An SVF licensee may choose not to identify and take reasonable measures to verify the beneficial owner of a customer, if the customer is - (a) an FI as defined in the AMLO; (b) an institution that- (i) is incorporated or established in an equivalent jurisdiction (see paragraph 4.14); (ii) carries on a business similar to that carried on by an FI as defined in the AMLO; (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; (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 as defined in the AMLO; (ii) an institution incorporated or established in Hong Kong, or in an equivalent jurisdiction that- (A) has measures in place to ensure compliance with requirements relating to CDD and record-keeping similar to those imposed under this Guideline; and (B) 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.
	4.7.11	If a customer not falling within paragraph 4.7.10 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 the customer. However, the SVF licensee 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.
	4.7.12	Where a customer is a corporation listed on any stock exchange, an SVF licensee may choose not to identify and take reasonable measures to verify its beneficial owners. For this purpose, the SVF licensee should assess whether the customer is subject to any disclosure requirements (either by stock exchange rules, or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership of the customer.
4.8 Enhanced due diligence		
General		
	4.8.1	An SVF licensee should apply EDD measures in relation to a business relationship or transaction to mitigate and manage the high ML/TF risks in: (a) a situation that by its nature may present a high ML/TF risk; or (b) a situation specified by the HKMA in a notice in writing given to the SVF licensee.
	4.8.2	The EDD measures applied should be commensurate with the nature and level of ML/TF risks, based on the higher ML/TF risk factors identified by the SVF licensee. The extent of EDD measures should be proportionate, appropriate and discriminating, and be able to be justified to the HKMA.
	4.8.3	An SVF licensee should obtain approval from its senior management to establish or continue a business relationship that presents a high ML/TF risk.
	4.8.4	An SVF licensee should conduct enhanced ongoing monitoring of a business relationship that presents a high ML/TF risk, for example, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination. Reference should be made to Chapter 5.
	4.8.5	Examples of potentially higher risk factors[47] include: (a) customer risk factor: (i) business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic difference between the SVF licensee and the customer); (ii) nature and scope of business activities generating the funds/assets (e.g. merchants), having regard to high-risk

[47] In assessing ML/TF risk of a business relationship, an SVF licensee should consider a range of factors in a holistic approach.

		activities; (iii) legal persons or legal arrangements that involve a shell vehicle without a clear and legitimate commercial purpose; (iv) the ownership structure of the legal person or legal arrangement appears unusual or excessively complex given the nature of the legal person's or legal arrangement's business; or (v) the customer or the beneficial owner of the customer is a foreign politically exposed person; or (vi) companies that have nominee shareholders or shares in bearer form. (b) product, service, transaction or delivery channel risk factors: (i) anonymous transactions (which may involve cash); or (ii) frequent payments received from unknown or un-associated third parties. (c) country risk factors: (i) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as not having effective AML/CFT Systems; (ii) countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity; (iii) countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the United Nations; or (iv) countries, jurisdictions or geographical areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operation.
	4.8.6	Examples of possible EDD measures[48] include: (a) obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner; (b) obtaining additional information on the intended nature of the business relationship; (c) obtaining information on the source of funds or source of wealth of the customer (see paragraphs 4.8.22 and 4.8.23); (d) obtaining information on the reasons for intended or performed transactions; or (e) requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

[48] For the avoidance of doubt, there is no expectation for an SVF licensee to conduct all the examples of possible EDD measures for each business relationship that presents a high ML/TF risk. SVF licensees are reminded of the requirements set out in paragraph 4.8.2.

Politically exposed persons		
Foreign PEPs		
Definition		
	4.8.7	A (foreign) PEP 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 4.8.8).
	4.8.8	A close associate is: (a) an individual who has close business relations with a person falling under paragraph 4.8.7(a) above, including an individual who is a beneficial owner of a legal person or trust of which the person falling under paragraph 4.8.7(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 4.8.7(a) above.
Identification of foreign PEPs		
	4.8.9	An SVF licensee should establish and maintain effective procedures (e.g. by 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 foreign PEP.
EDD measures for foreign PEPs		
	4.8.10	When an SVF licensee knows that a customer or a beneficial owner of a customer is a foreign 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 foreign PEP, apply all the following EDD measures: (a) obtaining approval from its senior management for establishing or continuing such business relationship;

		(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) conducting enhanced ongoing monitoring of that business relationship (see Chapter 5).
Domestic PEPs & international organisation PEPs		
Definition		
	4.8.11	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 4.8.8).
	4.8.12	An international organisation PEP is defined as: (a) an individual who is or has been entrusted with a prominent function by an international organisation, and (i) includes members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions; (ii) but does not include a middle-ranking or more junior official of the international organisation; (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 4.8.8).
	4.8.13	International organisations referred to in paragraph 4.8.12 are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organization;

		regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Co-operation in Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization, and economic organisations such as the World Trade Organization or the Association of Southeast Asian Nations, etc.
Identification of and EDD measures for domestic PEPs & international organisation PEPs		
	4.8.14	An SVF licensee should take reasonable measures to determine whether a customer or a beneficial owner of a customer is a domestic PEP or an international organisation PEP.
	4.8.15	An SVF licensee should apply the EDD measures set out in paragraph 4.8.10 in any of the following situations[49]: (a) before establishing a high risk business relationship with a customer who is or whose beneficial owner is a domestic PEP or an international organisation PEP; (b) when continuing an existing business relationship with a customer who is or whose beneficial owner is a domestic PEP or an international organisation PEP where the relationship subsequently becomes high risk; or (c) when continuing an existing high risk business relationship where the SVF licensee subsequently knows that the customer or the beneficial owner of the customer is a domestic PEP or an international organisation PEP.
	4.8.16	If a domestic PEP or an international organisation PEP is no longer entrusted with a prominent (public) function, an SVF licensee may adopt an RBA[50] to determine whether to apply or continue to apply the EDD measures set out in paragraph 4.8.10 in a high risk business relationship with a customer who is or whose beneficial owner is that domestic PEP or international organisation PEP, taking into account various risk factors, such as: (a) the level of (informal) influence that the individual could still exercise; (b) the seniority of the position that the individual held as a PEP; or (c) whether the individual's previous and current function are linked in any way (e.g. formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

[49] For the avoidance of doubt, an SVF licensee should consider whether the application of EDD measures in paragraph 4.8.10 could mitigate the ML/TF risk arising from the high risk business relationship with a domestic PEP or an international organisation PEP. Where applicable, an SVF licensee should also apply EDD measures to mitigate such risk in accordance with the guidance provided in paragraphs 4.8.1 to 4.8.6.

[50] The handling of a domestic PEP or an international organisation PEP who is no longer entrusted with a prominent public function should be based on an assessment of risk and not merely on prescribed time limits.

		The SVF licensee should obtain approval from its senior management for such a decision.
Further guidance applied to all types of PEPs		
Scope of PEPs		
	4.8.17	An SVF licensee should implement appropriate risk management systems to identify PEPs. Under-classification of PEPs poses a higher ML risk to the SVF licensee whilst over-classification of PEPs leads to an unnecessary compliance burden to the SVF licensee and its customers.
	4.8.18	The definitions of PEPs set out above provide some non-exhaustive examples of the types of prominent (public) functions that an individual may be or may have been entrusted with by a foreign or domestic government, or by an international organisation. An SVF licensee should provide sufficient guidance and examples to its staff to enable them to identify all types of PEPs. In determining what constitutes a prominent (public) function, the SVF licensee should consider on a case-by-case basis taking into account various factors, for example: the powers and responsibilities associated with particular public function; the organisational framework of the relevant government or international organisation; and any other specific concerns connected to the jurisdiction where the public function is/has been entrusted.
	4.8.19	While an SVF licensee may refer to commercially available databases to identify PEPs, the use of these databases should never replace traditional CDD processes (e.g. understanding the occupation and employer of a customer). When using commercially available databases, an SVF licensee should be aware of their limitations, for example, the databases are not necessarily comprehensive or reliable as they generally draw solely from information that is publicly available; the definition of PEPs used by the database providers may or may not align with the definition of PEPs applied by the SVF licensee; and any technical incapability of such databases that may hinder the SVF licensee's effectiveness of PEP identification. Therefore, the SVF licensee should only use such databases as a support tool and ensure they are fit for purpose.
	4.8.20	Although the EDD requirements also apply to family members and close associates of the PEP, the risks associated with them may vary depending to some extent on the social-economic and cultural structure of the jurisdiction of the PEP.

EDD measures for PEPs		
	4.8.21	Since not all PEPs pose the same level of ML risks, an SVF licensee should adopt an RBA in determining the extent of EDD measures in paragraph 4.8.10 taking into account relevant factors, such as: (a) the prominent (public) functions that a PEP holds; (b) the geographical risk associated with the jurisdiction where a PEP holds prominent (public) functions; (c) the nature of the business relationship (e.g. the delivery/distribution channel used; or the product or service offered); or (d) the level of influence that a PEP may continue to exercise after stepping down from the prominent (public) function.
	4.8.22	Source of wealth refers to the origin of an individual's entire body of wealth (i.e. total assets). This information will usually give an indication as to the size of wealth the customer would be expected to have, and a picture of how the individual acquired such wealth. Although an SVF licensee may not have specific information about assets not stored with or processed by it, it may be possible to gather general information from the individual, commercial databases or other open sources.
	4.8.23	Source of funds refers to the origin of the particular funds or other assets which are the subject of the business relationship between an individual and the SVF licensee (e.g. the amounts being stored or wired as part of the business relationship). Source of funds information should not simply be limited to knowing from which the funds may have been transferred, but also the activity that generates the funds. The information obtained should be substantive and establish a provenance or reason for the funds having been acquired.
	4.8.24	It is for an SVF licensee to decide which measures it deems appropriate, 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. The SVF licensee should however note that not all declarations are publicly available and that a PEP customer may have legitimate reasons for not providing a copy. The SVF licensee 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.

4.9 Customer not physically present for identification purposes		
	4.9.1	SVF licensees may establish business relationships through various channels, both physically present(e.g. in the premises of SVF licensees) and non-physically present (e.g. via internet). However, an SVF licensee should take additional measures to mitigate the risk (e.g. impersonation risk) associated with customers not physically present for identification purposes. If a customer has not been physically present for identification purposes, the SVF licensee may, in addition to taking the measures as specified in paragraph 4.3.17, carry out the following additional measures to mitigate the risks posed, where appropriate: (a) further verifying the customer's identity on the basis of documents, data or information referred to in paragraph 4.3.1 but not previously used for the purposes of verification of the customer's identity under that paragraph; (b) taking supplementary measures to verify information relating to the customer that has been obtained by the SVF licensee; or (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.
	4.9.2	The extent of additional measures set out in paragraph 4.9.1 will depend on the nature and characteristics of the product or service requested and the assessed ML/TF risks presented by the customer.
	4.9.3	Paragraph 4.9.1(b) allows an SVF licensee to utilise different methods to mitigate the risk. These may include measures such as (i) use of an independent and appropriate person to certify identification documents; (ii) checking relevant data against reliable databases or registries; or (iii) using appropriate technology[51] etc. Whether a particular measure or a combination of measures is acceptable should be assessed on a case by case basis. The SVF licensee should ensure and be able to demonstrate to the HKMA that the supplementary measure(s) taken can adequately guard against impersonation risk.
	4.9.4	While the requirements to undertake additional measures generally apply to a customer that is a natural person, an SVF licensee should also mitigate any increased risk (e.g. applying additional due diligence measures set out in paragraph 4.9.1) if a customer that is not a natural person establishes a business relationship with an SVF licensee through a non-physically present channel. The increased

[51] SVF licensees may make reference to the technology solutions for remote on-boarding provided in paragraph 4.3.17.

		risk may arise from circumstances where the natural person acting on behalf of the customer to establish the business relationship is not physically present for identification purposes. In addition, where an SVF licensee is provided with copies of documents for identifying and verifying a legal person customer's identity, an SVF licensee should also mitigate any increased risk (e.g. applying additional due diligence measures set out in paragraph 4.9.1).
4.10 Reliance on CDD performed by intermediaries		
General		
	4.10.1	An SVF licensee may rely upon an intermediary to perform any part of the CDD measures[52] 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. In a third-party reliance scenario, the third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying SVF licensee, and would apply its own procedures to perform the CDD measures.
	4.10.2	For the avoidance of doubt, reliance on intermediaries does not apply to outsourcing or agency relationships, in which the outsourced entity or agent applies the CDD measures on behalf of the SVF licensee, in accordance with the SVF licensee's procedures, and subject to the SVF licensee's control of effective implementation of these procedures by the outsourced entity or agent.
	4.10.3	When relying on an intermediary, an SVF licensee should: (a) obtain written confirmation from the intermediary that the intermediary agrees to act as the SVF licensee's intermediary and perform which part of the CDD measures specified in paragraph 4.1.3; and (b) be satisfied that the intermediary will on request provide a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out the CDD measures without delay.
	4.10.4	An SVF licensee that carries out a CDD measure by means of an intermediary should 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

[52] For the avoidance of doubt, an SVF licensee cannot rely on an intermediary to continuously monitor its business relationship with a customer for the purpose of complying with the requirements set out in Chapter 5 of this Guideline.

		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.
	4.10.5	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 five 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. The SVF licensee should ensure that the intermediary will, if requested by the SVF licensee within the period specified in the record-keeping requirements of this Guideline, 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. The SVF licensee 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.
	4.10.6	An SVF licensee 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.
	4.10.7	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.
<u>Domestic intermediaries</u>		
	4.10.8	An SVF licensee may rely upon any one of the following domestic intermediaries, to perform any part of the CDD measures specified in paragraph 4.1.3: (a) an FI that is an AI, a licensed corporation, an authorized insurer, an appointed insurance agent or an authorized insurance broker (intermediary FI); (b) an accounting professional meaning: (i) a certified public accountant or a certified public accountant (practising), as defined by section 2(1) of the

		Professional Accountants Ordinance; (ii) a corporate practice as defined by section 2(1) of the Professional Accountants Ordinance; or (iii) a firm of certified public accountants (practising) registered under Part IV of the Professional Accountants Ordinance; (c) an estate agent meaning: (i) a licensed estate agent as defined by section 2(1) of the Estate Agents Ordinance; or (ii) a licensed salesperson as defined by section 2(1) of the Estate Agents Ordinance; (d) a legal professional meaning: (i) a solicitor as defined by section 2(1) of the Legal Practitioners Ordinance; or (ii) a foreign lawyer as defined by section 2(1) of the Legal Practitioners Ordinance; or (e) a trust or company service provider (TCSP) licensee meaning: (i) a person who holds a licence granted under section 53G or renewed under section 53K of the AMLO; or (ii) a deemed licensee as defined by section 53ZQ(5) of the AMLO, provided that in the case of an accounting professional, an estate agent, a legal professional or a TCSP licensee, the SVF licensee is satisfied that the domestic intermediary has adequate procedures in place to prevent ML/TF and is required to comply with the relevant requirements set out in Schedule 2 to the AMLO with respect to the customer[53].
	4.10.9	An SVF licensee should take appropriate measures to ascertain if the domestic intermediary satisfies the criteria set out in paragraph 4.10.8, which may include: (a) where the domestic intermediary is an accounting professional, an estate agent, a legal professional or a TCSP licensee, ascertaining whether the domestic intermediary is required to comply with the relevant requirements set out in Schedule 2 to the AMLO with respect to the customer; (b) making enquiries concerning the domestic intermediary's stature or the extent to which any group AML/CFT standards are applied and audited; or (c) reviewing the AML/CFT policies and procedures of the domestic intermediary.

[53] CDD requirements set out in Schedule 2 to the AMLO apply to an accounting professional, an estate agent, a legal professional or a TCSP licensee with respect to a customer only when it, by way of business, prepares for or carries out for the customer a transaction specified under section 5A of the AMLO.

Overseas intermediaries		
	4.10.10	An SVF licensee may rely upon an overseas intermediary[54] carrying on business or practising in an equivalent jurisdiction[55] to perform any part of the CDD measures specified in paragraph 4.1.3, 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 intermediary FI; (ii) a lawyer or a notary public; (iii) an auditor, a professional accountant, or a tax advisor; (iv) a TCSP; (v) a trust company carrying on trust business; and (vi) a person who carries on a business similar to that carried on by an estate agent; (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 similar to those under Schedule 2 to the AMLO; 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 or the regulatory bodies (as may be applicable).
	4.10.11	An SVF licensee should take appropriate measures to ascertain if the overseas intermediary satisfies the criteria set out in paragraph 4.10.10. Appropriate measures that should be taken to ascertain if the criterion set out in paragraph 4.10.10(c) is satisfied may include: (a) making enquiries concerning the overseas intermediary's stature or the extent to which any group's AML/CFT standards are applied and audited; or (b) reviewing the AML/CFT policies and procedures of the overseas intermediary.
Related foreign financial institutions as intermediaries		
	4.10.12	An SVF licensee may also rely upon a related foreign financial institution (related foreign FI) to perform any part of the CDD measures specified in paragraph 4.1.3, if the related foreign FI: (a) carries on, in a place outside Hong Kong, a business similar to that carried on by an intermediary FI; and falls within any of the following descriptions:

[54] The overseas intermediary and the SVF licensee could be unrelated or within the same group of companies to which the SVF licensee belongs.

[55] Guidance on jurisdictional equivalence is provided in paragraph 4.14.

		(i) it is within the same group of companies as the SVF licensee; (ii) if the SVF licensee is incorporated in Hong Kong, it is a branch of the SVF licensee; (iii) if the SVF licensee is incorporated outside Hong Kong: (A) it is the head office of the SVF licensee; or (B) it is a branch of the head office of the SVF licensee; (b) is required under group policy: (i) to have measures in place to ensure compliance with requirements similar to the requirements imposed under Schedule 2 to the AMLO; and (ii) to implement programmes against ML/TF; and (c) is supervised for compliance with the requirements mentioned in paragraph (b) at a group level: (i) by an RA; or (ii) by an authority in an equivalent jurisdiction that performs, in relation to the holding company or the head office of the SVF licensee, functions similar to those of an RA under the AMLO.
	4.10.13	The group policy set out in paragraph 4.10.12(b) refers to a policy of the group of companies to which the SVF licensee belongs and the policy applies to the SVF licensee and the related foreign FI. The group policy should include CDD and record-keeping requirements similar to the requirements imposed under Schedule 2 to the AMLO and the group-wide AML/CFT System[56] (e.g. compliance and audit functions). The group policy should also be able to mitigate adequately any higher country risk in relation to the jurisdiction where the related foreign FI is located. The SVF licensee should be satisfied that the related foreign FI is subject to regular and independent reviews over its ongoing compliance with the group policy conducted by any group-level compliance, audit or other similar AML/CFT functions.
	4.10.14	The SVF licensee should be able to demonstrate that the implementation of the group policy is supervised at a group level by either an RA or an authority in an equivalent jurisdiction that performs functions similar to those of an RA under the AMLO, which practises group-wide supervision which extends to the related foreign FI.
4.11 Failure to satisfactorily complete CDD		
	4.11.1	Where the SVF licensee is unable to comply with relevant CDD requirements set out in this Chapter and the ongoing due diligence requirements set out in Chapter 5, it should not establish a business relationship or should terminate business relationship as soon as

[56] Reference should be made to Chapter 3.

		reasonably practicable (where applicable), and where there is relevant knowledge or suspicion, should make an STR to the JFIU.
4.12 Prohibition on anonymous accounts		
	4.12.1	Other than the low risk SVF products which are permitted under the tiered approach as specified under paragraphs 1.4.6 to 1.4.21, an SVF licensee should not maintain anonymous accounts or accounts in fictitious names for any new or existing customer. Where numbered accounts exist, the SVF licensee should maintain them in such a way that full compliance with this Guideline can be achieved. The SVF licensee should properly identify and verify the identity of the customer in accordance with this Guideline. In all cases, whether the relationship involves numbered accounts or not, the customer identification and verification records should be available to the HKMA, other competent authorities, the CO, auditors, and other staff with appropriate authority.
4.13 Jurisdictions subject to a call by the FATF		
	4.13.1	An SVF licensee should apply EDD measures, proportionate to the risks, to business relationships and transactions with natural and legal persons, and FIs, from jurisdictions for which this is called for by the FATF in accordance with the guidance provided in paragraph 4.8.
	4.13.2	Where mandatory EDD or countermeasures[57] are called for by the FATF, or in other circumstances independent of any call by the FATF but also considered to be higher risk, the HKMA may also, through a notice in writing: (a) impose a general obligation on SVF licensees to comply with the requirements set out in paragraph 4.8 of this Guideline or; (b) require SVF licensees to undertake specific countermeasures described in the notice. The type of measures in paragraph (a) and (b) would be proportionate to the nature of the risks and/or deficiencies.
4.14 Jurisdictional equivalence		
<u>General</u>		
	4.14.1	Jurisdictional equivalence and the determination of equivalence may be a consideration in the application of CDD measures under this Guideline. Equivalent jurisdiction means: (a) a jurisdiction that is a member of the FATF, other than Hong Kong; or (b) a jurisdiction that imposes requirements similar to those

[57] For jurisdictions with serious deficiencies in applying the FATF Recommendations and where inadequate progress has been made to improve their positions, the FATF may recommend the application of countermeasures.

		imposed under Schedule 2 to the AMLO.
Determination of jurisdictional equivalence		
	4.14.2	An SVF licensee may therefore be required to evaluate and determine for itself which jurisdictions other than FATF members apply requirements similar to those imposed under Schedule 2 to the AMLO for jurisdictional equivalence purposes. The SVF licensee should document its assessment of the jurisdiction, and may include consideration of the following factors: (a) whether the jurisdiction concerned is a member of FATF-style regional bodies and recent mutual evaluation report published by the FATF-style regional bodies; (b) whether the jurisdiction concerned is identified by the FATF as having strategic AML/CFT deficiencies and the recent progress of improving its AML/CFT regime; (c) any advisory circular issued by the HKMA from time to time alerting SVF licensees to jurisdictions with poor AML/CFT controls; (d) any other AML/CFT-related publications published by specialised national, international, non-governmental or commercial organisations.
	4.14.3	As the AML/CFT regime of a jurisdiction will change over time, an SVF licensee should review the jurisdictional equivalence assessment on a regular basis and/or upon trigger events.

Chapter 5 – ONGOING MONITORING		
General		
	5.1	Ongoing monitoring is an essential component of effective AML/CFT Systems. An SVF licensee should continuously monitor its business relationship with a customer in two aspects: (a) **ongoing CDD**: reviewing from time to time documents, data and information relating to the customer that have been obtained by the SVF licensee for the purpose of complying with the requirements imposed under this Guideline to ensure that they are up-to-date and relevant ; and (b) **transaction monitoring**: (i) conducting appropriate scrutiny of transactions carried out for the customer to ensure that they are consistent with the SVF licensee's knowledge of the customer, the customer's business, risk profile and source of funds; and (ii) identifying transactions that (i) are complex, unusually large in amount or of an unusual pattern; and (ii) have no apparent economic or lawful purpose, and examining the background and purposes of those transactions and setting out its finding in writing.
Ongoing CDD		
	5.2	To ensure documents, data and information of a customer obtained are up-to-date and relevant[58], an SVF licensee should undertake reviews of existing CDD records of customers on a regular basis and/or upon trigger events[59]. Clear policies and procedures should be developed, especially on the frequency of periodic review or what constitutes a trigger event.
	5.3	All customers that present high ML/TF risks should be subject to a minimum of an annual review, or more frequent reviews if deemed necessary by the SVF licensee, to ensure the CDD information retained remains up-to-date and relevant.
Transaction monitoring		
Transaction monitoring systems and processes		
	5.4	An SVF licensee should establish and maintain adequate systems and processes to monitor transactions. The design, degree of automation and sophistication of transaction monitoring systems and processes should be developed appropriately having regard to the following factors:

[58] Keeping the CDD information up-to-date and relevant does not mean that an SVF licensee has to re-verify identities that have been verified (unless doubts arise as to the veracity or adequacy of the evidence previously obtained for the purposes of customer identification).

[59] While it is not necessary to regularly review the existing CDD records of a dormant customer, an SVF licensee should conduct a review upon reactivation of the relationship. The SVF licensee should define clearly what constitutes a dormant customer in its policies and procedures.

		(a) the size and complexity of its business; (b) 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 provided (which includes the means of delivery or communication).
	5.5	An SVF licensee should ensure that the transaction monitoring systems and processes can provide all relevant staff who are tasked with conducting transaction monitoring and investigation with timely and sufficient information required to identify, analyse and effectively monitor customers' transactions.
	5.6	An SVF licensee should ensure that the transaction monitoring systems and processes can support the ongoing monitoring of a business relationship in a holistic approach, which may include monitoring activities of a customer's multiple accounts within or across lines of businesses, and related customers' accounts within or across lines of businesses. This means preferably the SVF licensee adopts a relationship-based approach rather than on a transaction-by-transaction basis.
	5.7	In designing transaction monitoring systems and processes, including setting of parameters and thresholds, an SVF licensee should take into account the transaction characteristics, which may include: (a) the nature and type of transactions (e.g. abnormal size or frequency); (b) the nature of a series of transactions (e.g. structuring a single transaction into a number of cash top-up); (c) the counterparties of transactions; (d) the geographical origin/destination of a payment or receipt; and (e) the customer's normal account activity or turnover.
	5.8	An SVF licensee should regularly review the adequacy and effectiveness of its transaction monitoring systems and processes, including parameters and thresholds adopted. The parameters and thresholds should be properly documented and independently validated to ensure that they are appropriate to its operations and context.

Risk-based approach to transaction monitoring and review of transactions		
	5.9	An SVF licensee should conduct transaction monitoring in relation to all business relationships following the RBA. The extent of monitoring (e.g. frequency and intensity of monitoring) should be commensurate with the ML/TF risk profile of a customer. Where the ML/TF risks are high[60], the SVF licensee should conduct enhanced transaction monitoring. In low risk situations, the SVF licensee may reduce the extent of monitoring.
	5.10	An SVF licensee should take appropriate steps (e.g. examining the background and purposes of the transactions; making appropriate enquiries to or obtaining additional CDD information from a customer) to identify if there are any grounds for suspicion, when: (a) the customer's transactions are not consistent with the SVF licensee's knowledge of the customer, the customer's business, risk profile and source of funds; or (b) the SVF licensee identifies transactions that (i) are complex, unusually large in amount or of an unusual pattern, and (ii) have no apparent economic or lawful purpose[61].
	5.11	Where an SVF licensee conducts enquiries and obtains what it considers to be a satisfactory explanation of the transaction or activity, it may conclude that there are no grounds for suspicion, and therefore take no further action. Even if no suspicion is identified, the SVF licensee should consider updating the customer risk profile based on any relevant information obtained.
	5.12	However, where the SVF licensee cannot obtain a satisfactory explanation of the transaction or activity, it may conclude that there are grounds for suspicion. In any event where there is any suspicion identified during transaction monitoring, an STR should be made to the JFIU.
	5.13	An SVF licensee should be aware that making enquiries to customers, when conducted properly and in good faith, will not constitute tipping off. However, if the SVF licensee reasonably believes that performing the CDD process will tip off the customer, it may stop pursuing the process. The SVF licensee should document the basis for its assessment and file an STR to the JFIU.

[60] Examples of high ML/TF risk situations that require enhancing transaction monitoring include: (a) a customer or a beneficial owner of a customer being a foreign PEP; and (b) a business relationship presenting a high risk of ML/TF.

[61] An SVF licensee should examine the background and purposes of the transactions and set out its findings in writing.

	5.14	The findings and outcomes of steps taken by the SVF licensee in paragraph 5.10, as well as the rationale of any decision made after taking these steps, should be properly documented in writing and be available to the HKMA, other competent authorities and auditors.

Chapter 6 – TERRORIST FINANCING, FINANCIAL SANCTIONS AND PROLIFERATION FINANCING		
Terrorist financing		
	6.1	TF is the financing of terrorist acts, and of terrorists and terrorist organisations. It generally refers to the carrying out of transactions involving property owned by terrorists or terrorist organisations, or that has been, or is intended to be, used to assist the commission of terrorist acts. Different from ML, the focus of which is on the handling of criminal proceeds (i.e. the source of property is what matters), the focus of TF is on the destination or use of property, which may have derived from legitimate sources.
UNSCR 1267 (1999), 1373 (2001), 1988 (2011), 1989 (2011), 2253 (2015), and 2368(2017)	6.2	The UNSC has passed UNSCR 1373 (2001), which calls on all member states to act to prevent and suppress the financing of terrorist acts. The UN has also published the names of individuals and organisations in relation to involvement with Al-Qa'ida, ISIL (Da'esh) and the Taliban under relevant UNSCRs (e.g. UNSCR 1267 (1999), 1988 (2011), 1989 (2011), 2253 (2015), 2368 (2017) and their successor resolutions). All UN member states are required to freeze any funds, or other financial assets, or economic resources of any person(s) named in these lists and to report any suspected name matches to the relevant authorities.
	6.3	UNATMO is an ordinance to further implement a decision under UNSCR 1373 (2001) relating to measures for prevention of terrorist acts and a decision under UNSCR 2178 (2014) relating to the prevention of travel for the purpose of terrorist acts or terrorist training; as well as to implement certain terrorism-related multilateral conventions and certain FATF Recommendations.
s.4 & 5, UNATMO	6.4	Where a person or property is designated by a Committee of the UNSC established pursuant to the relevant UNSCRs as stated in paragraph 6.2 as a terrorist/terrorist associate or terrorist property[62] respectively, the Chief Executive may publish a notice in the Gazette specifying the name of the person or the property under section 4 of the UNATMO. Besides, section 5 of the UNATMO provides that the Chief Executive may make an application to the Court of First Instance for an order to specify a person or property as a terrorist/terrorist associate or terrorist property respectively, and if the order is made, it will also be published in the Gazette.
s.6, 7, 8, 8A & 11L UNATMO	6.5	A number of provisions in the UNATMO are of particular relevance to SVF licensees, and are listed below: (a) section 6 empowers the Secretary for Security (S for S) to

[62] According to section 2 of the UNATMO, terrorist property means the property of a terrorist or terrorist associate, or any other property that is intended to be used or was used to finance or assist the commission of terrorist acts.

		freeze suspected terrorist property; (b) section 7 prohibits the provision or collection of property for use to commit terrorist acts; (c) section 8 prohibits any person from making available or collecting or soliciting property or financial (or related) services for terrorists or terrorist associates; (d) section 8A prohibits any person from dealing with any property knowing that, or being reckless as to whether, the property is specified terrorist property or property of a specified terrorist or terrorist associate; and (e) section 11L prohibits any person from providing or collecting any property to finance the travel of a person between states with the intention or knowing that the travel will be for a specified purpose, i.e. the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs); or the provision or receiving of training that is in connection with the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs as a result of the training).
s.6(1), 8 & 8A(1), UNATMO	6.6	The S for S can licence exceptions to the prohibitions to enable frozen property to be unfrozen and to allow payments to be made to or for the benefit of a designated party under the UNATMO (e.g. reasonable living/legal expenses and payments liable to be made under the Employment Ordinance). An SVF licensee seeking such a licence should write to the Security Bureau.
Financial sanctions and proliferation financing		
	6.7	The UNSO empowers the Chief Executive to make regulations to implement sanctions decided by the UNSC, including targeted financial sanctions[63] against individuals and entities designated by the UNSC or its Committees. Designated persons and entities are specified by notice published in the Gazette or on the website of the Commerce and Economic Development Bureau. It is an offence to make available, directly or indirectly, any funds, or other financial assets, or economic resources, to, or for the benefit of, a designated person or entity, as well as those acting on their behalf, at their direction, or owned or controlled by them; or to deal with any funds, other financial assets or economic resources belonging to, or owned or controlled by, such persons and entities, except under the authority of a licence granted by the Chief Executive.
Applicable UNSO Regulation	6.8	The Chief Executive may grant licence for making available or dealing with any funds, or other financial assets, and economic resources to or belonging to a designated person or entity under specified circumstances in accordance with the provisions of the

[63] Targeted financial sanctions refer to both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.

		relevant regulation made under the UNSO. An SVF licensee seeking such a licence should write to the Commerce and Economic Development Bureau.
	6.9	To combat PF, the UNSC adopts a two-tiered approach through resolutions made under Chapter VII of the UN Charter imposing mandatory obligations on UN member states: (a) global approach under UNSCR 1540 (2004) and its successor resolutions; and (b) country-specific approach under UNSCR 1718 (2006) against DPRK and UNSCR 2231 (2015) against Iran and their successor resolutions.
s.4, WMD(CPS)O	6.10	The counter proliferation financing regime in Hong Kong is implemented through legislation, including the regulations made under the UNSO which are specific to DPRK and Iran, and the WMD(CPS)O. Section 4 of WMD(CPS)O prohibits a person from providing any services where he believes or suspects, on reasonable grounds, that those services may be connected to PF. The provision of services is widely defined and includes the lending of money or other provision of financial assistance.
Sanctions imposed by other jurisdictions		
	6.11	While SVF licensees do not normally have any obligation under Hong Kong laws to have regard to unilateral sanctions imposed 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 sanctions regimes in those jurisdictions. Where these sanctions regimes may affect its operations, the SVF licensee should consider what implications exist for its procedures and take appropriate measures, such as including relevant overseas designations in its database for screening purpose, where applicable.
Database maintenance, screening and enhanced checking		
	6.12	An SVF licensee should establish and maintain effective policies, procedures and controls to ensure compliance with the relevant regulations and legislation on TF, financial sanctions and PF. The legal and regulatory obligations of SVF licensees and those of their staff should be well understood and adequate guidance and training should be provided to the latter.
	6.13	It is particularly vital that an SVF licensee should be able to identify terrorist suspects and possible designated parties, and detect prohibited transactions. To this end, an SVF licensee should ensure that it maintains a database of names and particulars of terrorists and designated parties, which consolidates the various lists that have been made known to the SVF licensee. Alternatively, an SVF licensee may subscribe to such a database maintained by a third party service provider and take appropriate measures (e.g. conduct

		sample testing periodically) to ensure the completeness and accuracy of the database.
	6.14	Whether or not a UNSCR or sanctions list has been implemented through Hong Kong legislation, there are offences under existing legislation relating to ML, TF and PF that are relevant. Inclusion of a country, individual, entity or activity in the UNSCR or sanctions list may constitute grounds for knowledge or suspicion for the purposes of relevant ML, TF and PF laws, thereby triggering statutory (including reporting) obligations as well as offence provisions. The HKMA draws to the attention to SVF licensees from time to time whenever there are any updates to UNSCRs or sanctions lists relating to terrorism, TF and PF promulgated by the UNSC. SVF licensees should ensure that countries, individuals and entities included in UNSCRs and sanctions lists are included in the database as soon as practicable after they are promulgated by the UNSC and regardless of whether the relevant sanctions have been implemented by legislation in Hong Kong.
	6.15	An SVF licensee should include in its database: (i) the lists published in the Gazette or on the website of the Commerce and Economic Development Bureau; (ii) the lists that the HKMA draws to the attention of SVF licensees from time to time; and (iii) any relevant designations by overseas authorities which may affect its operations. The database should also be subject to timely update whenever there are changes, and should be made easily accessible by relevant staff.
	6.16	To avoid establishing business relationship or conducting transactions with any terrorist suspects and possible designated parties, an SVF licensee should implement an effective screening mechanism[64], which should include: (a) screening its customers and any beneficial owners of customers against current database at the establishment of the relationship; (b) screening its customers and any beneficial owners of the customers against all new and any updated designations to the database as soon as practicable; and (c) screening all relevant parties in a cross-border wire transfer against current database before executing the transfer.
	6.17	The screening requirements set out in paragraph 6.16(a) and (b) should extend to connected parties as defined in paragraph 4.3.20 and PPTAs of a customer using an RBA.

[64] Screening should be carried out irrespective of the risk profile attributed to the customer.

	6.18	When possible name matches are identified during screening, an SVF licensee should conduct enhanced checks to determine whether the possible matches are genuine hits. In case of any suspicions of TF, PF or sanctions violations, the SVF licensee should make a report to the JFIU. Records of enhanced checking results, together with all screening records, should be documented, or recorded electronically.
	6.19	An SVF licensee may rely on its overseas office to maintain the database or to undertake the screening process. However, the SVF licensee is reminded that the ultimate responsibility for ensuring compliance with the relevant regulations and legislation on TF, financial sanctions and PF remains with the SVF licensee.

Chapter 7 – SUSPICIOUS TRANSACTION REPORTS AND LAW ENFORCEMENT REQUESTS		
Suspicious transaction reporting regime in Hong Kong		
General issues		
s.25A(1)&(7), DTROP & OSCO, s.12(1)& 14(5), UNATMO	7.1	It is a statutory obligation under sections 25A(1) of the DTROP and the OSCO, as well as section 12(1) of the UNATMO, that where a person knows or suspects that any property: (a) in whole or in part directly or indirectly represents any person's proceeds of, (b) was used in connection with, or (c) is intended to be used in connection with drug trafficking or an indictable offence; or that any property is terrorist property, the person shall as soon as it is reasonable for him to do so, file an STR with the JFIU. The STR should be made together with any matter on which the knowledge or suspicion is based. Under the DTROP, the OSCO and the UNATMO, failure to report knowledge or suspicion carries a maximum penalty of imprisonment for three months and a fine of HK$50,000.
Knowledge vs. suspicion		
	7.2	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.
	7.3	Suspicion is more subjective. Suspicion is personal and falls short of proof based on firm evidence. As far as an SVF licensee is concerned, when a transaction or a series of transactions of a customer is not consistent with the SVF licensee's knowledge of the customer, or is unusual (e.g. in a pattern that has no apparent economic or lawful purpose), the SVF licensee should take appropriate steps to further examine the transactions and identify if there is any suspicion (see paragraphs 5.10 to 5.14).
	7.4	For a person to have knowledge or suspicion, he does not need to know the nature of the criminal activity underlying the ML, or that the funds themselves definitely arose from the criminal offence. Similarly, the same principle applies to TF.
	7.5	Once knowledge or suspicion has been formed, (a) an SVF licensee should file an STR even where no transaction has been conducted by or through the SVF licensee[65]; and

[65] 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".

		(b) the STR should be made as soon as reasonably practical after the suspicion was first identified.
Tipping off		
s.25A(5), DTROP & OSCO, s.12(5), UNATMO	7.6	It is an offence ("tipping off") to reveal to any person any information which might prejudice an investigation; if a customer is told that a report has been made, this would prejudice the investigation and an offence would be committed. The tipping off provision includes circumstances where a suspicion has been raised internally within an SVF licensee, but has not yet been reported to the JFIU.
AML/CFT Systems in relation to suspicious transaction reporting		
	7.7	An SVF licensee should implement appropriate AML/CFT Systems in order to fulfil its statutory reporting obligations, and properly manage and mitigate the risks associated with any customer or transaction involved in an STR. The AML/CFT Systems should include: (a) appointment of an MLRO (see Chapter 3); (b) implementing clear policies and procedures over internal reporting, reporting to the JFIU, post-reporting risk mitigation and prevention of tipping off; and (c) keeping proper records of internal reports and STRs.
	7.8	An SVF licensee should have measures in place to check, on an ongoing basis, that its AML/CFT Systems in relation to suspicious transaction reporting comply with relevant legal and regulatory requirements and operate effectively. The type and extent of the measures to be taken should be appropriate having regard to the risk of ML/TF as well as the nature and the size of its business.
Money laundering reporting officer		
	7.9	An SVF licensee should appoint an MLRO as a central reference point for reporting suspicious transactions and also as the main point of contact with the JFIU and law enforcement agencies. The MLRO should play an active role in the identification and reporting of suspicious transactions. Principal functions of the MLRO should include having oversight of: (a) review of all internal disclosures and exception reports and, in light of all available relevant information, determination of whether or not it is necessary to make a report to the JFIU; (b) maintenance of all records related to such internal reviews; and (c) provision of guidance on how to avoid tipping off.

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.

Identifying suspicious transactions and internal reporting		
	7.10	An SVF licensee should provide sufficient guidance to its staff to enable them to form suspicion or to recognise the signs when ML/TF is taking place. The guidance should take into account the nature of the transactions and customer instructions that staff is likely to encounter, the type of product or service and the means of delivery.
	7.11	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 CDD for a verified customer (e.g. a few transactions within a short period of time with an amount just

		below the limit for conducting CDD for a verified customer, purchase of multiple non-reloadable prepaid cards just below the limit for conducting CDD for a verified customer 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 [66] and SVF licensees should be familiar with the characteristics in that guidance.
	7.12	An SVF licensee may adopt, where applicable, the "SAFE" approach promoted by the JFIU, which includes: (a) screening the account for suspicious indicators; (b) asking the customers appropriate questions; (c) finding out the customer's records; and (d) evaluating all the above information. Details of the "SAFE" approach are available at JFIU's website (www.jfiu.gov.hk).
	7.13	An SVF licensee should establish and maintain clear policies and 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 report; and (b) all internal reports should reach the MLRO without undue delay.
	7.14	While an SVF licensee 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.
s.25A(4), DTROP & OSCO, s.12(4), UNATMO	7.15	Once a staff of an SVF licensee has reported suspicion to the MLRO in accordance with the policies and procedures established by the SVF licensee for the making of such reports, the statutory obligation of the staff has been fully satisfied.

[66] 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.

	7.16	The internal report should include sufficient details of the customer concerned and the information giving rise to the suspicion.
	7.17	The MLRO should acknowledge receipt of an internal report and provide a reminder of the obligation regarding tipping off to the reporting staff upon internal reporting.
	7.18	When evaluating an internal report, an MLRO should take reasonable steps to consider all relevant information, including CDD and ongoing monitoring information available within or to the SVF licensee concerning the customer to which the report relates. This may include: (a) making a review of other transaction patterns and volumes through connected accounts, preferably adopting a relationship-based approach rather than on a transaction-by-transaction basis; (b) making reference to any previous patterns of instructions, the length of the business relationship, and CDD and ongoing monitoring information and documentation; and (c) appropriate questioning of the customer per the systematic approach to identify suspicious transactions recommended by the JFIU[67].
	7.19	The need to search for information concerning connected accounts or relationships should strike an appropriate balance between the statutory requirement to make a timely STR to the JFIU and any delays that might arise in searching for more relevant information concerning connected accounts or relationships. The review process should be documented, together with any conclusions drawn.
<u>Reporting to the JFIU</u>		
	7.20	If after completing the review of the internal report, an 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. Dependent on when knowledge or suspicion arises, an STR 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.
	7.21	Providing an MLRO acts 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 the MLRO concludes that there is no suspicion after taking into account all available information. It is

[67] For details, please see JFIU's website (www.jfiu.gov.hk).

		however vital for the MLRO to keep proper records of their deliberations and actions taken to demonstrate he has acted in reasonable manner.
	7.22	In the event that an urgent reporting is required (e.g. 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 etc.), particularly when the account is part of an ongoing investigation by law enforcement agency, an SVF licensee should indicate this in the STR. Where exceptional circumstances exist in relation to an urgent reporting, an initial notification by telephone to the JFIU should be considered.
	7.23	An SVF licensee is recommended to indicate any intention to terminate a business relationship in its initial STR to the JFIU, thereby allowing the JFIU to comment, at an early stage, on such a course of action.
	7.24	An SVF licensee should ensure STRs filed to the JFIU are of high quality taking into account feedback and guidance provided by the JFIU in its quarterly report[68] and the HKMA from time to time.
Post STR reporting		
s.25A(2)(a), DTROP & OSCO, s.12(2B)(a), UNATMO	7.25	The JFIU will acknowledge receipt of an STR made by an SVF licensee 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 SVF licensee to operate the account under the provisions of section 25A(2)(a) of both the DTROP and the OSCO, and section 12(2B)(a) of the UNATMO. If a no-consent letter is issued, the SVF licensee should act according to the contents of the letter and seek legal advice where necessary.
s.25A(2), DTROP & OSCO, s.12(2), UNATMO	7.26	Filing an STR to the JFIU provides an SVF licensee 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.

[68] 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 at a secure area of the JFIU's website at www.jfiu.gov.hk. SVF licensees can apply for a login name and password by completing the registration form available on the JFIU's website or by contacting the JFIU directly.

	7.27	However, the statutory defence stated in paragraph 7.26 does not absolve an SVF licensee from the legal, reputational or regulatory risks associated with the account's continued operation. An SVF licensee should also be aware that 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.
	7.28	An SVF licensee should conduct an appropriate review of a business relationship upon the filing of an STR to the JFIU, irrespective of any subsequent feedback provided by the JFIU, and apply appropriate risk mitigating measures. 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. If necessary, the issue should be escalated to the SVF licensee's senior management to determine how to handle the relationship concerned 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.
	7.29	An SVF licensee should be aware that 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, should continue to be reported to the MLRO who should make further reports to the JFIU if appropriate.
<u>Record-keeping</u>		
	7.30	An SVF licensee should establish and maintain a record of all ML/TF reports made to the MLRO. The record should include details of the date the report was made, the staff members subsequently handling the report, the results of the assessment, whether the internal report resulted in an STR to the JFIU, and information to allow the papers relevant to the report to be located.
	7.31	An SVF licensee should establish and maintain a record of all STRs made to the JFIU. The record should include details of the date of the STR, the person who made the STR, and information to allow the papers relevant to the STR to be located. This register may be combined with the register of internal reports, if considered appropriate.
Requests from law enforcement agencies		
	7.32	An SVF licensee may receive various requests from law enforcement agencies, e.g. search warrants, production orders, restraint orders or confiscation orders, pursuant to relevant legislations in Hong Kong. These requests are crucial to aid law

		enforcement agencies to carry out investigations as well as restrain and confiscate illicit proceeds. Therefore, an SVF licensee should establish clear policies and procedures to handle these requests in an effective and timely manner, including allocation of sufficient resources and appointing a staff as the main point of contact with law enforcement agencies.
	7.33	An SVF licensee should respond to any search warrant and production order within the required time limit by providing all information or materials that fall within the scope of the request. Where an SVF licensee encounters difficulty in complying with the timeframes stipulated, the SVF licensee should at the earliest opportunity contact the officer-in-charge of the investigation for further guidance.
s.10 & 11, DTROP, s.15 & 16, OSCO, s.6, UNATMO	7.34	During a law enforcement investigation, an SVF licensee may be served with a restraint order which prohibits the dealing with particular funds or property pending the outcome of an investigation. The SVF licensee should ensure that it is able to freeze the relevant property that is the subject of the order. It should be noted that the restraint order may not apply to all funds or property involved within a particular business relationship and the SVF licensee should consider what, if any, funds or property may be utilised subject to the laws of Hong Kong.
s.3, DTROP, s.8, OSCO, s.13, UNATMO	7.35	Upon the conviction of a defendant, a court may order the confiscation of his criminal proceeds and an SVF licensee may be served with a confiscation order in the event it holds funds or other property belonging to that defendant that are deemed by the court to represent his benefit from the crime. A court may also order the forfeiture of property where it is satisfied that the property is terrorist property.
	7.36	When an SVF licensee receives a request from a law enforcement agency, e.g. search warrant or production order, in relation to a particular customer or business relationship, the SVF licensee should assess the risks involved and the need to conduct an appropriate review on the customer or the business relationship to determine whether there is any suspicion and should be aware that the customer subject to the request can be a victim of crime.

Chapter 8 – RECORD-KEEPING		
General		
	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	An SVF licensee should maintain CDD information, transaction records 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 nature, size and complexity of its businesses. The SVF licensee should ensure that: (a) the audit trail for funds moving through the SVF licensee that relate to any customer and, where appropriate, the beneficial owner of the customer, account or transaction is clear and complete; (b) all CDD information and transaction records are available swiftly to the HKMA, other authorities and auditors upon appropriate authority; and (c) it can demonstrate compliance with any relevant requirements specified in other sections of this Guideline and other guidelines issued by the HKMA.
Retention of records relating to CDD and transactions		
	8.3	An SVF licensee 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, where applicable, 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) other documents and records obtained throughout the CDD and ongoing monitoring process, including tiered approach, SDD and EDD; (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 or risk

		assessment form) and business correspondence[69] 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); and (e) the results of any analysis undertaken (e.g. inquiries to establish the background and purposes of transactions that are complex, unusually large in amount or of unusual pattern, and have no apparent economic or lawful purpose).
	8.4	All documents and records mentioned in paragraph 8.3 should be kept throughout the continuance of the business relationship with the customer and for a period of at least five years after the end of the business relationship. Similarly, for a transaction equal to or exceeding the CDD thresholds (e.g. HK$8,000 for wire transfers, HK$25,000 for purchase of multiple non-reloadable network based SVFs at one time and HK$120,000 for money changing transactions), an SVF licensee should keep all documents and records mentioned in paragraph 8.3 for a period of at least five years after the date of the transaction.
	8.5	An SVF licensee should maintain the original or a copy of the documents, and a record of the data and information, obtained in connection with each transaction the SVF licensee carries out, both domestic and international, which should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.
	8.6	All documents and records mentioned in paragraph 8.5 should be kept for a period of at least five 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, by notice in writing to an SVF licensee, require it to keep the records relating to a specified transaction or customer for a 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.

[69] An SVF licensee is 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.

	8.9	Irrespective of where CDD and transaction records are held, an SVF licensee is required to comply with all legal and regulatory requirements in Hong Kong, including the requirements specified under this Guideline.
Records kept by intermediaries		
	8.10	Where customer identification and verification documents are held by an intermediary on which an SVF licensee is relying to carry out CDD measures, the SVF licensee concerned remains responsible for compliance with all record-keeping requirements. The SVF licensee should ensure that the intermediary being relied on has systems in place to comply with all the record-keeping requirements under this Guideline (including the requirements of paragraphs 8.3 to 8.9), and that documents and records will be provided by the intermediary as soon as reasonably practicable after the intermediary receives the request from the SVF licensee.
	8.11	For the avoidance of doubt, an SVF licensee that relies on an intermediary for carrying out a CDD measure should immediately obtain data or information that the intermediary has obtained in the course of carrying out that measure.
	8.12	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.

Chapter 9 – STAFF TRAINING		
	9.1	Ongoing 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	It is an SVF licensee's responsibility to provide adequate training for its staff so that they are adequately trained to implement its AML/CFT Systems. The scope and frequency of training should be tailored to the specific risks faced by the SVF licensee and pitched according to the job functions, responsibilities and experience of the staff. New staff should be required to attend initial training as soon as possible after being hired or appointed. Apart from the initial training, an SVF licensee should also provide refresher training regularly to ensure that its staff are reminded of their responsibilities and are kept informed of new developments related to ML/TF.
	9.3	An SVF licensee should implement a clear and well-articulated policy for ensuring that relevant staff receive adequate AML/CFT training.
	9.4	Staff should be made aware of: (a) their SVF licensee's and their own personal statutory obligations and the possible consequences for failure to comply with AML/CFT requirements under the PSSVFO; (b) 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; (c) 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; (d) the SVF licensee's policies and procedures relating to AML/CFT, including suspicious transaction identification and reporting; and (e) 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.
	9.5	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 roles 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 suspicious transaction reports submitted to them and reporting of suspicious transactions to the JFIU; and (ii) training to keep abreast of AML/CFT requirements/developments generally.
	9.6	An SVF licensee is 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. An SVF licensee may consider including available FATF papers and typologies as part of the training materials. The SVF licensee should be able to demonstrate to the HKMA that all materials are up-to-date and in line with current requirements and standards.
	9.7	No matter which training approach is adopted, an SVF licensee should 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.

	9.8	An SVF licensee 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; (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; and (c) monitoring attendance and following up with staff who miss such training without reasonable cause.

Chapter 10 – WIRE TRANSFERS		
General		
	10.1	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) at an 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. An SVF licensee should follow the relevant requirements set out in this Chapter with regard to its role in a wire transfer.
	10.2	Where an SVF licensee is the originator or recipient of a wire transfer, it is not acting as an ordering institution, an intermediary institution or a beneficiary institution and thus is not required to comply with the requirements in this Chapter in respect of that transaction.
	10.3	The requirements set out in this Chapter are also applicable to wire transfers using cover payment mechanism (e.g. MT202COV payments)[70].
	10.4	This Chapter does not apply to the following wire transfers: (a) a wire transfer between an SVF licensee and an FI as defined in the AMLO if each of them acts on its own behalf; (b) a wire transfer between an SVF licensee and a foreign institution[71] 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.

[70] Reference should be made to the paper "Due diligence and transparency regarding cover payment messages related to cross-border wire transfer" published by the Basel Committee on Banking Supervision in May 2009 and the "Guidance Paper on Cover Payment Messages Related to Cross-border Wire Transfers" issued by the HKMA in February 2010.

[71] For the purpose of this Chapter, "foreign institution" means an institution that is located in a place outside Hong Kong and that carries on a business similar to that carried on by an FI as defined in the AMLO.

Ordering institutions		
	10.5	An ordering institution should ensure that a wire transfer of amount equal to or above HK$8,000 (or an equivalent amount in any other currency) is accompanied by the following originator and recipient information: (a) the originator's name; (b) the number of the originator's account maintained with the ordering institution and from which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned to the wire transfer by the ordering institution; (c) the originator's address or, the originator's customer identification number[72] or identification document number or, if the originator is an individual, the originator's date and place of birth; (d) the recipient's name; and (e) the number of the recipient's account maintained with the beneficiary institution and to which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned to the wire transfer by the beneficiary institution.
	10.6	An ordering institution should ensure that a wire transfer of amount below HK$8,000 (or an equivalent amount in any other currency) is accompanied by the following originator and recipient information: (a) the originator's name; (b) the number of the originator's account maintained with the ordering institution and from which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned to the wire transfer by the ordering institution; (c) the recipient's name; and (d) the number of the recipient's account maintained with the beneficiary institution and to which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned to the wire transfer by the beneficiary institution.
	10.7	The unique reference number assigned by the ordering institution or beneficiary institution referred to in paragraphs 10.5 and 10.6 should permit traceability of the wire transfer.

[72] Customer identification number refers to a number which uniquely identifies the originator to the originating institution and is a different number from the unique transaction reference number referred to in paragraph 10.7. The customer identification number should refer to a record held by the originating institution which contains at least one of the following: the customer address, the identification document number, or the date and place of birth.

	10.8	For a wire transfer of amount equal to or above HK$8,000 (or an equivalent amount in any other currency), an ordering institution should ensure that the required originator information accompanying the wire transfer is accurate.
	10.9	For a wire transfer, including an occasional wire transfer, involving an amount equal to or above HK$8,000 (or an equivalent amount in any other currency), an ordering institution should verify the identity of the originator in compliance with Chapter 4 of this Guideline. For a wire transfer below HK$8,000 (or an equivalent amount in any other currency), the ordering institution is 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 above HK$8,000 (or an equivalent amount in any other currency), or when there is a suspicion on ML/TF.
	10.10	An ordering institution may bundle a number of wire transfers from a single originator into a batch file for transmission to a recipient or recipients in a place outside Hong Kong. In such cases, the ordering institution may only include the originator's account number or, in the absence of such an account, a unique reference number in the wire transfer but the batch file should contain required and accurate originator information, and required recipient information, that is fully traceable within the recipient country.
	10.11	For a domestic wire transfer[73], an ordering institution may choose not to include the complete required originator information in the wire transfer but only include the originator's account number or, in the absence of an account, a unique reference number, provided that the number permits traceability of the wire transfer.
	10.12	If an ordering institution chooses not to include complete required originator information as stated in paragraph 10.11, it should, on the request of the institution to which it passes on the transfer instruction or the HKMA, provide complete required originator information within 3 business days after the request is received. In addition, such information should be made available to law enforcement agencies immediately upon request.
Intermediary institutions		
	10.13	An intermediary institution should ensure that all originator and recipient information which accompanies the wire transfer is retained with the transfer and is transmitted to the institution to which it passes on the transfer instruction.

[73] Domestic wire transfer means a wire transfer in which the ordering institution and the beneficiary institution and, if one or more intermediary institutions are involved in the transfer, the intermediary institution or all the intermediary institutions are FIs (as defined in the AMLO) located in Hong Kong.

	10.14	Where technical limitations prevent the required originator or recipient information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary institution should keep a record, for at least five years, of all the information received from the ordering institution or another intermediary institution. The above requirement also applies to a situation where technical limitations prevent the required originator or recipient information accompanying a domestic wire transfer from remaining with a related cross-border wire transfer.
	10.15	An intermediary institution should establish and maintain effective procedures for identifying and handling incoming wire transfers that do not comply with the relevant originator or recipient information requirements, which include: (a) taking reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or required recipient information; and (b) having risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator information or required recipient information; and (ii) the appropriate follow-up action.
	10.16	In respect of the risk-based policies and procedures referred to in paragraph 10.15, if a cross-border wire transfer is not accompanied by the required originator information or required recipient information, the intermediary institution should as soon as reasonably practicable, obtain the missing information from the institution from which it receives the transfer instruction. If the missing information cannot be obtained, the intermediary institution should either consider restricting or terminating its business relationship with that institution, or take reasonable measures to mitigate the risk of ML/TF involved.
	10.17	If the intermediary institution is aware that the accompanying information that purports to be the required originator information or required recipient information is incomplete or meaningless, it should as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved.
Beneficiary institutions		
	10.18	A beneficiary institution should establish and maintain effective procedures for identifying and handling incoming wire transfers that do not comply with the relevant originator or recipient information requirements, which include: (a) taking reasonable measures (e.g. post-event monitoring) to

		identify domestic or cross-border wire transfers that lack required originator information or required recipient information; and (b) having risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator information or required recipient information; and (ii) the appropriate follow-up action.
	10.19	In respect of the risk-based policies and procedures referred to in paragraph 10.18, if a domestic or cross-border wire transfer is not accompanied by the required originator information or required recipient information, the beneficiary institution should as soon as reasonably practicable, obtain the missing information from the institution from which it receives the transfer instruction. If the missing information cannot be obtained, the beneficiary institution should either consider restricting or terminating its business relationship with that institution, or take reasonable measures to mitigate the risk of ML/TF involved.
	10.20	If the beneficiary institution is aware that the accompanying information that purports to be the required originator information or required recipient information is incomplete or meaningless, it should as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved.
	10.21	For a wire transfer of amount equal to or above HK$8,000 (or an equivalent amount in any other currency), a beneficiary institution should verify the identity of the recipient in compliance with Chapter 4 of this Guideline, if the identity has not been previously verified.

APPENDIX

Limits for conducting CDD for SVF products

1. Device-based SVF

Maximum Stored Value (in HK$)	Domestic Payments for Goods or Services only	Cross-Border Payments for Goods or Services		Making Person-to-Person Fund Transfers / Cash Withdrawal Function
		Funding from Identifiable Source[74]	Funding from Unidentifiable Source	
≤ 3,000	No CDD required	No CDD required	CDD under Chapter 4 of this Guideline	CDD under Chapter 4 of this Guideline
> 3,000	CDD under Chapter 4 of this Guideline			

[74] An identifiable source may include (i) an account in a licensed bank, (ii) a credit card issued by an authorized institution or an authorized institution's subsidiary, (iii) an account of a verified customer or a pre-existing customer in an SVF licensee, or (iv) an account in 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. For the avoidance of doubt, any anonymous funding source, including cash, anonymous prepaid card or anonymous financial instrument would not be considered as an identifiable source.

2. Network-based SVF

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

<table>
<tr><th rowspan="2">Maximum Stored Value (in HK$)</th><th rowspan="2">Domestic Payments for Goods or Services only</th><th colspan="2">Cross-Border Payments for Goods or Services</th><th rowspan="2">Making Person-to-Person Fund Transfers / Cash Withdrawal Function</th></tr>
<tr><th>Funding from Identifiable Source</th><th>Funding from Unidentifiable Source</th></tr>
<tr><td>≤ 8,000</td><td>No CDD required</td><td>No CDD required</td><td>CDD under Chapter 4 of this Guideline</td><td rowspan="2">CDD under Chapter 4 of this Guideline</td></tr>
<tr><td>> 8,000</td><td colspan="3">CDD under Chapter 4 of this Guideline</td></tr>
</table>

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

<table>
<tr><th rowspan="2">Annual Transaction Amount (in HK$)</th><th rowspan="2">Domestic Payments for Goods or Services only</th><th colspan="2">Cross-Border Payments for Goods or Services / Making Person-to-Person Fund Transfers</th><th rowspan="2">Cash Withdrawal Function</th></tr>
<tr><th>Funding from Identifiable Source</th><th>Funding from Unidentifiable Source</th></tr>
<tr><td>≤ 25,000</td><td>No CDD required[75]</td><td>No CDD required[75]</td><td>CDD under Chapter 4 of this Guideline</td><td rowspan="2">CDD under Chapter 4 of this Guideline</td></tr>
<tr><td>> 25,000</td><td colspan="3">CDD under Chapter 4 of this Guideline</td></tr>
</table>

[75] 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.

(iii) Pre-existing customer

<table>
<tr><th>Annual Transaction Amount (in HK$)</th><th>Payments for Goods or Services / Making Person-to-Person Fund Transfers</th><th>Cash Withdrawal Function</th></tr>
<tr><td>≤ 8,000</td><td rowspan="2">(i) Obtain a copy of the customer's identification document; and
(ii) Require the customer to make a credit transfer from the customer's account in a licensed bank</td><td>(i) Obtain a copy of the customer's identification document; and
(ii) Require the customer to make a credit transfer from the customer's account in a licensed bank</td></tr>
<tr><td>> 8,000 to ≤ 100,000</td><td rowspan="2">CDD under Chapter 4 of this Guideline</td></tr>
<tr><td>> 100,000</td><td>CDD under Chapter 4 of this Guideline</td></tr>
</table>

GLOSSARY OF KEY TERMS AND ABBREVIATIONS	
Terms / abbreviations	**Meaning**
AI(s)	Authorized institution(s)
AMLO	Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)
AML/CFT	Anti-money laundering and counter-financing of terrorism
AML/CFT Systems	AML/CFT policies, procedures and controls
CDD	Customer due diligence
CO	Compliance officer
DTROP	Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405)
EDD	Enhanced due diligence
FATF	Financial Action Task Force
FI(s)	Financial institution(s) (Note: Unless specified otherwise (e.g. an FI as defined in the AMLO), the term "financial institutions (FIs)" has the same definition as set out in the FATF Recommendations. Financial institution(s) as defined in the AMLO includes 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.)
HKMA	Hong Kong Monetary Authority
JFIU	Joint Financial Intelligence Unit
MLRO	Money laundering reporting officer
ML/TF	Money laundering and terrorist financing
OSCO	Organized and Serious Crimes Ordinance (Cap. 455)
PEP(s)	Politically exposed person(s)
Proliferation financing or PF	Financing of proliferation of weapons of mass destruction
PSSVFO	Payment Systems and Stored Value Facilities Ordinance (Cap. 584)

RA(s)	Relevant authority (authorities) includes 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) and the Registrar of Companies (in relation to a TCSP licensee).
RBA	Risk-based approach
SDD	Simplified due diligence
STR(s)	Suspicious transaction report(s)
SVF	Stored value facility
TCSP	Trust or company service provider
Tiered approach	Tiered approach to customer due diligence
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)
WMD(CPS)O	Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap. 526)