SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

Consultation Conclusions on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators Licensed by the Securities and Futures Commission

23 May 2023

Table of Contents

Executive summary

1. On 20 February 2023, the Securities and Futures Commission (SFC) issued a consultation paper[1] inviting public comments on proposed regulatory requirements applicable to licensed virtual asset trading platform operators (VA trading platforms) as set out in: Guidelines for Virtual Asset Trading Platform Operators (VATP Guidelines); Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset Service Providers) (AML Guideline for LCs and SFC-licensed VASPs); Prevention of Money Laundering and Terrorist Financing Guideline issued by the Securities and Futures Commission for Associated Entities of Licensed Corporations and SFC-licensed Virtual Asset Service Providers (AML Guideline for AEs, together with the AML Guideline for LCs and SFC-licensed VASPs, the AML Guidelines); and Disciplinary Fining Guidelines.

2. During the consultation period, which ended on 31 March 2023, the SFC received 152 written submissions from industry and professional associations, professional firms, consultancy firms, market participants, licensed corporations, individuals and other stakeholders. A list of respondents (other than those who requested anonymity) is set out in Appendix E to this conclusions paper.

3. Respondents generally supported the proposed regulatory requirements for licensed VA trading platforms. Many of the comments sought clarification of the technical and implementation details. Key comments related to retail access to licensed VA trading platforms, the criteria for token admission, compensation arrangements for the risks associated with custody of client assets, trading in virtual asset derivatives, implementation details and the transitional arrangements. The key comments received and the SFC's responses are discussed in this conclusions paper.

4. The SFC has carefully considered the responses and revised the proposed regulatory requirements where appropriate. The marked-up texts of the revised proposed regulatory requirements are set out in Appendices A, B and C to this conclusions paper. We will also issue further guidance and clarifications where appropriate.

5. The SFC would like to thank all respondents for their time and effort in reviewing the proposals and providing us with their comments.

6. The revised proposed regulatory requirements will become effective on 1 June 2023.

7. The consultation paper, the responses (other than those from respondents who requested their submission be withheld from publication) and this conclusions paper are available on the SFC website at www.sfc.hk.

[1] Consultation Paper on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators Licensed by the Securities and Futures Commission (https://apps.sfc.hk/edistributionWeb/api/consultation/openFile?lang=EN&refNo=23CP1).

Comments received and the SFC's responses

Part I: Amendments to the proposed regulatory requirements for licensed VA trading platform operators

A. Allow retail access to licensed VA trading platforms

Question 1:

Do you agree that licensed platform operators should be allowed to provide their services to retail investors, subject to the robust investor protection measures proposed? Please explain your views.

Retail access

Public comments

8. A significant majority of respondents agreed to our proposal to allow licensed VA trading platforms to provide their services to retail investors. Many respondents echoed the view that denying retail access may result in investor harm as retail investors may be pushed to trade on unregulated VA trading platforms overseas.

9. A number of respondents expressed the view that allowing retail access to virtual assets traded on licensed VA trading platforms will not only provide retail investors with an opportunity to diversify their investment portfolios and deepen Hong Kong's liquidity pool but will also facilitate the development and growth of associated technologies and industries in Hong Kong.

10. Most respondents agreed that proper regulatory oversight is key to addressing the allegations of misuse of client assets and solvency concerns frequently seen in recent industry crises. A majority of these respondents were of the view that, if licensed VA trading platforms are required to comply with a range of robust investor protection measures in relation to, amongst other things, investor knowledge and training, investor risk assessments and information disclosures, then retail access to licensed VA trading platforms could be allowed.

11. Some respondents who disagreed with allowing retail access were of the view that many virtual assets did not have any substance or that retail investors would not have sufficient knowledge and understanding of the risks involved or lack the information needed to make an informed investment decision. While not objecting to the proposal, one respondent cautioned that allowing retail investors' participation should not be seen as an endorsement or an encouragement to trade virtual assets.

The SFC's response

12. We note the strong support expressed for allowing licensed VA trading platforms to provide their services to retail investors and will allow licensed VA trading platforms to provide their services to retail investors.

13. As explained in the consultation paper, we agree that licensed VA trading platforms should comply with a range of robust investor protection measures covering

onboarding, governance, disclosure and token due diligence and admission, before providing trading services to retail investors.

14. We also agree that it is important that retail investors understand the risks involved in investing in virtual assets. Before making any type of investment decision, investors should understand the features and risks and be prepared for losses. The SFC's approval of the admission of a virtual asset for retail trading by a licensed VA trading platform is not a recommendation or endorsement nor does it guarantee the virtual asset's commercial merits or performance. The SFC will continue its efforts with the Investor and Financial Education Council to educate investors about all aspects of virtual assets and their trading.

Onboarding requirements

Public comments

15. The majority of respondents agreed to the imposition of the requirements for onboarding retail clients. In particular, many respondents agreed that it is important to require knowledge and risk assessments and investor training as well as to impose an exposure limit. Most respondents who considered the issue were of the view that retail clients should have knowledge of virtual assets before trading. However, one respondent disagreed with the proposal that a client could be presumed to have knowledge of virtual assets if the client had executed five or more transactions in any virtual asset within the past three years.

16. Several respondents recommended various exemptions to the onboarding measures. For example, VA trading platforms serving clients subject to an exposure limit lower than a certain threshold (eg, retail clients who are purchasing a virtual asset for paying gas fees) could be exempt from the knowledge and risk assessment requirements, or clients who passed the knowledge assessment could be exempt from the risk assessment requirement. A few respondents requested that individual professional investors be exempt from the onboarding requirements entirely. Some respondents were of the view that onerous onboarding requirements would push retail investors to trade through unregulated platforms.

17. Many respondents suggested that the SFC work with industry associations to establish uniform standards for knowledge and risk assessments and investor education to ensure consistency amongst licensed VA trading platforms. Some respondents also asked that the SFC provide more detailed guidance, such as how to remedy a breach of the exposure limit due to market volatility.

The SFC's response

18. We welcome the general support for imposing the onboarding requirements in relation to retail clients.

19. As to whether individual professional investors should be exempt from the onboarding requirements, the proposed application of the requirements to individual professional investors is in line with the existing requirements governing derivatives knowledge assessments and suitability which apply without exception when intermediaries serve individual professional investors. Given that the onboarding requirements were designed in the spirit of suitability, it remains our view that

individual professional investors should be subject to similar protections as retail investors.

20. We have duly considered suggestions to relax specific aspects of the onboarding requirements for retail clients under certain circumstances. However, we are of the view that the terms, features and risks of virtual assets are generally not likely to be understood by a retail investor. Coupled with the fact that trading on VA trading platforms occurs automatically and VA trading platforms are unable to intervene if a trade is unsuitable, it is vital to ensure suitability in the onboarding of retail clients. This can only be achieved through the implementation of the full scope of proposed onboarding requirements. For example, the proposed requirement to assess a client's risk tolerance is part and parcel of the existing suitability requirement. As most virtual assets are high risk, they are only suitable for clients who have high risk tolerance. VA trading platforms thus should not be exempt from conducting the risk tolerance assessment even if a retail client is knowledgeable about virtual assets.

21. In light of the importance of ensuring retail investors have sufficient knowledge of virtual assets before they are allowed to trade, the SFC is of the view that platform operators should conduct a holistic assessment of an investor's understanding of the nature and risks of virtual assets, which could include an assessment of virtual asset training or courses that the investor has previously attended, the investor's current or previous work experience related to virtual assets and the investor's prior trading experience in virtual assets. We have thus revised the VATP Guidelines accordingly. As the knowledge assessment requirement applies not only to VA trading platforms but also to other intermediaries engaging in virtual asset-related activities, corresponding amendments will also be made to ensure alignment for all intermediaries.

22. The SFC fully acknowledges the requests for more guidance on the onboarding requirements. We will issue further guidance in the form of frequently-asked-questions (FAQs), for example, on how to assess a client's risk tolerance and exposure to virtual assets. While we understand that the industry may wish for more certainty, such as specifying the exposure limits for investors of different financial situations and risk tolerance levels, it may not be appropriate for the SFC to be prescriptive in this regard, as platform operators, and not the SFC, would be in the best position to impose limits which take into account information obtained from the know-your-client process on a best effort basis.

Governance

Public comments

23. A significant majority of the respondents who commented on this issue agreed to the establishment of a token admission and review committee. Queries on the proposal included who the persons "principally responsible for" different areas of the platform could be, and whether independent external members should be appointed to the committee due to members' possible conflicts of interest when considering token admissions.

The SFC's response

24. We are pleased to note the strong support for requiring a licensed VA trading platform to establish a token admission and review committee to enhance its

governance. It is our intention that members "principally responsible for" managing the key business line, compliance, risk management and information technology will at least include the corresponding managers-in-charge (MICs) of the platform operator[2].

25. We agree that any conflicts of interest involving committee members and the platform operator should be considered and adequately dealt with. This could be done through various measures such as declarations of interests by committee members and abstaining from considering matters in relation to those virtual assets which the committee member has an interest in. Platform operators should ensure that they have in place internal policies and procedures to deal with conflicts. Provided that adequate policies and procedures are in place, the SFC is of the view that it would not be necessary to require platform operators to appoint independent external members to the committee.

Disclosure obligations

Public comments

26. The majority of respondents agreed that the imposition of disclosure obligations for each admitted virtual asset is important for the protection of investors. However, considering that licensed VA trading platforms may republish information provided by an issuer or other parties, several respondents raised concerns about the potentially onerous burden of ensuring the accuracy of this information. A number of respondents weighed in by suggesting amendments to the list of information requiring disclosure.

The SFC's response

27. The SFC is aware that due to the unique nature of virtual assets, which unlike traditional securities are not regulated at a product level and are traded on numerous platforms globally, it may be difficult to obtain and verify information from an issuer.

28. On the other hand, a licensed VA trading platform is required to conduct due diligence on each virtual asset prior to admission for trading. To adequately discharge its due diligence obligations and enable it, and particularly its token admission and review committee, to decide whether to admit a particular token for trading, a platform operator is expected to obtain information for each virtual asset – whether directly from the issuer or otherwise – which it can be reasonably satisfied is reliable and sufficient to base its token admission decision on.

29. Based on the above, the SFC thus proposed requiring licensed VA trading platforms to act with due skill, care and diligence when disclosing information. This is aligned with requirements imposed on other intermediaries which post information on their online platforms. We have further refined the disclosure obligations in the VATP Guidelines to require platform operators to take all reasonable steps to ensure the product specific information they disclose is not false, biased, misleading or

[2] We will be issuing further guidance in the form of FAQs on a MICs regime to augment accountability of licensed VA trading platforms' senior management, which will be substantially the same as that for licensed corporations under the Securities and Futures Ordinance (Cap. 571) (SFO).

deceptive. We have also made amendments to the list of information requiring disclosure based on suggestions put forward by some respondents.

Question 2:

Do you have any comments on the proposals regarding the general token admission criteria and specific token admission criteria?

General token admission criteria and other token due diligence to be performed

Public comments

30. The majority of respondents agreed that licensed VA trading platforms should have regard to general token admission criteria prior to admitting any virtual asset for trading. Several respondents asked for exemptions for virtual assets with large market capitalisations, for virtual assets which have already been admitted for trading on a licensed VA trading platform or for unsolicited execution-only transactions.

31. Similar to the disclosure obligations, several respondents raised concerns about the potentially onerous burden on licensed VA trading platforms in conducting due diligence and ongoing monitoring of virtual assets based on the general token admission criteria (eg, they should be allowed to rely on information provided by an issuer or due diligence conducted by a third party). A few respondents requested that the SFC provide detailed guidance on the admission threshold for virtual assets (eg, how much of a concentration of holdings will make a virtual asset inadmissible).

32. Some respondents specifically asked that the SFC remove the requirement for a 12-month track record to facilitate the admission of newly-launched non-security tokens, while others took issue with the requirement for licensed VA trading platforms to conduct a smart contract audit.

33. Other respondents weighed in that retail investors should be allowed to trade security tokens and a licensed VA trading platform should not be required to seek and submit legal advice on whether a virtual asset is a “security”.

The SFC’s response

34. Fundamentally, an intermediary is required to know the product that it is offering. Intermediaries making investment products available on their online platforms are required to conduct product due diligence and this is irrespective of whether a client ultimately purchases an investment product via the online platform on an execution-only basis or under advice. Applying the same fundamental principle, a licensed VA trading platform should conduct due diligence on each token before admission for trading. As such, we do not deem it appropriate to provide any exemption from conducting due diligence such as for a token that has been admitted on another licensed VA trading platform.

35. The SFC believes that many technical comments arose due to the prescriptive nature of the due diligence requirements as set out in the proposed VATP Guidelines. For example, we proposed requiring a platform operator to consider the regulatory status of a virtual asset in each jurisdiction in which the platform operator provides trading services and also whether the virtual asset's regulatory status may affect the regulatory obligations of the platform operator. This was designed so that platform operators would consider whether a virtual asset should be admitted for trading in Hong Kong if, for example, it was found to be a security in another jurisdiction, and for platform operators to consider whether the continued provision of trading services in a particular token in another jurisdiction may be in breach of the laws of that jurisdiction.

36. Noting the comments that a token admitted for trading should comply with all laws, rules and regulations in Hong Kong and that any limitation in other jurisdictions which does not affect the token's regulatory status in Hong Kong may not be a relevant consideration, instead of requiring the platform operator to consider the token's regulatory status in each jurisdiction in which the platform operator provides trading services, we will only require the platform operator to consider the regulatory status of the virtual asset in Hong Kong. Nevertheless, platform operators are reminded that they should ensure that their operations are compliant with local laws and regulations in all jurisdictions where they or their affiliates operate, as any breach of those requirements would affect the fitness and properness of the platform operator to continue to provide services in Hong Kong.

37. Regarding the comments on the requirement for a non-security token to have at least a 12-month track record, this requirement was proposed specifically due to the inherent difficulties platform operators may face when conducting due diligence. While a 12-month requirement may not have prevented the recent collapses of some tokens, this requirement aims to reduce the risk of reasonably hard-to-detect fraud as well as the possible impact on the price of a token of the marketing efforts leading up to its initial offering, especially since token offerings are generally unregulated and not subject to the safeguards which are present in the traditional securities markets.

38. In relation to requiring a smart contract audit, we wish to clarify that the SFC only expects a licensed VA trading platform to engage an independent assessor or, where reasonable, to rely on an audit conducted by an independent assessor engaged by another party (for example, the issuer). We have made corresponding clarifications in the VATP Guidelines. This is a key requirement as a successful exploitation of a flaw in the smart contract could cause material harm to investors.

39. Security tokens cannot be offered to retail investors in breach of the prospectus regime under the Companies (Winding Up and Miscellaneous Provisions) Ordinance (Cap. 32) (C(WUMP)O) and the offers of investments regime under Part IV of the SFO. We thus proposed that platform operators obtain and submit to the SFC written legal advice confirming that each token made available for trading by retail clients would not amount to a security token. Acknowledging the potentially significant costs of obtaining legal advice on the regulatory status of each virtual asset, we have removed the requirement to submit such legal advice to the SFC from the VATP Guidelines. Platform operators are nevertheless reminded of their obligations and to take reasonable steps under the relevant laws to ensure that retail trading of any token they make available will not breach the public offering regimes in Hong Kong. Notwithstanding this, as part of the approval process, the

SFC may request legal opinions on specific tokens in light of developments in other jurisdictions.

40. With regard to the comments on the due diligence requirements, we would like to stress again that the underlying principle is that when selecting virtual assets to be made available for trading, licensed VA trading platforms should exercise due skill, care and diligence through conducting all reasonable due diligence. We have revised the due diligence requirements to be more principles-based and will supplement them with guidance in FAQs which will address some of the comments received.

Specific token admission criteria

Public comments

41. Several respondents commented that it was not clear from the list of criteria which indices would be acceptable and asked that the SFC publish a list of acceptable indices or a list of index providers with experience in publishing indices for the conventional securities market, as well as a list of eligible large-cap virtual assets. Some suggested that licensed VA trading platforms should be able to admit virtual assets by relying on such lists published by the SFC or admission on other licensed VA trading platforms.

42. Other respondents requested that the SFC provide additional guidance on the underlying principles for approving virtual assets for retail trading and questioned whether other factors such as adverse news should form part of the specific token admission criteria. Several respondents raised further concerns regarding the reliability of indices, for example, that transaction data may come from unreliable sources and the risks of potential collusion and exploitation of insider information.

43. A few respondents queried the need for the SFC's prior approval for virtual assets for retail trading on licensed VA trading platforms.

44. Certain respondents commented that the specific token admission criteria will result in a small number of virtual assets being eligible for retail trading. These respondents suggest that the specific token admission criteria be relaxed (eg, to include the top 200 virtual assets instead of the top 10) to allow licensed VA trading platforms to provide retail clients with access to a broader range of virtual assets. Several respondents noted having a large market capitalisation does not automatically translate to high liquidity. They also expressed concern that stablecoins and locally developed virtual assets are unlikely to be eligible for retail trading under these criteria.

The SFC's response

45. The SFC would like to take this opportunity to articulate the principles underlying the specific token admission criteria.

46. As explained in the consultation paper, in the conventional securities markets, investment products offered to the retail public in Hong Kong are subject to the

offers of investments[3] and prospectus[4] regimes. Retail products are generally subject to the SFC's regulation at the product level. The SFC would have vetted or reviewed their offering and marketing materials prior to public offering. This does not apply to non-security tokens, and most, if not all, non-security tokens are not regulated at the product level by any regulatory authority anywhere. This explains the need for the SFC's approval before a token can be admitted for retail trading on a licensed VA trading platform.

47. Therefore, we proposed that tokens meet additional minimum criteria before they could be traded by retail investors. These criteria are based on the underlying principle that tokens accessible by retail investors should be less prone to market manipulation, not just on the platform operated by the platform operator but across the virtual asset market as a whole, given that most, if not all, VA trading platforms are currently unregulated or only regulated from an AML/CFT (anti-money laundering/counter-financing of terrorism) perspective across the globe. This is reflected in our proposed requirement that, to be eligible for trading by retail investors, tokens must be eligible large-cap virtual assets included in at least two acceptable indices issued by two independent index providers.

48. We appreciate the comments on acceptable indices and the independence of an index provider. We agree that it is important the indices are robustly constituted and administered, including ensuring their quality and integrity. The criteria for determining whether an index is an acceptable index were formulated with these principles in mind, and the additional requirement that one index provider should have experience in publishing indices for the conventional securities market was introduced to enhance reliability. We agree that, as raised by some respondents, the reliability of the underlying data and possibility of conflicts of interest may affect an index's integrity. We thus find it appropriate to further require that the index provider with experience in publishing indices for the conventional securities market complies with the IOSCO[5] Principles for Financial Benchmarks[6] such that it has proper internal arrangements in place to protect the integrity and ensure the quality of its indices. In addition to being independent of each other, we will also require that the two index providers should be independent of the issuer of the virtual asset and also of the platform operator.

49. We acknowledge that for virtual assets a large market capitalisation does not automatically correlate to high liquidity. The SFC would like to reiterate that being included in two acceptable indices is not the sole criterion for admitting a virtual asset. It is merely a minimum criterion. This highlights the importance attached to the due diligence conducted by a licensed VA trading platform. Platform operators are required to conduct further due diligence based on, and ensure tokens admitted to trading satisfy, the platform's token admission criteria, and in the case of tokens for retail trading, ensure that they also have high liquidity. Platform operators should also ensure that admitted tokens continue to satisfy the token admission criteria. As the admissibility and continued eligibility of a token for trading depends on the due diligence conducted by a platform operator, it would not be appropriate for the SFC to publish lists of virtual assets eligible for retail trading, acceptable indices or index providers.

[3] Part IV of the SFO.
[4] Parts II and XII of the C(WUMP)O.
[5] The International Organization of Securities Commissions.
[6] Principles for Financial Benchmarks Final Report (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD415.pdf).

50. We thank respondents for their extensive comments on the specific token admission criteria and have revised the VATP Guidelines to reflect the discussion above.

51. We note the international focus on the risks posed by stablecoins and the push for regulation of stablecoins to ensure, amongst other things, that stablecoin reserves are properly managed to maintain price stability and enable investors to exercise redemption rights. These risks have fundamental implications for the stability of a stablecoin. A stablecoin which is unable to maintain its peg or return an investor's funds upon redemption cannot be said to be stable. In addition, heightened vulnerability to runs greatly affects their liquidity and renders them generally unsuitable for retail investors. The Hong Kong Monetary Authority (HKMA) published the conclusion on its discussion paper on crypto-assets and stablecoins in January 2023[7] and the regulatory arrangements for stablecoins are expected to be implemented in 2023/24. Prior to stablecoins being subject to regulation in Hong Kong, it is our view that they should not be admitted for retail trading.

Question 3:

What other requirements do you think should be implemented from an investor protection perspective if the SFC is minded to allow retail access to licensed VA trading platforms?

Public comments

52. Some respondents advocated for a prohibition on licensed VA trading platforms offering incentives and monetary benefits to retail investors to trade virtual assets. This could prevent the creation of inappropriate motives for retail investors to trade virtual assets.

53. Several respondents commented that the SFC may consider introducing a cooling-off mechanism for retail clients before (eg, the first 24 hours after account opening) and after (eg, with a right to unwind or cancel transactions or a right to request a buy-back) they conduct a transaction in a virtual asset.

The SFC's response

54. We agree that platform operators should not offer gifts tied to the trading of a specific virtual asset, as is the case with all other intermediaries. This principle formed the basis for the requirement that platform operators should not post any advertisement in connection with a specific virtual asset. In light of the comments received, we have now made the prohibition of gifts explicit in the VATP Guidelines, with the exception of discounts of fees or charges. The SFC would also like to take this opportunity to remind platform operators of their obligation to ensure that any product-specific materials they post, whether on- or off-platform, are factual, fair and balanced.

[7] Conclusion of discussion paper on crypto-assets and stablecoins (https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/01/20230131-9/).

55. The SFC currently does not impose a cooling-off period after account opening for retail clients of intermediaries conducting other regulated activities, including the provision of automated trading services. As platform operators are required to ensure suitability in the onboarding process, any retail client who was onboarded should have been assessed by the platform operator as being suitable for trading virtual assets. A cooling-off period after a trade is not practicable for automated trading services where trades are matched between clients as unwinding or cancelling a transaction would affect another client.

B. Maintain an insurance or compensation arrangement

Question 4:

Do you have any comments on the proposal to allow a combination of third-party insurance and funds set aside by the licensed platform operator or a corporation within its same group of companies? Do you propose other options?

Question 5:

Do you have any suggestions as to how funds should be set aside by the licensed platform operators (for instance, under house account of the licensed platform operator or under an escrow arrangement)? Please explain in detail the proposed arrangement and how it may provide the same level of comfort as third-party insurance.

Public comments

56. The majority of respondents supported requiring licensed VA trading platforms to have in place an insurance or compensation arrangement for risks associated with custody of client assets. However, some respondents pointed out that the arrangement to set aside funds would result in a high cost of capital and would affect the competitiveness of licensed VA trading platforms. While some respondents agreed that client virtual assets held in hot storage should be fully covered by insurance or funds set aside, they were of the view that client virtual assets held in cold storage need not be fully covered in view of the relatively lower risks involved. A number of respondents queried whether set aside funds could also include virtual assets. There were different views on the most appropriate arrangement.

57. Regarding the appropriate level of coverage, most respondents were of the view that full coverage over all client assets under custody may be too onerous, and their proposals included the following:

(a) a different coverage level for each platform based on the robustness of each platform's custody systems; and

(b) uniform coverage for each platform with decreasing coverage for each year during which no adverse custody-related events take place.

58. Several respondents asked the SFC to set out factors which it would consider in determining the appropriate level of coverage and the appropriate combination of arrangements.

59. With regard to the types of assets that could form part of a compensation arrangement in addition to third party insurance, suggestions included the following:

(a) bank guarantees, as they are currently allowed under the Hong Kong stored value facility regime;

(b) "eligible large-cap virtual assets"; and

(c) funds invested in guaranteed return products with high liquidity (or even virtual asset-related exchange traded funds).

60. In relation to how the compensation arrangement could be set up, suggestions included the following:

(a) an escrow agent could be used, as the funds would be segregated and would not form part of a VA trading platform's assets in the event of insolvency;

(b) a designated bank account could hold funds on trust (with an acknowledgement letter from the bank and monthly reports to be submitted to the SFC);

(c) a pool of funds could be established amongst licensed VA trading platforms which could take the form of an insurer authorised by the Insurance Authority or other compensation scheme; and

(d) a segregated wallet should be used if virtual assets could form part of the compensation arrangement. However, an escrow arrangement may not provide much comfort as it would require the use of a third-party custodian which may not be subject to the same custody requirements for wallet infrastructure and cybersecurity measures as licensed platform operators.

The SFC's response

61. We appreciate comments and suggestions received in response to this proposal and the requests for more clarity.

62. The risks to client virtual assets held in cold storage are generally similar to custody risks associated with client assets in the traditional financial markets, namely, misappropriation by employees and fraud. Noting that clients of traditional financial institutions are not fully insured against the loss of their assets, we believe there is room for lowering the coverage threshold for client virtual assets held in cold storage. This is especially so since licensed VA trading platforms are subject to a host of private key management and custody requirements under the VATP Guidelines which were designed to, amongst other things, reduce the risk of collusion amongst employees. However, as risks to client virtual assets held in hot and other storages (mainly hacking and other cybersecurity risks) are not typically associated with the custody of client assets in the traditional financial markets, we remain of the view that client virtual assets held in hot and other storages should be fully covered by the compensation arrangement of a licensed VA trading platform.

63. As client virtual assets will not be fully insured against loss, we find more comfort in knowing the bulk of client virtual assets are held in cold storage, which is generally safe from hacking and other cybersecurity risks. We are thus prepared to lower the coverage threshold to 50% for client virtual assets held in cold storage, on the basis that 98% of client virtual assets will be required to be held in cold storage. However, it may be preferrable for licensed VA trading platforms to hold less than 2% of client virtual assets in hot and other storages given that the platform operator would need to set aside its own funds if insurance coverage for hot and other storages is unavailable.

64. Regarding the types of assets that could form part of a compensation arrangement, we agree that bank guarantees, along with funds held in the form of demand deposits or fixed deposits with a maturity of six months or less would be acceptable. In terms of virtual assets, we see the benefits of holding reserve virtual assets that are the same as the client virtual assets required to be covered under the compensation arrangement, to reduce market risk given virtual assets' volatility.

65. We note the diverse views as to whether an escrow arrangement be put in place for the compensation arrangement or whether the licensed VA trading platform be allowed to hold the funds set aside. Both arrangements would be acceptable to us, provided that the funds set aside are segregated from the assets of the platform operator and its group companies, and are set aside on trust and designated for such purpose. Funds held by the platform operator or its associated entity should be held in a segregated account with an authorized financial institution. The VATP Guidelines have been revised accordingly.

66. We agree that licensed VA trading platforms should also have the flexibility to establish a pool of funds jointly or individually in the form of an insurer to cover the loss of their client assets. This flexibility has now been provided in the VATP Guidelines.

67. Finally, we also agree that virtual assets which form part of a compensation arrangement should be segregated from the virtual assets of the platform operator and its group companies and be held in cold storage by its associated entity. This is because the associated entity is subject to the host of private key management and custody requirements under the VATP Guidelines, while the custody standards of third-party custodians may vary greatly or could even be inadequate.

Question 6:

Do you have any suggestions for technical solutions which could effectively mitigate risks associated with the custody of client virtual assets, particularly in hot storage?

Public comments

68. Many respondents suggested that the SFC should allow third-party custodians to be engaged for the safekeeping of client virtual assets given their extensive technical expertise.

69. A number of respondents suggested that it should be mandatory for licensed VA trading platforms to provide publicly-accessible proof of reserves so that clients can verify the amount of virtual assets held in custody. Other respondents recommended that the SFC maintain a public register of wallet addresses of licensed VA trading platforms for a similar reason.

70. Many respondents further remarked that the latest custodial solutions, including multi-party computation, key sharding technology and other innovations, should be adopted for the storage of seeds and private keys. A few respondents took issue with the proposed requirement to keep all seeds and private keys in Hong Kong.

The SFC's response

71. We acknowledge that there may be third-party custodians with extensive technical expertise. However, there is currently no regulatory regime in Hong Kong for custodians of virtual assets. Given the importance of safe custody of client virtual assets, we would require a direct regulatory handle over the firm exercising control of client virtual assets (ie, a wholly-owned subsidiary of a licensed VA trading platform). This also forms the basis for requiring all seeds and private keys to be securely stored in Hong Kong. If the seeds and private keys are stored overseas, the corresponding client virtual assets would also be outside our jurisdiction. This would substantially hinder our supervision and enforcement.

72. We have noticed the increasing trend of VA trading platforms overseas providing proof of reserves or disclosing wallet addresses. Nonetheless, we are mindful that these disclosures mainly evidence a VA trading platform's assets, but not its liabilities, and disclosing the latter may require the involvement of external assessors (ie, an auditor).

73. We appreciate the views shared on technological advancements that may enhance the safe custody of client virtual assets. We are monitoring new custodial technologies such as multi-party computation and key sharding, and note the intense debate on these technologies in the cryptography industry. A requirement in the VATP Guidelines is that seeds and private keys (and their backups) should be stored securely with appropriate certification, for example, in an appropriately certified Hardware Security Module. We are open to allowing licensed VA trading platforms to adopt different custody solutions when the industry reaches a consensus on their security and appropriate certifications for the solutions emerge. The VATP Guidelines have retained such flexibility in its wording.

C. Trading in virtual asset derivatives

Question 7:

If licensed platform operators could provide trading services in VA derivatives, what type of business model would you propose to adopt? What type of VA derivatives would you propose to offer for trading? What types of investors would be targeted?

Public comments

74. Respondents expressed general support for allowing licensed VA trading platforms to provide trading services in virtual asset derivatives.

75. The proposed business model involved either an order-matching engine or over-the-counter trading where leverage is employed (eg, three times leverage) and with clients providing margin or premium (with client positions subject to automatic liquidation).

76. The type of virtual asset derivatives proposed included simple delivery futures, margined perpetual future contracts, options with settlement dates and other structured products. It was proposed that products could start with the major virtual assets acting as the underlying asset (eg, Bitcoin and Ether) with some suggesting products quoted and settled in stablecoins.

77. Most respondents suggested that virtual asset derivatives should be limited to professional investors. If retail investors were to gain access to virtual asset derivatives, extensive investor protection measures should be put in place (eg, confining eligible underlying assets to those meeting certain criteria).

The SFC's response

78. We are grateful for the detailed and informative responses submitted on this question. As we have explained in the consultation paper, the SFC is aware of the importance of virtual asset derivatives to institutional investors. We will take the large number of comments into consideration and conduct a separate review in due course.

D. Other adaptations to existing requirements

Question 8:

Do you have any comments on how to enhance the other requirements in the VATP Terms and Conditions when they are incorporated into the VATP Guidelines?

Public comments

79. Many comments were received in relation to the requirement that 98% of client virtual assets must be stored in cold storage and only 2% of client virtual assets could be stored in hot or other storages (cold to hot storage ratio). Many respondents requested the cold to hot storage ratio be lowered to more expediently deal with client withdrawal requests.

80. In response to the blanket ban on all types of proprietary trading by the licensed VA trading platform and its group companies, irrespective of where the proprietary trading took place, there were suggestions to allow proprietary trading, and in particular proprietary market making by the licensed VA trading platform's affiliates, to enhance the liquidity of the trading platform.

81. Some respondents noted the prohibition on platform operators providing algorithmic trading services to clients and asked whether a licensed VA trading platform's clients could use their own algorithmic trading systems.

82. Finally, respondents sought clarification of whether other virtual asset-related services such as earning, deposit-taking, lending and borrowing could be provided by licensed VA trading platforms.

The SFC's response

83. We maintain the view that to ensure the safe custody of client assets the cold to hot storage ratio should not be lowered and the bulk of client virtual assets should be held in cold storage, which is generally free from hacking and other cybersecurity risks. We would also like to remind platform operators that they should implement proper virtual asset withdrawal procedures and disclose these procedures to their clients. In particular, if a platform operator does not effect clients' withdrawal requests on a real time basis, it should specify the time generally required for transferring virtual assets to a client's private wallet after receiving a withdrawal request on its website.

84. With regard to proprietary trading, we agree that liquidity on a trading platform is important for clients. Hence, the SFC allows market making activities to be conducted by third-party market makers. However, the current prohibition on proprietary trading is all encompassing and effectively prohibits even the group companies of a licensed VA trading platform from having any positions in virtual assets. We have accordingly revised the requirements in the VATP Guidelines to allow trading by affiliates other than trading through the licensed VA trading platform.

85. In relation to algorithmic trading, the SFC would like to clarify that while platform operators are prohibited from providing algorithmic trading services to its clients, the platform's clients can use their own algorithmic trading systems in connection with trading via the licensed VA trading platform.

86. With respect to the provision of other services commonly seen in the virtual asset market such as earning, deposit-taking, lending and borrowing, the SFC does not allow licensed VA trading platforms to provide these services and this is covered by paragraph 7.26 of the VATP Guidelines. Ultimately, a licensed VA trading platform's primary business is to act as an agent and provide an avenue for the matching of orders between clients. Any other activities may lead to potential conflicts of interest and require additional safeguards. As such, licensed VA trading platforms will not be allowed to conduct these activities at this stage.

E. AML/CFT matters

Question 9:

Do you have any comments on the requirements for virtual asset transfers or any other requirements in Chapter 12 of the AML Guideline for LCs and SFC-licensed VASPs? Please explain your views.

87. The respondents generally welcomed the inclusion of virtual asset-specific AML/CFT requirements in Chapter 12 of the AML Guideline for LCs and SFC-licensed VASPs, which provides comprehensive guidance to assist the design and implementation of AML/CFT systems to mitigate the money laundering and terrorist financing (ML/TF) risks associated with virtual assets. The major comments received are discussed below.

(A) Virtual asset transfers

Implementation of the Travel Rule[8]

Public comments

88. While most respondents were supportive of or did not object to the implementation of the Travel Rule, some respondents suggested a transitional period ranging from 12 to 24 months given that the sunrise issue may make it difficult for licensed VA trading platforms to immediately comply. Those who supported the implementation of the Travel Rule with effect from 1 June 2023 commented that timely implementation is critical for Hong Kong's virtual asset businesses as any delay may drive international business partners away from our licensed VA trading platforms.

89. A few respondents expressed practical challenges to strict adherence to the Travel Rule. It takes time to develop systems and infrastructure for the exchange of the required information about originators and recipients between ordering and beneficiary institutions. One respondent suggested that, as an interim measure, licensed VA trading platforms should be given the flexibility to submit the required information manually and as soon as possible rather than "immediately" (ie, before or when the virtual asset transfer is conducted) when acting as the ordering institution.

90. Two respondents commented that the implementation of the Travel Rule may unintentionally force licensed VA trading platforms to conduct virtual asset transfers with unhosted wallets where the requirements appear to be less stringent and this may expose them to higher ML/TF risks.

The SFC's response

91. The Travel Rule is a key AML/CFT measure for virtual asset service providers (VASPs) and financial institutions as it provides fundamental information for carrying out sanctions screening and transaction monitoring, as well as other risk mitigating measures. It also helps to prevent the processing of virtual asset transfers for illicit actors and designated parties and detect such transfers when they occur.

92. The Financial Action Task Force (FATF) has reiterated the need for jurisdictions to implement the Travel Rule as soon as possible given the sunrise issue cannot be resolved until all VASPs and financial institutions operating in major jurisdictions comply with the Travel Rule.

[8] The Travel Rule refers to the requirements for virtual asset transfers to or from an institution set out in paragraphs 12.11.5 to 12.11.24 of the AML Guideline. Under the Travel Rule, licensed VA trading platforms are required to (i) when acting as the ordering institution, obtain, hold and submit required information about the originator and recipient to the beneficiary institution immediately and securely; and (ii) when acting as the beneficiary institution, obtain from the ordering institution and hold required information.

93. Other major jurisdictions (eg, the US, Singapore, the UK and Europe) have already implemented or will implement the Travel Rule soon[9]. Any delay in the implementation of the Travel Rule in Hong Kong would affect the competitiveness of the VA trading platforms licensed by us, as the VASPs and financial institutions operating in other major jurisdictions would be unable or unwilling to transact with them out of risk management concerns.

94. Nevertheless, it may take time to develop systems to facilitate the immediate submission of the required information to a beneficiary institution although licensed VA trading platforms have taken note of the FATF's advocacy of the Travel Rule over the past few years.

95. Considering that the active and rapid development of technological solutions and Travel Rule networks in recent years has gradually made it easier for institutions to exchange the required information, respondents' concerns about submitting information immediately will likely be resolved over time. In addition, more and more VASPs and financial institutions operating overseas will be subject to the Travel Rule.

96. Where the required information cannot be submitted to the beneficiary institution immediately, the SFC considers that submission as soon as practicable after the virtual asset transfer to be acceptable as an interim measure until 1 January 2024[10], having regard to the implementation status of the Travel Rule in other major jurisdictions. Licensed VA trading platforms should comply with all other Travel Rule and relevant requirements in paragraphs 12.11 to 12.13 with effect from 1 June 2023, including submitting the required information to the beneficiary institution securely, while adopting the said interim measure. Amendments have been made to paragraphs 12.11 to reflect this.

97. Some clients of licensed VA trading platforms may transfer virtual assets to or from unhosted wallets. This may pose higher ML/TF risks given there is typically no intermediary carrying out AML/CFT measures on the owners of unhosted wallets.

98. As such, we have set out requirements governing transfers to or from unhosted wallets in paragraphs 12.14. These requirements are similar to, if not more stringent than, the Travel Rule. Licensed VA trading platforms should obtain the required information from the customer and conduct sanctions screening. Further, licensed VA trading platforms should only accept transfers with unhosted wallets that are assessed to be reliable, having regard to the screening results of the virtual asset transactions and the associated wallet addresses, as well as the assessment results of the ownership or control of the unhosted wallet. Please also refer to the discussions in paragraphs 106 to 109 of this conclusions paper.

[9] While the US and Singapore have already implemented the Travel Rule, the Travel Rule will take effect in the UK on 1 September 2023; and it is expected that it will come into effect in Europe in January 2025.

[10] This means that paragraphs 12.11.10 and 12.11.13 will take effect on 1 January 2024. Licensed VA trading platforms should adopt the interim measure prior to 1 January 2024 where the required information cannot be submitted to the beneficiary institution immediately. An FAQ will be issued by the SFC to clarify our regulatory expectations in this regard.

VA transfer counterparty due diligence and additional measures

Public comments

99. While a few respondents were of the view that the requirements were too prescriptive or sought clarification of the extent of measures to be applied, two respondents commented that licensed VA trading platforms should conduct ongoing monitoring of VA transfer counterparties including screening of virtual asset transfers given risk exposures may change over time.

100. Some respondents sought clarification of which entity they should conduct due diligence on, in particular, when they conduct transfers with VASPs with group entities performing different functions or operating in different jurisdictions.

The SFC's response

101. The guidance on VA transfer counterparty due diligence and additional measures, including the factors that should be considered and the measures to be taken, are in line with FATF's standards and guidance. These measures should be applied using a risk-based approach, taking into account various factors such as the types of products and services offered by the VA transfer counterparty and the types of customers that it serves, as well as the AML/CFT regime in the jurisdiction that it operates.

102. In relation to the ongoing monitoring of VA transfer counterparties, this would include screening virtual asset transfers using a risk-based approach.

103. The due diligence measures should be applied to the entity which a licensed VA trading platform conducts virtual asset transfers with. Where virtual asset transfers are conducted with several VA transfer counterparties that belong to the same group, the licensed VA trading platform should take this into account while conducting due diligence on each of them independently to enable a more holistic view of the risks they pose. Corresponding amendments have been made to paragraphs 12.13 to reflect this.

Risk-based policies and procedures for handling incoming virtual asset transfers lacking the required information

Public comments

104. Several respondents raised concerns about returning virtual assets to the originator for virtual asset transfers lacking the required information which may contravene the Travel Rule and other requirements if the originator is found to be a sanctioned party, or if the transfer is associated with illicit sources.

The SFC's response

105. A licensed VA trading platform should only return virtual assets where appropriate and when there is no suspicion of ML/TF, taking into account the results of VA transfer counterparty due diligence as well as the screening of the virtual asset transactions and the associated wallet addresses. Further, returns should be made to the account of the ordering institution, rather than the originator's account. Additional guidance is provided in paragraph 12.11.22.

Virtual asset transfers to or from unhosted wallets

Public comments

106. Most respondents supported the requirements for virtual asset transfers to or from unhosted wallets. In particular, several respondents commented that the risk mitigating measures set out in paragraph 12.14.3 should be mandatory.

107. One respondent commented that a one-off confirmation of the ownership or control of an unhosted wallet may not be effective to ensure its ongoing reliability given that the anonymous transfer of ownership or control of an unhosted wallet is effortless. Another respondent suggested periodic confirmation of the ownership or control of unhosted wallets.

The SFC's response

108. It is mandatory for licensed VA trading platforms to take reasonable measures on a risk-sensitive basis to mitigate and manage the ML/TF risks associated with virtual asset transfers to or from an unhosted wallet, including the non-exhaustive risk-based measures set out in paragraph 12.14.3.

109. Obviously, the ownership or control of an unhosted wallet may change over time. Where a virtual asset transfer is conducted via an unhosted wallet which has been whitelisted, the licensed VA trading platform should ascertain the ownership or control of the unhosted wallet on a periodic and risk-sensitive basis, particularly when it becomes aware of any heightened ML/TF risks from the ongoing monitoring of the transactions conducted through the unhosted wallet, or additional customer information. Corresponding amendments have been made to paragraph 12.14.3.

(B) Other virtual asset-specific AML/CFT requirements

Occasional transactions

Public comments

110. Several respondents sought clarification of whether and how the thresholds for customer due diligence apply to licensed VA trading platforms before carrying out any occasional transaction.

The SFC's response

111. Licensed VA trading platforms should not carry out occasional transactions as they are required to establish a business relationship with all customers pursuant to the VATP Guidelines. Corresponding amendments have been made to paragraphs 12.3.

Cross-border correspondent relationships

Public comments

112. Two respondents sought clarification of the scope of application of cross-border correspondent relationships in the context of virtual assets, whether this covers virtual asset transfers and whether the screening of virtual asset transactions and the associated wallet addresses should be an ongoing monitoring requirement.

The SFC's response

113. The requirements for cross-border correspondent relationships apply to a licensed VA trading platform when it provides services in the course of providing a VA service as defined in section 53ZR of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) (AMLO) (ie, operating a VA exchange) to a VASP or financial institution located in a place outside Hong Kong which acts for its underlying customers. This includes instances where a licensed VA trading platform executes virtual asset trading transactions for these institutions but it does not include conducting virtual asset transfers with them.

114. A new paragraph 12.6.5 has been added to the AML Guideline for LCs and SFC-licensed VASPs to clarify that licensed VA trading platforms are required to conduct ongoing monitoring of virtual asset transactions and the associated wallet addresses.

Screening of virtual asset transactions and the associated wallet addresses

Public comments

115. Many respondents supported the requirements for screening virtual asset transactions and their associated wallet addresses. A few respondents sought clarification of the timing of the screening.

The SFC's response

116. Screening should be performed before conducting a virtual asset transfer, or before making the transferred virtual assets available to the customer; and after conducting a virtual asset transfer on a risk-sensitive basis. This would help licensed VA trading platforms identify the source and destination of the virtual assets, and any involvement or subsequent involvement of wallet addresses associated with illicit or suspicious activities or designated parties, in a more timely and accurate manner. A corresponding footnote has been incorporated to paragraph 12.7.3.

Others

117. In addition to the amendments discussed above, we also made other textual amendments to the consultative draft which aim to provide greater clarity without altering the substance of the requirements. The marked-up texts of the amendments to the AML Guidelines are set out in Appendices B and C and highlighted in grey. We will monitor the industry's implementation of these guidelines and, where necessary, engage with the industry to develop FAQs to help them understand their application.

(C) Non-virtual asset-specific AML/CFT requirements

118. As set out in paragraph 70 of the Consultation Paper, we have been working closely with fellow AMLO regulators to provide guidance in relation to other revised statutory AMLO provisions which will also take effect on 1 June 2023. In addition, we and our fellow AMLO regulators have taken the opportunity to make other non-substantive amendments to enhance clarity, provide facilitative or elaborative guidance and better align with existing statutory provisions.

119. We also conducted soft consultations with representatives from several industry associations to gauge feedback on the amendments. These amendments are applicable to both LCs[11] and licensed VA trading platforms, and are now incorporated in the final form of the AML Guideline for LCs and SFC-licensed VASPs, with marked-up texts highlighted in yellow.

F. Disciplinary Fining Guidelines

Question 10:

Do you have any comments on the Disciplinary Fining Guidelines? Please explain your views.

Public comments

120. Respondents generally supported the proposed Disciplinary Fining Guidelines. However, some respondents questioned why they are not the same as the guidelines in the existing regime under the SFO. A respondent commented that it is difficult to see why the same set of fining guidelines should not be applied to both AMLO-licensed VA trading platforms and SFO-licensed VA trading platforms, when the activities carried out by the two types of VA trading platforms are essentially the same and the only difference lies in the "securities" or "non-securities" nature of the tokens being traded.

121. One respondent noted that the SFC may impose a fine up to a maximum of HK$10 million or three times of the profit gained or loss avoided, and that the SFC will not automatically link the fine imposed with profit gained or loss avoided. It suggested that the SFC provide examples or circumstances of when the SFC will link the fine imposed with profit gained or loss avoided. Another respondent suggested that the SFC consider determining the fines based on other approaches, such as the total annual turnover of the VA trading platform.

122. Some respondents sought clarification of the considerations the SFC takes into account in determining whether a fine would be imposed and, if so, the amount of the fine. On the general considerations under the proposed Disciplinary Fining Guidelines and the specific consideration regarding the duration and frequency of the conduct, a respondent sought guidance on whether there will be a specific amount or numerical values for these considerations. Another respondent sought clarification of whether conduct that is widespread in unregulated entities would be a mitigating factor in assessing the conduct of a regulated person.

123. One respondent suggested that the SFC elaborate on the specific considerations listed in the proposed Disciplinary Fining Guidelines and consider including more factors, such as the positions of the individuals involved, the level of sophistication of the market participants affected by the conduct and the remedial actions taken by the persons involved.

[11] A circular would be issued by the SFC summarising these amendments in due course.

124. Some respondents sought guidance on how the SFC determines whether to take disciplinary action against a corporation, an individual or both, noting that there are significantly more enforcement actions against individuals than against corporations. They suggested that the SFC set out a list of factors that it may consider when determining this.

125. A respondent commented that the board and senior management of licensed corporations should take more responsibility to enhance the security and reliability of the information systems which provide virtual asset trading services to their customers, as these assets are more prone to cyberattacks due to their intrinsic nature. The respondent suggested that the SFC consider requiring licensed corporations to appoint a MIC for information technology and security to enhance governance in this regard.

126. A respondent sought guidance on the process for challenging the proposal to impose a fine, and the imposition of a fine.

The SFC's response

127. We agree that the same set of fining criteria should be applied to both SFO-licensed VA trading platforms and AMLO-licensed VA trading platforms. The SFC has issued the following fining guidelines which are applicable to SFO-licensed VA trading platforms:

(a) the SFC Disciplinary Fining Guidelines issued under section 199(1)(a) of the SFO, which set out the factors the SFC takes into account in exercising its power to impose a pecuniary penalty on a regulated person under section 194(2) or 196(2) of the SFO (SFO Fining Guidelines); and

(b) the SFC Disciplinary Fining Guidelines issued under section 23(1) of the AMLO, which set out the factors the SFC takes into account in exercising its power to impose a pecuniary penalty on a financial institution under sections 21(1) and 21(2)(c) of the AMLO (AMLO Fining Guidelines).

128. The proposed Disciplinary Fining Guidelines are based on both the SFO Fining Guidelines and the AMLO Fining Guidelines. SFO-licensed VA trading platforms and AMLO-licensed VA trading platforms will be subject to the same fining criteria irrespective of the ordinance under which they are licensed.

129. It is not our intention to automatically link the fine with the profit gained or loss avoided as this may not always reflect the severity of the misconduct. Instead, we will consider each case on its own merits, taking into account all relevant factors when determining the appropriate fine. As such, we do not consider it to be helpful to give examples of specific circumstances where the fine imposed will be linked with the profit gained or loss avoided.

130. Section 53ZSP(3) of the AMLO provides that the fine should not exceed HK$10 million or three times the profit gained or loss avoided by the regulated person, whichever is higher. Depending on the nature and character of the misconduct, it may consist of a number of culpable acts or culpable omissions which may attract multiple penalties. We note the suggestion to determine the fine with reference to the total annual turnover of the VA trading platform (as opposed to profit gained or loss avoided). While we consider the current statutory limit to be adequate, we will closely monitor its implementation and consider legislative changes if necessary.

131. The proposed Disciplinary Fining Guidelines already provide sufficient information regarding the factors we will consider in determining whether to impose a fine as well as the appropriate fine. As each case has to be considered on its own merits, we will not follow a rigid framework in applying a specific amount or numerical value to any of these factors. This will allow us to maintain the flexibility to respond to changes in market practices. We also do not consider the fact that the conduct in question is widespread in unregulated entities would be a mitigating factor. The fact that unregulated entities may also engage in similar conduct does not excuse or mitigate the gravity of a misconduct.

132. In determining the appropriate fine, we will take into account factors such as the positions of the individuals involved, the level of sophistication of the market participants affected by the conduct and the remedial actions taken by the persons involved. These factors are already reflected in the specific considerations listed in the proposed Disciplinary Fining Guidelines (under "the nature and seriousness of the conduct" and "other circumstances of the firm or individual").

133. With respect to the question of how the SFC decides in practice whether disciplinary action should be taken against individuals, corporations or both, we will consider all the circumstances including the conduct of the corporation and individual in question and, in relation to those involved in the management of a corporation, whether there is any consent, connivance or negligence on their part[12], any failure in supervision, or the management of business. By taking a holistic approach, we aim to ensure that all culpable parties are held accountable for their conduct. Whether we discipline a regulated person depends on the specific facts of each case. As such, we do not consider it to be helpful to provide a list of factors for determining whether to take disciplinary action against a corporation, an individual or both.

134. Paragraph 5.1(k) of the proposed VATP Guidelines already states that the "senior management of a Platform Operator should bear primary responsibility for ensuring the maintenance of appropriate standards of conduct and adherence to proper procedures by the Platform Operator". The senior management of a licensed VA trading platform generally includes, amongst other things, its directors, responsible officers and MICs. We understand the importance of added clarity as to the scope of each senior manager's duties and obligations. As mentioned above in relation to the token admission and review committee, we will issue further guidance in the form of FAQs on the augmentation of the accountability of senior management (including in respect of the information technology function of a licensed VA trading platform).

135. Under the AMLO, there are established procedures which ensure a regulated person is entitled to due process. Before exercising any power to discipline, the SFC must first give the regulated person a reasonable opportunity to be heard by allowing that person to make representations explaining the matter in question and commenting on the appropriateness of the proposed sanctions. If a regulated person feels aggrieved by a disciplinary decision, that person may apply to the Anti-Money Laundering and Counter-Terrorist Financing Review Tribunal for a review of the decision.

[12] See section 53ZSR(5) of the AMLO.

Part II: Key measures of the transitional arrangements and implementation details of the new regulatory regime

Responses to the key measures and implementation details

Public comments

Licence application-related matters

136. We received many requests for clarification in relation to a wide range of technical matters. For example, there were questions about the scope of "providing a virtual asset service" as defined in the AMLO, including whether it covered over-the-counter virtual asset trading activities and virtual asset brokerage activities.

137. Regarding the dual licences arrangement, respondents asked whether there was a need to obtain both SFO and AMLO licences, particularly as some platform operators may not intend to trade security tokens. Noting the possibility that a non-security token may evolve into a security token, respondents also commented that the platform operator could discontinue trading services in that particular security token or only allow clients to sell down their positions in that token such that an SFO licence may not be required. In connection with the dual licences arrangement, respondents also asked whether a dually-licensed VA trading platform would be required to maintain two or four responsible officers, and whether a pragmatic approach could be adopted in assessing competence, including the relevant industry experience of responsible officers, in light of the shortage of talent having both virtual asset and traditional securities experience.

138. In relation to the external assessment report (EAR) requirements, questions asked included whether a firm which has drafted the policies and procedures for a VA trading platform applicant and provided system implementation advice could act as an assessor in the Phase 1 Report and also in the Phase 2 Report; whether the Phase 1 Report need not be submitted together with the licence application, whether platform operators which intended to seek a licence could submit the capability statements of their external assessors of choice to the SFC prior to submitting the EAR and whether only a Phase 2 Report could be submitted for established and operating VA trading platforms.

Transitional arrangement-related matters

139. Respondents also submitted many requests for clarification ranging from eligibility for the deeming arrangement and compliance with the VATP Guidelines during the transitional period to general questions about the application process under the deeming arrangement and how the deeming arrangement would operate.

140. There were also questions about the removal of the licensing conditions in respect of the VATP Terms and Conditions and whether compliance with the VATP Guidelines would be imposed as a licensing condition instead.

Other matters

141. In light of the proposals to allow retail access, respondents also enquired whether revisions would be made to the regulatory requirements for intermediaries under the SFO when engaging in virtual asset-related activities, such as, the joint circular on

intermediaries' virtual asset-related activities issued jointly by the SFC and the HKMA[13]. Respondents also sought additional guidance related to security tokens (eg, on conducting security token offerings).

The SFC's response

Licence application related matters

142. Regarding the scope of "providing a virtual asset service", the AMLO regime will cover VA trading platforms which are centralised and operate in a manner similar to traditional automated trading venues licensed under the SFO. Such platforms typically provide virtual asset trading services to their clients using an automated trading engine which matches client orders and also provide custody services as an ancillary service to their trading services. Accordingly, the provision of virtual asset services without an automated trading engine and ancillary custody services (for instance, over-the-counter virtual asset trading activities and virtual asset brokerage activities) would not fall under the scope of the AMLO regime.

143. As we have explained in the consultation paper, given that the terms and features of a virtual asset may evolve over time, a virtual asset's classification may change from a non-security token to a security token (or vice versa). To avoid contravention of the licensing regimes and to ensure business continuity, it would be prudent for VA trading platforms to apply for approvals under both the existing SFO regime and the AMLO VASP regime. We note with concern the suggestion that rather than obtain an SFO licence, a VA trading platform could simply suspend and ultimately withdraw trading services in a particular token which evolved into a security token. Fundamentally, withdrawing a token previously admitted for trading may not be in the best interests of clients, and should be a measure of last resort. The proposition that clients only be allowed to sell down their positions is also misconstrued, as any sell down order by one client would be matched with a buy order of another client.

144. We will adopt a streamlined application process so that only a single consolidated application needs to be submitted for a dual licences application. With respect to responsible officers, one individual may be concurrently approved under both the SFO and the AMLO so it is not required that a dually-licensed VA trading platform maintain four different responsible officers. As there may be a lack of talent with both virtual asset and traditional securities experience, we are prepared to adopt a pragmatic approach, details of which will be supplemented by way of further guidance.

145. As mentioned in the consultation paper, the EAR requirements were proposed to streamline the application process, particularly as the industry may not fully understand our regulatory expectations. We expect that the external assessor could substantially assist an applicant, for example, by advising on or drafting the applicant's policies and procedures, by advising on system implementation and by suggesting enhancements or rectification measures in case deficiencies in the design, implementation or effectiveness of the policies, procedures, systems and

[13] Joint circular on intermediaries' virtual asset-related activities issued by the SFC and the HKMA on 28 January 2022 (https://apps.sfc.hk/edistributionWeb/api/circular/openFile?lang=EN&refNo=22EC10).

controls are noted. As such, it would be acceptable for an external assessor to be involved prior to and in both the Phase 1 and 2 Reports[14].

146. As an external assessor is expected to be involved in the early preparation stages of applying for a licence and as the Phase 1 Report requirement was introduced to streamline the application process, the Phase 1 Report should be submitted together with the licence application. Further, given that the industry may not yet fully understand our regulatory expectations, the submission of a Phase 1 Report for established and operating VA trading platform applicants would still be necessary. VA trading platforms which are uncertain about whether the external assessor they intend to engage is sufficiently qualified are encouraged to discuss with the Fintech unit of the SFC in advance.

147. In light of the wide-ranging questions received, we will be issuing further guidance in the form of circulars, FAQs and a licensing handbook for common questions relating to the new AMLO VASP regime.

Transitional arrangement-related matters

148. Many of the questions received about the transitional arrangements were quite fundamental in nature (eg, when would VA trading platforms be required to comply with the AMLO). Given the vast number of diverse questions, we will issue further information on the transitional arrangements in the form of a circular.

149. Regarding the VATP Terms and Conditions, as explained in the consultation paper, the VATP Guidelines will supersede the Terms and Conditions for VA trading platform operators and compliance with the VATP Guidelines will be imposed as a licensing condition. For existing SFO-licensed VA trading platforms, given the 12-month transitional period for compliance with the requirements in the VATP Guidelines, the SFC will not remove the corresponding licensing conditions on compliance with the Terms and Conditions for VA trading platform operators from their licences until the VA trading platform can fully comply with the VATP Guidelines or by the deadline of the 12-month transitional period, whichever is earlier.

Other matters

150. We are mindful of the need to maintain coherence and consistency between the different virtual asset-related regulatory frameworks administered by the SFC (eg, ensuring consistent requirements for retail access to virtual assets under the joint circular). We will revise the joint circular to set out the regulatory requirements applicable to intermediaries engaging in virtual asset-related activities. In relation to security tokens, we will issue additional guidance in due course.

[14] The scope of external assessment report (which was also appended to the consultation paper) and, where appropriate, further guidance will be made available on the SFC website at www.sfc.hk..

Implementation timetable

151. In light of the public's general support, the SFC will implement the VATP Guidelines and the AML Guidelines with some modifications and clarifications as set out and discussed in this conclusions paper. Marked-up versions of the amendments to the VATP Guidelines, the AML Guideline for LCs and SFC-licensed VASPs and the AML Guideline for AEs are set out in Appendices A, B and C to this conclusions paper. The SFC will also implement the Disciplinary Fining Guidelines as set out in Appendix D to this conclusions paper.

152. We will proceed to publish the guidelines in the Gazette and they will become effective on 1 June 2023.

153. The SFC will publish further guidance so that the industry can better understand the implementation of the new regulatory regime.

154. Once again, the SFC would like to take this opportunity to thank all the respondents for their submissions.

SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

Guidelines for Virtual Asset Trading Platform Operators

June 2023

Table of Contents

I. Interpretation and Application

Interpretation

1.1 ~~A reference in these Guidelines to:~~Definitions

- "*Associated Entity*" means a company which (i) has notified the Securities and Futures Commission (SFC) that it has become an "associated entity" of ~~the~~ a ~~licensee~~ Platform Operator under section 165 of the Securities and Futures Ordinance (Cap. 571) (SFO) and/or section 53ZRW of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) (AMLO); (ii) is incorporated in Hong Kong; (iii) holds a "trust or company service provider licence" under the AMLO; and (iv) is a wholly owned subsidiary of the Platform Operator.~~;~~

- "*C~~c~~lient*" means a person to whom the Platform Operator provides services in the course of carrying out the Relevant Activities.~~;~~

- "*C~~c~~lient asset*" means client virtual assets and client money.~~;~~

- "*C~~c~~lient money*" means any money:

  (a) received or held by or on behalf of the Platform Operator; or

  (b) received or held by or on behalf of the Associated Entity,

  which is so received or held on behalf of a client or in which a client has a legal or equitable interest, and includes any accretions thereto whether as capital or income~~;~~.

- "*C~~c~~lient virtual asset*" means any virtual asset:

  (a) received or held by or on behalf of the Platform Operator~~;~~ or

  (b) received or held by or on behalf of the Associated Entity,

  which is so received or held on behalf of a client or in which a client has a legal or equitable interest, and includes any rights thereto~~;~~.

- "*Financial Resources Rules*" means the Securities and Futures (Financial Resources) Rules (Cap. 571N)~~;~~.

- "*Group of companies*" has the meaning as defined in section 1 of Part 1 of Schedule 1 to the SFO and/or section 53ZRJ of the AMLO.

- "*I~~i~~nstitutional professional investor"* has the meaning specified in Schedule 1 to these Guidelines~~;~~.

- "*L~~l~~icensed person*" means a Platform Operator or a licensed representative~~;~~.

- "*L~~l~~icensed representative*" or *"LR"* means an individual who is granted a licence under section 120 of the SFO (SFO-LR) and/or section 53ZRL of the AMLO ~~(AMLO-LR)~~, and is accredited to a Platform Operator~~;~~.

- "*Mmonthly accounting period*" means:

  (a) in relation to the first statement of account required to be prepared and provided to a client of a Platform Operator, a period not exceeding one month ending on a date selected by the Platform Operator; and

  (b) in relation to any subsequent statement of account, a period the duration of which shall be not less than four4 weeks and not exceed one month, commencing on the day after the date on which the previous monthly accounting period ended, and ending on a date selected by the Platform Operator;.

- "*Platform Operator*" means:

  (a) a corporation which is granted a licence for Type 1 (dealing in securities) and Type 7 (providing automated trading services) regulated activities under section 116 of the SFO and carries out any Relevant Activities (SFO-licensed Platform Operator); and/or

  (b) a corporation which is granted a licence for providing a VA service under section 53ZRK of the AMLO and carries out any Relevant Activities (AMLO-licensed Platform Operator).

  Note: A reference in these Guidelines to "Platform Operator" shall, except where the context otherwise requires, include licensed representatives accredited to the Platform Operator.

- "*Pprofessional investor*" has the meaning as defined in section 1 of Part 1 of Schedule 1 to the SFO;.

- *"Qqualified corporate professional investor"* has the meaning specified in Schedule 1 to these Guidelines;.

- "*Rresponsible officer*" or *"RO"* means a licensed representative who is approved as a responsible officer of a Platform Operator under section 126 of the SFO (SFO-RO) and/or section 53ZRP of the AMLO (AMLO-RO);.

- "*Rretail client*" or "*retail investor*" means any person other than a professional investordoes not include any person who is a professional investor;.

- "*Relevant Activities*" means:

  (a) providing services through means of electronic facilities:

    (i) whereby:

      (A) offers to sell or purchase virtual assets are regularly made or accepted in a way that forms or results in a binding transaction; or

      (B) persons are regularly introduced, or identified to other persons in order that they may negotiate or conclude, or with the

reasonable expectation that they will negotiate or conclude sales or purchases of virtual assets in a way that forms or results in a binding transaction; and

(ii) where client money or client virtual assets comes into direct or indirect possession of the person~~s~~ providing such service; and

(b) any off-platform virtual asset trading activities and incidental services provided by the Platform Operator to its clients, and any activities conducted in relation to off-platform virtual asset trading activities~~;~~.

- "*S~~s~~ecurity token*" means a cryptographically secured digital representation of value which constitutes "securities" as defined in section 1 of Part 1 of Schedule 1 to the SFO~~;~~.

- "*Senior management*" means person(s) involved in the management of the business of the Platform Operator~~;~~.

- "*V~~v~~irtual asset*" or *"VA"* *or "token"* means:

(a) any "virtual asset" as defined in section 53ZRA of the AMLO; and

(b) any security token.

Note: These Guidelines are published under section 399 of the SFO and section 53ZTK of the AMLO. Unless otherwise defined above or the context otherwise requires, terms used in these Guidelines bear the same meaning as defined in the SFO and the AMLO.

~~1.2 A reference in these Guidelines to "Platform Operator" shall, except where the context otherwise requires, include licensed representatives of the Platform Operator.~~

Application

1.~~3~~2 These Guidelines are applicable to all Platform Operators (whether they are licensed under the SFO and/or the AMLO) when they carry on Relevant Activities.

1.~~4~~3 Parts II and III of these Guidelines are also applicable to the following persons:

(a) a corporation which applies for a licence to become a Platform Operator;

(b) an individual who applies for a licence to become an LR; and

(c) an individual who applies for approval to become an RO.

1.~~5~~4 The SFC recognises that some aspects of compliance with these Guidelines may not be within the control of a licensed representative. In considering the conduct of representatives under these Guidelines, the SFC will consider their levels of responsibility within the firm, any supervisory duties they may perform, and the levels of control or knowledge they may have concerning any failure by their firms or persons under their supervision to follow these Guidelines.

~~1.6 These Guidelines are published under section 399 of the SFO and section 53ZTK of the AMLO. Unless otherwise defined above or the context otherwise requires, terms used in these Guidelines bear the same meaning as defined in the SFO and the AMLO.~~

1.~~7~~5 A Platform Operator licensed under both the SFO and the AMLO is expected to comply with the requirements under the SFO and its subsidiary legislation, the AMLO and the codes, guidelines (including these Guidelines), circulars and frequently asked questions (FAQs) published by the SFC from time to time. Where there are any inconsistencies ~~between~~ amongst (i) the requirements under the SFO and its subsidiary legislation, the AMLO~~,~~ and the codes ~~and~~, guidelines, circulars and FAQs published by the SFC from time to time; and (ii) the requirements under these Guidelines, the more stringent requirement should prevail.

1.6 If any obligations of the Platform Operator under these Guidelines, the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset Service Providers) and any other applicable regulatory requirements can only be performed together with the Associated Entity or solely by the Associated Entity on behalf of the Platform Operator, the Platform Operator should ensure that its Associated Entity observes such obligations.

1.7 The Platform Operator is primarily responsible for compliance with these Guidelines, the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset Service Providers) and other regulatory requirements applicable to the Platform Operator.

1.8 A failure by any person to comply with any provision of these Guidelines:

(a) shall not by itself render that person liable to any judicial or other proceedings, but in any proceedings under the SFO and/or the AMLO before any court these Guidelines shall be admissible in evidence, and if any provision set out in these Guidelines appears to the court to be relevant to any question arising in the proceedings it shall be taken into account in determining the question; and

(b) the SFC shall consider whether such failure tends to reflect adversely on the person's fitness and properness.

II. Fitness and Properness Requirements

2.1 Persons applying to become a licensed person must satisfy the SFC that they are fit and proper to be ~~so~~ licensed~~,~~ and, upon being licensed, ~~such persons~~they must continue to be fit and proper. When assessing a person's fitness and properness, the SFC shall have regard to the matters below which are set out ~~under~~ with reference to section 129(1) of the SFO and section 53ZRJ(1) of the AMLO (as further elaborated in paragraphs 2.5 to 2.8 below), whether taking place in Hong Kong or elsewhere:

(a) f~~F~~inancial status or solvency;

(b) e~~E~~ducational or other qualifications or experience;

(c) a~~A~~bility to carry on the Relevant Activities competently, honestly and fairly; and

(d) r~~R~~eputation, character, reliability and financial integrity.

Note 1: According to section 53ZRJ(1) of the AMLO, the SFC shall also have regard to the matters below:

(i) conviction of an offence under the AMLO, the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575), the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) or the Organized and Serious Crimes Ordinance (Cap. 455);

(ii) conviction in a place outside Hong Kong for an offence in respect of an act that would have constituted an offence specified in paragraph (i) above had it been done in Hong Kong, for an offence relating to money laundering or terrorist financing or for an offence for which it was necessary to find that the person had acted fraudulently, corruptly or dishonestly; and

(iii) failure to comply with a requirement imposed under the AMLO.

Note ~~1~~2: Where the person is a corporation, those matters must be considered in respect of the corporation and any of its officers.

Note ~~2~~3: Where the "recency" of a matter of concern is mentioned in those matters, it is normally taken to mean within the last five years for all persons.

2.2 The SFC may also take into consideration the matters under section 129(2) of the SFO and/or section 53ZRJ(2) of the AMLO in considering whether a person is fit and proper.

2.3 The SFC is obliged to refuse a licence application if a licence applicant fails to satisfy the SFC that it is fit and proper to be licensed. The onus is on the applicant to make out a case that ~~he~~the applicant is fit and proper to be licensed.

2.4 Notwithstanding that a person fails to comply with all the individual elements set out in ~~this~~ Part II of these Guidelines, the SFC may nonetheless be satisfied that the

person is fit and proper. The SFC will look to the substance of the requirements and the materiality of any failure to meet them. Persons who are unsure whether they meet the substance of any criteria or believe that failure to meet any requirements may not be material to their ~~own~~ case are encouraged to discuss their concerns with the SFC before submitting an application.

Financial status or solvency

2.5 The SFC is not likely to be satisfied that a person is fit and proper if that person:

(a) ~~i~~In the case of an individual,

(i) is an undischarged bankrupt, is currently subject to bankruptcy proceedings or is a bankrupt who has recently been discharged;

Note: In considering whether to license a bankrupt who has been discharged, the SFC would have regard to the circumstances ~~of the discharge~~ and ~~the~~ recency of the discharge.

(ii) is subject to receivership or other similar proceedings; or

(iii) has failed to meet any judgment debt~~.~~; and

Note: The SFC would have regard to the circumstances of the failure to meet a judgment debt and the recency of the failure.

(b) ~~i~~In the case of a corporation,

(i) is subject to receivership, administration, liquidation or other similar proceedings;

(ii) has failed to meet any judgment debt; or

Note: These ~~are~~ requirements aim~~ed at~~ to identify~~ing~~ corporations of dubious financial status or solvency. As with ~~the same requirements in respect of~~ individuals, the SFC would have regard to the circumstances of the failure to meet a judgment debt and the recency of the act.

(iii) is unable to meet any financial or capital requirements applicable to it.

Educational or other qualifications or experience

2.6 In considering a person's ~~the~~ educational or other qualifications or experience, the SFC will take into account the nature of the functions which the person will perform. A person is unlikely to meet the fit and proper requirement if that person~~:~~ ~~(a) In~~ in the case of an individual, (~~i~~a) applying for a licence to become a licensed representative is under 18 years of age; or (~~ii~~b) has failed to demonstrate that he or she is competent to carry out the Relevant Activities efficiently and effectively.

Note 1: The general expectations are set out in Part III (Competence requirements) below.

Note 2: Competence is assessed with reference to the person's academic and industry qualifications together with relevant experience. Persons should be equipped with the skills, knowledge and professionalism necessary to perform their duties. The level of knowledge expected varies according to the level of responsibility and the type of function to be carried out in relation to the Relevant Activities ~~to be carried out~~. Persons are generally expected to be able to display an understanding of:

(a) the general structure of the regulatory framework ~~that~~ which applies to their proposed activities;

(b) the particular legislative provisions, codes and guidelines ~~that~~ which apply to the functions ~~that~~ they would perform;

(c) the fiduciary obligations owed to clients and the general obligations owed to their principals or employers; and

(d) virtual assets and the virtual asset market.

Ability to carry on the Relevant Activities competently, honestly and fairly

2.7 A person has to demonstrate the ability to carry on the Relevant Activities competently, honestly and fairly; and in compliance with all relevant laws, codes and guidelines promulgated by the SFC. The SFC is not likely to be satisfied that a person is fit and proper if that person:

(a) i~~I~~n the case of an individual,

(i) has been a patient as defined in section 2 of the Mental Health Ordinance (Cap. 136) to the extent that, in the opinion of the SFC~~,~~ after ~~having taken~~ taking into account ~~such~~ relevant factors including ~~that of~~ the person's past training, experience and qualifications, ~~that~~ the person would be unable to carry out the inherent requirements of the Relevant Activities; or

(ii) has evidenced incompetence, negligence or mismanagement, which may be indicated by the person having been disciplined by a professional, trade or regulatory body; or dismissed or requested to resign from any position or office for negligence, incompetence or mismanagement~~.~~; and

Note: Competence and efficiency are key elements to being fit and proper. However, the weight given to events of the types listed above in considering whether a person is fit and proper will depend on a number of factors, such as the time since the event, the seriousness of the event~~,~~ and the responsibility to be undertaken. The source and quality of evidence will also be taken into account.

(b) i~~I~~n the case of a corporation,

(i) has non-executive directors, key personnel (such as managers, officers, directors and chief executives), substantial shareholders, ultimate

owners or other controllers who fail to meet the requirements in ~~this~~ Part II of these Guidelines other than ~~that~~ the requirement regarding~~on~~ competence to carry on the Relevant Activities (unless such requirements are otherwise applicable); or

Note: In the SFC's view~~s~~, all persons involved in the management or control of the Platform Operator must be honest and fair.

(ii) has failed to demonstrate that it is competent to carry on the Relevant Activities efficiently and effectively.

Note: The general expectations ~~on~~ for competence are set out in Part III (Competence Requirements) below. The competence of a person is generally assessed with reference to its organisational structure and personnel. Reference should be made to paragraphs 3.4 to 3.7 below. The SFC is unlikely to be satisfied that ~~the~~ a person is competent if:

- its organisational structure and personnel are unable to comply with the relevant legislative or regulatory requirements; or
- it lacks the infrastructure and internal control systems to manage risks effectively, avoid conflicts of interest and maintain a proper audit trail.

Reputation, character, reliability and financial integrity

2.8 The SFC is not likely to be satisfied that a person is fit and proper if that person:

(a) ~~i~~In the case of an individual,

(i) was found to be of poor reputation, character or reliability, lacking in financial integrity, or dishonest. The weight given to events of the types listed below will depend on a number of factors, such as the time since the event, the seriousness of the event, and the level of responsibilities to be undertaken. Instances which, if remain~~ing~~ unexplained, might result in the person being regarded as having failed to meet this test are where the person has been:

(I) found by a court or other competent authority ~~for~~ to be involved in or liable for fraud, dishonesty or misfeasance;

(II) convicted of a criminal offence or is the subject of unresolved criminal charges which are of direct relevance to fitness and properness;

(III) censured, disciplined or disqualified by any professional or regulatory body in relation to any trade, business or profession;

(IV) refused or restricted from the right to carry on any trade, business or profession for which a specific licence, registration or other authorisation is required by law;

(V) disqualified by a court of competent jurisdiction from being a director;

(VI) found culpable of market misconduct by the Market Misconduct Tribunal, or unable to abide by any codes and guidelines promulgated by the SFC, other regulators or any relevant exchanges in Hong Kong or overseas (if applicable); or

(VII) a director, substantial shareholder, ultimate owner, or involved in the management, of a corporation or business ~~that~~which:

- was wound up (otherwise than by a solvent members' voluntary dissolution) or was otherwise insolvent or had a receiver or administrator appointed, however described;
- was found guilty of fraud;
- has not met all its obligations to clients, compensation funds established for the protection of investors~~,~~ or inter-~~-~~member guarantee funds; or
- has been found to have committed the acts described in subparagraphs (I), (II), (III), (IV) or (VI) above~~.~~; or

Note 1: The extent of the person's involvement in the relevant events, and the person's behaviour at that time, will have a substantial impact on the weight ~~that~~ the SFC attaches to the events in considering the person's fitness and properness.

Note 2: The SFC is also unlikely to be satisfied that a person is fit and proper if a person has failed to comply with a requirement imposed under the AMLO[1].

(ii) has been a party to a scheme of arrangement or entered into any form of compromise with a creditor involving a considerable amount; and~~.~~

Note: Where the amount involved is in excess of HK$ 100,000 or equivalent, the SFC would have regard to the recency of, and the circumstances leading to, the event.

(b) i~~I~~n the case of a corporation,

(i) was found to be of poor reputation or reliability, or lacking in financial integrity. Similar considerations will be given to the events described in paragraphs 2.8(a)(i) (except for subparagraph (V)) and 2.8(a)(ii) above; or

(ii) has been served with a winding up petition.

[1] See section 53ZRJ(1)(g) of AMLO.

III. Competence Requirements

3.1 The competence requirements stem from the fitness and properness requirements~~,~~. ~~whereby i~~Individuals and corporations will generally not be considered fit and proper unless they can demonstrate that they have the ability to carry on the Relevant Activities competently. The objective is to ensure a person, in carrying on any Relevant Activities, is equipped with the necessary technical skills and professional expertise to be "fit"~~,~~ and is aware of the relevant ethical standards and regulatory knowledge to be "proper" ~~in carrying on any Relevant Activities~~.

3.2 ~~This~~ Part III of these Guidelines sets out the non-exhaustive matters ~~that~~ the SFC will normally consider in assessing whether a person is competent to carry on any Relevant Activities. Failure to follow these Guidelines may reflect adversely on the fitness and properness of a person to carry on any Relevant Activities.

3.3 The key elements for the competence requirements ~~of~~ for corporations and individuals set out in ~~this~~ Part III of these Guidelines are high-level. The SFC is ~~cognisant of the fact~~aware that the application of these elements ~~would~~ may be different, ~~taking into account~~depending on a corporation's business model, the complexity of its business lines and an individual's particular circumstances, amongst other factors. The SFC will administer the competence requirements in a pragmatic manner.

Requirements for corporations

3.4 In determining whether a corporation is competent to carry on any Relevant Activities, the SFC will consider various key elements including its business, corporate governance, internal controls, operational review, risk management and compliance as well as the combined competence of its senior management and other staff members.

3.5 A corporation applying to carry on Relevant Activities should have a clear business model, detailing its modus operandi and target clientele. It should also have written policies and procedures to ensure continuous compliance with the relevant legal and regulatory requirements.

3.6 The SFC ~~highlights~~ emphasises that corporations must remain competent and ensure that the individuals they engage remain competent, including compliance with the continuous professional training (CPT) requirements. They must also keep the SFC informed of any material changes in their business plans, organisational structures and personnel.

3.7 The following non-exhaustive examples illustrate key elements ~~that~~ the SFC will consider for assessing the competence of a corporation:

(a) Business

(i) Information about the proposed business lines

(ii) Information about its target clientele, products and services

(iii) Information about its remuneration model and basis of calculation

(iv) Description of its modes of operation such as the extent of system automation and outsourcing arrangements

(v) Analysis of risks inherent to the key business lines, such as market risk, credit risk, liquidity risk and operational risk

(b) Corporate governance

(i) The presence of a shareholding structure clearly setting out its chain of ownership and voting power[2] such that all substantial shareholders[3], ~~and/or~~all ultimate owners[4] or both can be properly identified

(ii) The presence of an organisational structure clearly setting out the management structure of the corporation, including the roles, responsibilities, accountability and reporting lines of its senior management personnel

(iii) Policies and procedures for establishing, documenting and maintaining an effective management and organisational structure

(iv) The board of directors and senior management, including committees of the board, are composed of individuals with an appropriate range of skills and experience to understand and run the corporation's proposed activities

(v) The board of directors and senior management, including committees of the board, are organised in a way ~~that~~ which enables the board to address and control the activities of the corporation

(vi) Systems and controls to supervise those who act under the authority delegated by the board of directors

(c) Staff competencies

(i) Policies and procedures to ensure that positions are taken by suitably qualified staff including, but not limited to, all ROs, LRs, Managers-In-Charge (MICs)[5] and other supervisory staff

(ii) All supervisory staff for both front and back offices should have not less than three years of relevant experience and appropriate qualifications

(iii) Arrangements to ensure that operational and control policies and procedures are communicated to new recruits

---

2 For a corporation ~~that has~~with a complex ownership or control structure (~~eg~~for example, structures involving multiple layers, cross-holdings, trusts or~~,~~ nominee arrangements) without an obvious commercial purpose, the SFC may obtain further information to understand whether there is a legitimate reason for the particular structure.

3 As defined in section 6 of Part 1 of Schedule 1 to the SFO.

4 As defined in section 53ZR of the AMLO.

5 MICs refer to individuals appointed by a Platform Operator to be principally responsible, either alone or with others, for managing any of the core functions of the Platform Operator. A Platform Operator should ensure that any person it employs or appoints to conduct business is fit and proper and qualified to act in the capacity so employed or appointed.

(iv) Arrangements to ensure that updated operational and control manuals are distributed to staff and are accessible at all times

(v) Arrangements to ensure that any changes to operational and control policies and procedures are communicated to staff

(vi) Policies and procedures to ensure staff competencies including compliance with the CPT requirements

(d) Internal controls

(i) Adequate internal control systems set up in accordance with the relevant codes and guidelines published by the SFC

(ii) Arrangements to ensure that proper audit trails are maintained

(iii) Requirements for the proper documentation of all operational and control procedures[6]

(iv) Reporting systems ensuring that robust information is produced for risk management and decision-making purposes

(v) Appropriate control procedures to ensure data integrity and that data flowing into the risk management system should be consistent with trade and financial information

(vi) Appointment of a qualified information technology manager who is appropriately experienced to maintain the integrity of the corporation's operating systems

(e) Operational review[7]

(i) The presence of a function for reviewing the adherence to, and the adequacy and effectiveness of, the corporation’s internal control systems

(ii) Operational review personnel have appropriate qualifications and working experience to understand the corporation’s activities and risk profile

(iii) Operational review personnel are independent of core business functions and report directly to an independent, high-level authority

(iv) Operational review function to perform periodic (at least annual) risk assessment and ascribe various levels of risk to an appropriate review cycle

---

6 Proper documentation of all operational and control procedures is essential for providing staff with the necessary guidance in running the business in accordance with the corporation’s business objectives, professional standards and regulatory requirements.

7 The review function may not necessarily be performed by internal auditors.

(v) All review findings and issues that are not resolved within established time frames must be reported to senior management

(f) Risk management

(i) Policies and procedures with reference to the proposed business lines including:

(I) the setting of proper exposure limits for each key business line

(II) the manner in which risk exposure limits are set and communicated to the responsible persons

(III) the manner in which risks are being measured and monitored

(IV) the procedures to deal with exceptions to risk limits

(ii) Anticipated risks and ~~outgoings~~ outlays being supported by sufficient capital available to the corporation (typically demonstrated by a projection of excess liquid capital computed according to Part VI (Financial Soundness) below)

(iii) The timing of reviews of established policies (for example, subject to regular review, or with respect to changes in business and markets)

(iv) Appointment of an independent risk manager[8] ~~or an MIC of risk management function~~ who has the appropriate qualifications and authority to oversee and monitor the corporation's risk exposures and systems ~~of the corporation~~

(v) Processes to ensure that the corporation regularly carries out stress testing using appropriate measures

(g) Compliance

(i) Policies and procedures to ensure its compliance with all applicable legal and regulatory requirements as well as with its own internal policies and procedures

(ii) Policies and procedures to ensure that information submitted to the SFC is complete and accurate

(iii) Policies and procedures to deal with non-compliance

[8] The SFC expects there to be ~~will not insist that an independent risk manager be appointed if there are alternative arrangements in place which are sufficient to manage business risk exposures and exercise effective control over operations. This is irrespective of whether the alternative arrangement is undertaken in Hong Kong or elsewhere, at the company level or group level. In any case, there should be~~ clear segregation of duties; the responsibilities of the risk manager should be clearly separated from that of front office personnel. ~~Clearly~~ and, in most circumstances, more than one person will need to be appointed. The SFC will only permit alternative arrangements to the appointment of an independent risk manager in limited circumstances if the arrangements are sufficient to manage business risk exposures and enable effective control to be exercised over operations.

(iv) Adequate internal control systems to ensure its compliance with Part VI (Financial Soundness) below, and for it to commence and maintain its business operations

(v) Policies and procedures ~~on~~ for "Chinese Walls" including a "Wall Crossing Procedure" and other control procedures to address conflicts of interest arising from or in relation to carrying on the Relevant Activities in the corporation or its group of companies

(vi) Adequate internal control systems to address other conflicts of interest such as employee dealing and client priority

(vii) Policies and procedures to ensure that the corporation's business activities conducted in a jurisdiction outside Hong Kong, if any, fully comply with the relevant legal and regulatory requirements of that other jurisdiction, including activities performed by any individuals acting for and on behalf of it in such a jurisdiction

(viii) Policies and procedures to ensure any branch office in Hong Kong or elsewhere has an appropriate risk management and control strategy to comply with the relevant legal and regulatory requirements as well as internal policies and procedures

Requirements for individuals

3.8 An individual applying to carry on the Relevant Activities has to demonstrate competence and satisfy the SFC that he or she:

(a) has the necessary academic, professional or industry qualifications;

~~(b) is knowledgeable about virtual assets and the virtual asset market;~~

~~(c)~~(b) has sufficient relevant industry and management experience (where applicable);

~~(d)~~(c) has a good understanding of the regulatory framework, including the laws, regulations and associated codes governing the virtual asset sector; and

~~(e)~~(d) is familiar with the ethical standards expected of a financial practitioner[9].

Recognised industry qualification (RIQ) and local regulatory framework paper (LRP)

3.9 Individuals are expected to obtain the RIQs (Hong Kong Securities and Investment Institute (HKSI) administered Licensing Examination for Securities and Futures Intermediaries (LE) Papers 7 ~~&~~ and 8) and pass the LRPs (HKSI LE Paper 1 for LR, HKSI LE Papers 1 ~~&~~ and 2 for RO) ~~within~~ not more than three years prior to the submission of the application.

3.10 However, the SFC may recognise RIQs gained more than three years ago if the individual has substantial relevant working experience and has remained in the

[9] For example, *Ethics in Practice – A Practical Guide for Financial Practitioners* first published jointly by the SFC, the Independent Commission Against Corruption and other organisations in October 1999.

industry or can prove a recent licence or registration with a relevant regulator either in Hong Kong or elsewhere. The SFC may also recognise LRPs gained more than three years ago if the individual is or has been an LR or RO within the past three years for a regulated activity[10] in which ~~such~~ the LRPs are relevant.

3.11 Without compromising investor protection, the SFC may, at its sole discretion, consider granting an individual an exemption from obtaining an RIQ, passing an LRP or both if the individual can demonstrate that he or she possesses comparable qualifications. Criteria under which exemptions may be considered are detailed below in paragraphs 3.24 to 3.38.

Note: For the avoidance of doubt, the exemptions from the RIQ and LRP requirements in paragraphs 3.24 to 3.~~2~~38 below will also apply to (i) an individual who was previously given consent to act as an executive officer of a registered institution under section 71C of the Banking Ordinance (Cap. 155) as if ~~he~~ the individual ~~was~~ were an RO, and (ii) a relevant individual whose name was entered in the register maintained by the Hong Kong Monetary Authority under section 20 of the Banking Ordinance as if ~~he~~ the individual ~~was~~ were an LR.

Industry experience

3.12 Relevant industry experience generally refers to hands-on working experience acquired through the carrying on of the Relevant Activities in Hong Kong or similar activities regulated elsewhere. The SFC may also accept experience gained in a non-regulated situation, for example, where the experience is relevant to the carrying on of the Relevant Activities but the related activities are exempted from the licensing or registration requirements in Hong Kong or elsewhere.

3.13 In assessing the "relevance" of an individual's experience, the SFC will consider whether the substance of the experience is directly relevant or crucial to the Relevant Activities proposed to be carried on by the individual and the role that the individual will undertake (see also paragraph 3.18 below).

3.14 In assessing whether an individual has acquired "sufficient" relevant industry experience, the SFC may consider the individual's overall career history accumulated within the industry in totality. However, the SFC will critically review the experience of an individual who, for example:

(a) claims industry experience with any firm or virtual asset trading platform which has been largely or completely dormant for a prolonged period; or

(b) shows a pattern of being accredited to his or her previous principals only for a short period.

These kinds of situations may cast doubt as to whether the individual has in fact carried on Relevant Activities for his or her principal, and such industry experience purportedly gained by him or her will less likely fulfil the competence requirements.

[10] As specified under Part 1 of Schedule 5 to the SFO.

3.15 The SFC will consider all relevant factors in assessing each individual's application on a case-by-case basis, taking into account his or her principal's business model, governance structure and internal control systems as well as the competence of all its key personnel.

Responsible officers

3.16 In assessing the competence of an individual applying to be an RO (whether under the SFO, the AMLO or both), the SFC will need to be satisfied that he or she possesses the appropriate ability, skills, knowledge and experience to properly manage and supervise the corporation's proposed activities. For an individual applying to be an RO (whether under the SFO, the AMLO or both), a summary of the options for satisfying the competence requirements is set out below:

	Option A	Option B	Option C	
Academic or professional qualifications	Degree[11] in the designated fields[12]; other degree[11] (with passes in at least two courses in the designated fields[12]); or professional qualifications[13]	Other degree (without passes in two courses in the designated fields[12])	Attained Level 2 in either English or Chinese as well as in Mathematics in the HKDSE or equivalent[14]	
Relevant industry experience	At least 3 years over the past 6 years	At least 3 years over the past 6 years	At least 3 years over the past 6 years	At least 5 years over the past 8 years

[11] If an applicant who is a degree holder has attained a post-graduate diploma or certificate which is (a) issued by a university or other similar tertiary institution in Hong Kong or elsewhere; or (b) recognised as Level 6 or above under the Qualifications Framework in Hong Kong, then the post-graduate diploma or certificate will also be taken into account in assessing the applicant's competence. For further details about the Qualifications Framework in Hong Kong, please visit www.hkqf.gov.hk.

[12] "Designated fields" refer to accounting, business administration, economics, finance and law.

[13] Internationally-recognised professional qualifications in law, accounting or finance. Internationally-recognised professional qualifications in finance include Chartered Financial Analyst (CFA), Certified International Investment Analyst (CIIA) and Certified Financial Planner (CFP).

[14] The SFC also recognises as equivalent to HKDSE (a) the attainment of grade E or above in either English or Chinese as well as in Mathematics in the Hong Kong Certificate of Education Examination (HKCEE) and (b) passes in the same subjects in other high school public examinations (such as university entry examinations) in Hong Kong or elsewhere ~~as equivalent to HKDSE~~.

RIQ[15] or Extra CPT[16]	-	Obtained RIQ (HKSI LE Papers 7 ~~&~~ and 8) or completed relevant Extra CPT[16]	Obtained RIQ (HKSI LE Papers 7 ~~&~~ and 8)	Completed relevant Extra CPT[16]
Management experience	2 years	2 years	2 years	
LRP[17]	Pass (HKSI LE Papers 1 ~~&~~ and 2)	Pass (HKSI LE Papers 1 ~~&~~ and 2)	Pass (HKSI LE Papers 1 ~~&~~ and 2)	

3.17 For an individual who does not possess the academic or professional qualifications set out in paragraph 3.16 but ~~has been~~was a licensee before 1 January 2022[18], the SFC will consider his or her application if he or she has:

(a) acquired at least eight years of relevant industry experience in the Relevant Activities over the past 11 years; and

(b) met the management experience and LRP requirements set out in paragraph 3.16 above.

3.18 In assessing the "relevant industry experience" of an individual, the SFC will take a pragmatic approach. For example, the SFC may recognise an individual's previous direct experience in technology as relevant ~~industry experience~~ if the individual has been a key person in developing, or ensuring the proper and continued functioning of, a technology, platform or system (ie, not merely providing system support); and the technology, platform or system in which the individual has expertise is central to the virtual asset trading platform operated by his or her new principal[19].

3.19 "Management experience" refers to ~~the~~ hands-on experience in supervising and managing essential regulated functions or projects in a business setting, including the management of staff engaging in these functions or projects. For example, managing individuals conducting Relevant Activities may be considered relevant management experience.

3.20 The SFC will also accept management experience acquired in the financial industry. However, the SFC would not normally accept management experience which is

---

15 Please note: (i) ~~t~~The RIQ requirements will be updated on the SFC's website as and when changes occur~~.~~; (ii) ~~t~~The SFC will also accept industry qualifications for Type 1 regulated activity listed in Appendix C of the previous Guidelines on Competence published by the SFC under section 399 of the SFO in June 2011 (please refer to the SFC's website for the previous version). Whilst the SFC may also accept qualifications obtained elsewhere, the individual has to provide supporting documents issued by the relevant academic or professional body which demonstrate the equivalence of ~~such~~ the qualifications to the required HKSI or Vocational Training Council papers ~~concerned~~.

16 "Extra CPT" means that the individual must complete five CPT hours which is a one-off requirement, irrespective of whether the individual is applying under the SFO ~~and/or~~, the AMLO or both. The additional CPT hours should be taken within six months preceding the submission of the application.

17 Please note the LRP requirements will be updated on the SFC's website as and when changes occur.

18 1 January 2022 is the effective date of the revised Guidelines on Competence which is applicable to applications for SFO-licensed Platform Operators, SFO-LRs and SFO-ROs. Similar requirements have been introduced here for consistency ~~purpose~~.

19 Where an RO applicant mainly relies on a technology background for the purpose of satisfying the "relevant industry experience" requirement, and subject to meeting other licensing requirements, the SFC may approve the RO application and impose a "non-sole" condition on the individual's licence. This means that the individual must, when actively participating in or directly supervising the Relevant Activities for which the Platform Operator is licensed, do so under the advice of another RO who is not subject to the same condition.

purely administrative (for example, supervision of human resources or office administration staff).

3.21 An individual who holds a directorship in, or is engaged in the business of, companies other than his or her principal should properly address any conflicts of interest arising from such activities, especially when the directorship or engagement will likely prejudice the interests of investors due to concerns about confidentiality or other factors.

Licensed representatives

3.22 In assessing the competence of an individual applying to be an LR, the SFC will expect him or her to have a basic understanding of the market in which he or she is to work as well as the laws and regulatory requirements applicable to the industry. For an individual applying to be an LR (whether under the SFO, the AMLO or both), a summary of the options for satisfying the competence requirements is set out below:

	Option A	Option B		Option C	
Academic or professional qualifications	Degree[20] in the designated fields[21]; other degree[20] (with passes in at least two courses in the designated fields[21]); or professional qualifications[22]	Other degree (without passes in two courses in the designated fields[21])		Attained Level 2 in either English or Chinese as well as in Mathematics in the HKDSE or equivalent[23]	
Relevant industry experience	—	At least 2 years over the past 5 years	—	At least 2 years over the past 5 years	—
RIQ[24] or Extra CPT[25]	—	—	Obtained RIQ (HKSI LE Papers 7 ~~&~~ and 8) or completed relevant Extra CPT[25]	Completed relevant Extra CPT[25]	Obtained RIQ (HKSI LE Papers 7 ~~&~~ and 8)
LRP[26]	Pass (HKSI LE Paper 1)	Pass (HKSI LE Paper 1)		Pass (HKSI LE Paper 1)	

3.23 For an individual who does not possess the academic or professional qualifications set out in paragraph 3.22 but ~~has been~~was a licensee before 1 January 2022[27], the SFC will consider his or her application if he or she has:

(a) acquired either:

---

[20] If an applicant who is a degree holder has attained a post-graduate diploma or certificate which is (a) issued by a university or other similar tertiary institution in Hong Kong or elsewhere; or (b) recognised as Level 6 or above under the Qualifications Framework in Hong Kong, then the post-graduate diploma or certificate will also be taken into account in assessing the applicant's competence. For further details about the Qualifications Framework in Hong Kong, please visit www.hkqf.gov.hk.

[21] "Designated fields" refer to accounting, business administration, economics, finance and law.

[22] Internationally-recognised professional qualifications in law, accounting or finance. Internationally-recognised professional qualifications in finance include Chartered Financial Analyst (CFA), Certified International Investment Analyst (CIIA) and Certified Financial Planner (CFP).

[23] The SFC also recognises as equivalent to HKDSE (a) the attainment of grade E or above in either English or Chinese as well as in Mathematics in the HKCEE and (b) passes in the same subjects in other high school public examinations (such as university entry examinations) in Hong Kong or elsewhere ~~as equivalent to HKDSE~~.

[24] Please note: (i) the RIQ requirements will be updated on the SFC's website as and when changes occur~~.~~ ; (ii) the SFC will also accept industry qualifications listed in Appendix C of the previous Guidelines on Competence published by the SFC under section 399 of the SFO in June 2011 (please refer to the SFC's website for the previous version).

[25] "Extra CPT" means that the individual must complete five CPT hours which is a one-off requirement. The additional CPT hours should be taken within six months preceding the submission of the application.

[26] Please note the LRP requirements will be updated on the SFC's website as and when changes occur.

[27] See explanation in footnote 18 above.

(i) at least five years of relevant industry experience in the Relevant Activities over the past eight years; or

(ii) at least two years of relevant industry experience in the Relevant Activities over the past five years and obtained the relevant RIQ; and

(b) met the LRP requirements set out in paragraph 3.22 above.

Exemptions from the RIQ and LRP requirements

General principles

3.24 The objective of requiring individuals conducting Relevant Activities to obtain RIQ and pass LRP is to ensure ~~that~~ they are adequately equipped to carry on the Relevant Activities and are aware of their legal responsibilities ~~as well as~~and potential liabilities.

3.25 Notwithstanding ~~the above~~this fundamental ~~principle~~objective, the SFC will review and consider all relevant facts and circumstances presented in an application in a pragmatic manner, and may at its sole discretion consider:

(a) granting an individual an exemption from obtaining an RIQ ~~or~~, passing an LRP or both, if he or she can demonstrate possession of comparable qualifications or industry experience; or

(b) approving the licence application of an individual on the condition that he or she must pass an LRP within six months of obtaining the approval.

3.26 In granting the exemptions or approvals, the SFC may impose licensing conditions on, and request the provision of confirmations or undertakings from, the individuals, sponsoring corporation or both, as and when appropriate.

3.27 Exemptions or approvals so granted are specific to the facts and circumstances set forth in the application and in the context of the individual's engagement with the sponsoring corporation, and are therefore~~,~~ non-transferable. The individual may be required to obtain an RIQ or pass an LRP if there are changes to his or her role or the sponsoring corporation.

3.28 The ~~Criteria~~ criteria under which exemptions may be considered are detailed in paragraphs 3.30 to 3.38 below. These criteria may be changed and updated where necessary.

3.29 Individuals and sponsoring corporations are reminded that:

(a) breaching any of the conditions imposed or undertakings provided, or providing false or misleading information in the confirmations, may impugn the fitness and properness of the individual, the sponsoring corporation~~,~~ or both; and

(b) failure to pass the requisite LRP within the specified time may render the approval invalid and cause the licence to lapse unless the SFC grants a further extension~~.~~. The SFC may consider ~~such~~ an extension under exceptional circumstances as it considers appropriate. Where appropriate, the

SFC may also impose additional conditions on the individual licensee limiting the scope of his or her business activities. In addition, the above grace period (including any further extension) is usually granted once with respect to each LRP. If the individual has previously been granted a grace period (including any further extension) but did not pass the LRP concerned, he or she is expected to obtain a pass in that LRP before submitting his or her application again.

RIQ exemptions

A. Full exemption for ROs and LRs

3.30 An individual may apply for a full exemption from the RIQ requirements if he or she has been licensed by the SFC within the past three years or is currently licensed by the SFC and now applies to carry on the Relevant Activities with the same RIQ requirements[28] and in the same role[29] as previously licensed by the SFC.

B. Conditional exemption for ROs and LRs

3.31 Under exceptional circumstances, an individual may apply for a conditional exemption from the RIQ requirements if he or she is currently licensed by the SFC and has five years of related local experience over the past eight years and now applies to carry on the Relevant Activities with different RIQ requirements[28] but in the same role[29].

(a) Conditions to be imposed: The SFC would consider imposing licensing conditions which restrict the scope of activities to be undertaken by the individual or any other licensing conditions as the SFC considers appropriate.

(b) Confirmations and undertakings to be provided: The individual must complete an additional five CPT hours in ~~the~~ industry or product knowledge in respect of the conduct of the Relevant Activities, which is a one-off requirement.

Note 1: The additional CPT hours may be completed within six months preceding the submission of the application. In this case, both the individual and the sponsoring corporation should provide confirmation that the individual has already completed the required CPT hours.

Note 2: Alternatively, the additional CPT hours may be completed within 12 months after licence approval is granted. In this case, both the individual and the sponsoring corporation should provide undertakings to this effect.

Note 3: The ~~related~~ supporting records and documentary evidence for the CPT hours completed may be inspected by the SFC as and when required.

LRP exemptions

[28] Please refer to paragraphs 4.2.2 (RO) and 4.3.2 (LR) of the Guidelines on Competence published under the SFO by the SFC for the RIQ requirements for different regulated activities.

[29] Either as RO or as LR.

A. Full exemption for ROs and LRs

3.32 An individual may apply for a full exemption from the LRP requirements if he or she:

(a) has been a licensee within the past three years or is a current licensee and now applies to carry on Relevant Activities with the same LRP requirements[30] and in the same role[31] as previously licensed; or

Note: An individual applying to be an LR may only rely on this exemption if he or she has attempted HKSI LE Paper 1. Where the individual has never attempted HKSI LE Paper 1, he or she may consider relying on LRP Conditional Exemption 5.

(b) has been actively involved in regulatory or compliance work:

(i) in Hong Kong;

(ii) on a full-time basis;

(iii) for at least three years over the past six years; and

(iv) in the Relevant Activities for a Platform Operator licensed by the SFC.

The SFC would consider imposing licensing conditions which restrict the scope of activities to be undertaken by the individual or any other licensing conditions as the SFC considers appropriate.

B. Conditional exemptions for ROs only

LRP Conditional Exemption 1

3.33 An RO applicant may apply for a conditional exemption from the LRP requirements if he or she can demonstrate all of the following:

(a) Experience: The individual has proven, substantial related experience but simply lacks the required level of local regulatory exposure.

Note: "Substantial" means having at least:

(i) eight years of related experience in a jurisdiction where any of the specified exchanges in Schedule 3 to the Financial Resources Rules is domiciled; or

(ii) six years of related experience with at least two of these years ~~of being~~ licensed in Hong Kong,

with some part of it gained in the most recent three years.

(b) Restriction of permitted activities:

[30] Please refer to paragraphs 4.2.3 (RO) and 4.3.3 (LR) of the Guidelines on Competence published under the SFO by the SFC for the LRP requirements for different regulated activities.

[31] Either as RO or as LR.

(i) The individual is either only involved in a limited scope of activities for the sponsoring corporation or only assuming a very senior management level role; or

(ii) the sponsoring corporation will only be carrying on a limited scope of business activities.

(c) Regulatory support from other personnel:

(i) There is at least one approved RO at the sponsoring corporation who is licensed for conducting the Relevant Activities, and would be directly reporting to or otherwise responsible for advising the individual as well as supervising the daily conduct of the Relevant Activities.

(ii) This approved RO should be designated by name to the SFC and replaced with someone else equivalently approved if the designated person changes job functions or employment. Instead of notifying the SFC whenever there are changes in the designated persons, the sponsoring corporation should provide a confirmation to the SFC that it has a system to maintain records whereby these designations are kept current to reflect personnel changes so that the SFC can inspect them if needed. ~~and that i~~If a designated person is not available, the exempted individual and the sponsoring corporation will immediately inform the SFC.

(d) Internal control systems in place: The sponsoring corporation has in place an appropriate risk and regulatory compliance infrastructure (including a comprehensive risk management system, internal audit, compliance staff and procedures).

(e) Conditions to be imposed: The SFC would consider imposing licensing conditions which restrict the scope of activities to be undertaken by the individual, the sponsoring corporation~~,~~ or both (for example, the individual's activities are all confined within the same group of related companies, or the individual does not engage in any activities with retail clients) or any other licensing conditions as the SFC considers appropriate.

(f) Confirmations and undertakings to be provided: The individual and sponsoring corporation should provide the following confirmations and undertakings ~~on the following~~[32], as applicable:

(i) confirmation from the sponsoring corporation that it has suitably qualified back office staff (including finance, compliance, and audit staff);

(ii) undertakings from both the individual and the sponsoring corporation that they will update the SFC on any significant change to the underlying circumstances, including the job functions or the Relevant Activities the individual engages in, the sponsoring corporation's business activity relevant to the individual, or changes in any designated licensed or support personnel; and

[32] These items are not intended to be exhaustive.

(iii) the individual must complete an additional five CPT hours in local regulatory knowledge in the Relevant Activities which is a one-off requirement.

- The additional CPT hours may be completed within six months preceding the submission of the application. In this case, both the individual and the sponsoring corporation should provide confirmation that the individual has already completed the required CPT hours.
- Alternatively, the additional CPT hours may be completed within 12 months after the licence approval is granted. In this case, both the individual and the sponsoring corporation should provide undertakings to this effect.
- The ~~related~~ supporting records and documentary evidence for the CPT hours completed may be inspected by the SFC as and when required.

Note: After the individual has obtained the above conditional exemption and been licensed for three years, the requirement for a designated RO to provide regulatory support can be removed.

LRP Conditional Exemption 2

3.34 An RO may apply for a conditional exemption from the LRP requirements if he or she has five years of related local experience over the past eight years and now applies to carry on Relevant Activities with different LRP requirements[33].

(a) Conditions to be imposed: The SFC would consider imposing licensing conditions which restrict the scope of activities to be undertaken by the individual, the sponsoring corporation~~,~~ or both, or imposing any other licensing conditions as ~~the SFC~~it considers appropriate.

(b) Confirmations and undertakings to be provided: The individual must complete an additional five CPT hours in local regulatory knowledge relevant to the Relevant Activities, which is a one-off requirement.

(i) The additional CPT hours may be completed within six months preceding the submission of the application. In this case, both the individual and the sponsoring corporation should provide confirmation that the individual has already completed the required CPT hours.

(ii) Alternatively, the additional CPT hours may be completed within 12 months after the licence approval is granted. In this case, both the individual and the sponsoring corporation should provide undertakings to this effect.

[33] See footnote 30 above.

(iii) The ~~related~~ supporting records and documentary evidence for the CPT hours completed may be inspected by the SFC as and when required.

LRP Conditional Exemption 3

3.35 An LR of a Platform Operator applying for approval to become an RO of a~~ny~~ Platform Operator may apply for a conditional exemption from the LRP requirements if he or she possesses at least three more years of relevant industry experience in addition to the general competence requirements set out in paragraph 3.16. The additional three years must be recent and licensed experience acquired in Hong Kong.

(a) Confirmations and undertakings to be provided: The individual must complete an additional five CPT hours in local regulatory knowledge in the Relevant Activities, which is a one-off requirement.

(i) The additional CPT hours may be completed within six months preceding the submission of the application. In this case, both the individual and the sponsoring corporation should provide confirmation that the individual has already completed the required CPT hours.

(ii) Alternatively, the additional CPT hours may be completed within 12 months after the licence approval is granted. In this case, both the individual and the sponsoring corporation should provide undertakings to this effect.

(iii) The ~~related~~ supporting records and documentary evidence for the CPT hours completed may be inspected by the SFC as and when required.

C. Conditional exemptions for LRs only

LRP Conditional Exemption 4

3.36 Itinerant professionals, being individuals from elsewhere who need to visit Hong Kong repeatedly for a short period each time to conduct Relevant Activities in Hong Kong, may apply for a conditional exemption from the LRP requirements.

(a) Conditions to be imposed:

(i) The individual shall not carry on Relevant Activities in Hong Kong for more than 30 days in each calendar year;

(ii) the individual shall at all times be accompanied by a licensed person in carrying on Relevant Activities in Hong Kong; and

(iii) without compromising investor protection, the SFC may consider removing the chaperoning requirement in condition (ii) and impose an alternative condition to the effect that the individual can only provide services which constitute Relevant Activities to institutional professional investors.

(b) Undertakings to be provided:

(i) For itinerant professionals subject to conditions (i) and (ii) above, the sponsoring corporation should provide an undertaking to the effect that it will assume full responsibility for the supervision of the individual's activities during his or her stay in Hong Kong and ensure that he or she will comply with the relevant rules and regulations at all times.

(ii) For itinerant professionals subject to condition (i) and alternative condition (iii) above, the sponsoring corporation should provide additional undertakings that it will:

- provide training to the individual in the form of a structured course ~~to the individual~~ to ensure that he or she is fully aware of the Hong Kong regulatory framework before he or she commences carrying on Relevant Activities in Hong Kong; and

- comply with the requirements set out under paragraph 3.33(c), ~~in which~~whereby it will arrange for at least one approved RO who is licensed in the Relevant Activities to directly supervise or otherwise be responsible for advising the individual in conducting Relevant Activities in Hong Kong.

LRP Conditional Exemption 5

3.37 An individual who has been an LR within the past three years or is a current LR and (a) has never attempted HKSI LE Paper 1 before and now applies to carry on Relevant Activities with the same LRP requirements[34] and in the same role[35]; or (b) now applies to carry on Relevant Activities with different LRP requirements[34] but in the same role[35], may apply for a conditional exemption from the LRP requirements.

(a) Confirmations and undertakings to be provided:

The individual must complete an additional five CPT hours in local regulatory knowledge in Relevant Activities, which is a one-off requirement.

(i) The additional CPT hours may be completed within six months preceding the submission of the application. In this case, both the individual and the sponsoring corporation should provide confirmation that the individual has already completed the required CPT hours.

(ii) Alternatively, the additional CPT hours may be completed within 12 months after the licence approval is granted. In this case, both the individual and the sponsoring corporation should provide undertakings to this effect.

(iii) The ~~related~~ supporting records and documentary evidence for the CPT hours completed may be inspected by the SFC as and when required.

Re-entrant exemption

[34] See footnote 30 above.
[35] Either as RO or ~~as~~ LR.

3.38 An individual may apply for a conditional exemption from both the RIQ and LRP requirements if he or she is a former practitioner who has left the industry for between three to eight years~~,~~ and re-applies for a licence with the same RIQ and LRP requirements[36] and in the same role[37] as previously licensed.

To be eligible for the exemption:

(a) the individual must complete five CPT hours, per year of absence (any fraction of a year would be rounded up), ~~where~~ with training in local regulatory knowledge ~~must make~~ making up at least 50% of the CPT activities;

(b) the required CPT hours should be completed before the submission of the application;

(c) both the individual and the sponsoring corporation should provide confirmation that the individual has already completed the required CPT hours and that training in local regulatory knowledge ~~was~~ made up not less than 50% of the CPT activities; and

(d) the ~~related~~ supporting records and documentary evidence for the CPT hours completed may be inspected by the SFC as and when required.

[36] See footnotes 28 (RIQ requirements) and 30 (LRP requirements) above.
[37] Either as RO or ~~as~~ LR.

IV. Continuous Professional Training Requirements

4.1 CPT is the systematic maintenance, improvement and broadening of knowledge and skills to enable individuals carrying on Relevant Activities to perform their duties competently and professionally. The objectives of the CPT programme are:

(a) to maintain and enhance their technical knowledge and professional expertise;

(b) to provide reasonable assurance to investors at large that they have the technical knowledge, professional skills and ethical standards required to carry on Relevant Activities efficiently, effectively and fairly; and

(c) to maintain and enhance Hong Kong's international reputation for high professional standards.

4.2 The SFC takes the view that the CPT objectives ~~of CPT~~ could not be achieved solely through work experience or on-the-job training. It will generally be necessary for individuals to undertake CPT if they are to remain fit and proper.

4.3 The CPT requirements ~~for CPT~~ will vary according to the size and nature of the business and the nature of the responsibilities to be undertaken by an individual. Rather than mandating particular programmes, these Guidelines describe the general attributes of the CPT programme.

4.4 Licensed persons are required to confirm their compliance (or explain non-compliance) with the applicable CPT requirements annually with the SFC, and shall provide such confirmation for the previous calendar year when they submit their annual returns electronically[38].

4.5 Failure to satisfy any applicable CPT requirements will cast doubt on the fitness and properness of corporations and individuals to remain licensed and may lead to disciplinary action by the SFC. Nevertheless, the SFC will adopt a pragmatic approach taking into account the circumstances and the facts of the breach before taking any action.

Requirements for corporations

4.6 Corporations are held primarily responsible for planning and implementing a continuous education programme best suited to the training needs of the individuals they engage which will enhance their industry knowledge, skills and professionalism. The apportioning of training costs will be a matter between the corporations and the individuals.

4.7 Corporations should ~~at least annually~~ evaluate their training programmes at least annually and make commensurate adjustments to cater for the training needs of the individuals they engage.

[38] For example, in their electronic submission of an annual return with an anniversary date in 2024, they would confirm their compliance (or non-compliance) with the CPT requirements for calendar year 2023.

4.8 In developing ~~the~~ training programmes, consideration should be given to the corporation's size, organisational structure, risk management system and scope of business activities as well as the prevailing regulatory framework and market development.

4.9 The training programmes can be provided internally or the corporations can make use of appropriate external sources. In selecting training courses, corporations should satisfy themselves of the quality of the trainers and the standard of the training programmes. They should also ensure that the contents of ~~such~~ the courses are appropriately structured and of benefit to the individuals in performing their functions. Subjects which are relevant to the individuals' functions and may help to enhance the performance of their functions would meet the CPT purpose.

4.10 Neither the SFC nor its Academic and Accreditation Advisory Committee (AAAC)[39] would endorse any training courses, whether provided internally or externally.

4.11 Corporations should keep the details of the training conducted, the attendance records and materials provided for individuals who have completed the training.

4.12 Sufficient records of the programmes and the CPT activities undertaken by ~~the~~ individuals should be kept for a minimum of three years and ~~be~~ made available for inspection or upon request by the SFC.

Requirements for individuals

4.13 Individuals must remain fit and proper at all times. One of the criteria is that an individual is continuously competent to carry on Relevant Activities. The SFC considers that an individual's continued competence to carry on Relevant Activities may be achieved by undertaking training that enhances his or her technical skills, professional expertise, ethical standards and regulatory knowledge.

4.14 An LR must undertake a minimum of 10 CPT hours per calendar year[40]. In view of the ~~higher level of~~greater responsibility and accountability placed on ROs, they are required to complete two additional CPT hours (ie, at least 12 CPT hours per calendar year[41]). These two additional CPT hours should cover topics relating to regulatory compliance.

4.15 An individual should complete at least five CPT hours per calendar year (out of the 10 hours for LRs and 12 hours for ROs) on topics directly ~~relevant~~ related to the Relevant Activities. As a general principle, such CPT hours should be allocated to cover the practice areas of the individual in proportion to the time and effort that the individual~~he or she~~ spends in each area.

4.16 Within the 12 months after a person first becomes LR or RO[42], that person must undertake two CPT hours on ~~"~~ethics~~"~~, which include, but are not limited to, topics

---

[39] The AAAC is comprised of representatives from the SFC, the industry and academic institutions. It regularly reviews the CPT requirements to ensure ~~that~~ they meet general market needs and international standards and also considers applications as recognised institutions for CPT purposes.

[40] For the avoidance of doubt, an LR, irrespective of whether he or she is licensed under the SFO, the AMLO or both, is only required to take 10 CPT hours per calendar year.

[41] For the avoidance of doubt, an RO, irrespective of whether he or she is licensed under the SFO, the AMLO or both, is only required to take 12 CPT hours per calendar year.

[42] This refers to an individual who first becomes an LR or RO under the SFO or the AMLO, whichever is earlier.

relating to integrity, fairness, due care and diligence, good faith, objectivity, best interests of clients, treating clients fairly, avoidance of conflicts of interest and confidentiality of clients' information. Thereafter, he or she is required to complete at least two CPT hours per calendar year on topics relating to ethics or compliance. Topics relating to ~~"~~compliance~~"~~ include, but are not limited to, the legal and regulatory framework for the financial industry~~,~~ and the codes of conduct and industry guidelines issued by regulatory authorities~~,~~ as well as policies and guidelines set out by individual corporations internally or by other professional bodies.

4.17 For the avoidance of doubt, an individual who first joins the industry can count the mandatory two CPT hours on ethics towards the annual CPT requirement set out in paragraph 4.16 above. However, thesey~~e~~ do not count towards the two additional CPT hours required of ROs set out in paragraph 4.14 above nor may they be used to meet the CPT requirements for a conditional exemption ~~of~~ from the RIQ and ~~the~~ LRP requirements.

4.18 Individuals are also required to retain appropriate records of all CPT activities completed in ~~a~~ each calendar year. Documentary evidence sufficient to support their attendance or completion of the CPT activities, such as certificates of attendance issued by the course providers and examination results, should be kept by the individuals for a minimum of three years. The SFC may request LRs and ROs to produce ~~such~~ this documentary evidence as and when required.

4.19 Several practical issues regarding the accumulation of CPT hours are set out in the following paragraphs.

(a) The CPT hours required for an individual[43]~~,~~ who is first licensed during the year~~,~~ can be applied pro-rata with reference to the licensed period[44]. For example, if an individual was granted a licence as an LR on 1 July, the total number of CPT hours required of him or her for the calendar year would be five (ie, half of the annual CPT requirement for LRs).

(b) The training courses attended prior to the date of licence but within the same calendar year can count towards CPT hours. This would include study hours for fulfilling competence requirements if a pass in the relevant examination is proven.

(c) When an individual changes his or her employer within the same calendar year, he or she can carry forward his or her CPT hours undertaken at the previous employer. The new employer does not need to ~~get~~ obtain the CPT information from the previous employer. It can rely on the declaration and ~~the~~ documentary evidence provided by the individual.

(d) It is not necessary for an individual to apportion ~~his or her~~the CPT hours he or she undertakes to accord~~undertaken in accordance~~ with his or her periods of employment with the previous and new employers.

---

[43] Including the (i) 10 CPT hours per calendar year for LRs and ROs; (ii) additional two CPT hours on regulatory compliance for ROs; and (iii) five CPT hours on topics directly relevant to the Relevant Activities in which an individual engages~~; and (iv) two CPT hours on topics relating to ethics or compliance~~.

[44] Except for the one-off mandatory requirement of two CPT hours on ethics required of new joiners as set out in paragraph 4.16 above.

(e) The new employer will not be accountable for the non-compliance of the individual who has not undertaken enough CPT hours at his or her previous employer. Thereafter, it has to ensure that the individual meets the annual CPT hour requirements, ie, 10 CPT hours for LRs or 12 CPT hours for ROs.

(f) Excess CPT hours accumulated in one calendar year cannot be carried forward to the following year.

Relevant CPT activities

4.20 CPT hours are time spent by individuals in undertaking CPT activities. The CPT activities should be relevant to the functions to be performed by them[45] and they should incorporate significant intellectual and practical content and involve interaction with other persons.

4.21 The following are acceptable means of obtaining CPT:

(a) attending courses, workshops, lectures and seminars[46];

(b) distance learning which requires submission of assignments;

(c) self-study or online learning courses[47];

(d) industry research;

(e) publication of papers;

(f) delivery of speeches[46];

(g) giving lectures or teaching[46];

(h) providing comments ~~to~~ on industry consultation papers;

(i) attending meetings or undertaking activities as members of the SFC's regulatory committees or formal working groups[48]; and

(j) attending luncheon talks which normally last for one to two hours in total (0.5 hour will be counted).

4.22 Normal working activities, general reading of financial press or technical, professional, financial or business literature and activities which do not involve interaction with other persons are generally not regarded as CPT activities.

---

[45] See paragraph 4.15 above for specific requirements.
[46] Both face-to-face and virtual formats are acceptable.
[47] Independent assessments (such as evaluation or test results) and sufficient records are required to demonstrate fulfilment and duration of training.
[48] Formal working groups set up for the purpose of making decisions on a predetermined subject, meetings of which are presided over by a chairman and with minutes.

Relevant topics

4.23 Individuals are required to remain fit and proper to perform their functions at a professional level. Relevant topics for individuals at the LR level include:

(a) applicable compliance, legislative and regulatory standards[49];

(b) business conduct and ethical standards[50];

(c) market developments, new financial products and risk management systems;

(d) business communication skills and trade practices;

(e) general law principles;

(f) basic accounting theories;

(g) fundamental economic analysis;

(h) Fintech and virtual assets;

(i) environmental, social and governance (ESG);

(j) cybersecurity; and

(k) information technology.

4.24 Relevant topics for ROs who play a crucial role in ensuring effective corporate governance and control may, in addition to the above topics, include the following:

(a) business management;

(b) risk management and control strategies;

(c) general management and supervisory skills;

(d) macro and micro economic analysis; and

(e) financial reporting and quantitative analysis.

4.25 The topics listed above are only examples and are by no means exhaustive.

4.26 Generally speaking, language courses do not count towards CPT. Management training can count towards CPT if the training assists in enhancing the person's ability to carry out the Relevant Activities.

4.27 Seminars given by the SFC pertaining to regulatory updates and other relevant topics can count towards CPT.

---

[49] See paragraph 4.16 above.
[50] See paragraphs 4.16 and 4.17 above.

4.28 Repeatedly undertaking the same CPT activity with the same content will not satisfy the requirements.

V. ~~General~~ Conduct of Business Principles

5.1 Platform Operators should comply with the spirit of these principles when carrying on any Relevant Activities.

(a) In conducting its business activities, a Platform Operator should act honestly, fairly, and in the best interests of its clients and the integrity of the market.

(b) In conducting its business activities, a Platform Operator should act with due skill, care and diligence, in the best interests of its clients and the integrity of the market.

(c) A Platform Operator should have and employ effectively the resources and procedures which are needed for the proper performance of its business activities.

(d) A Platform Operator should seek from its clients[51] information about their financial situation, investment experience and investment objectives and assess their risk tolerance level and risk profile relevant to the services to be provided.

(e) A Platform Operator should make clear and adequate disclosure of relevant material information in its dealings with clients.

(f) A Platform Operator should try to avoid conflicts of interest, and when they cannot be avoided, should ensure that its clients are fairly treated.

(g) A Platform Operator should ensure the reliability and security of its trading platform.

(h) A Platform Operator should comply with all regulatory requirements applicable to the conduct of Relevant Activities so as to promote the best interests of clients and the integrity of the market. The Platform Operator should also respond to requests and enquiries from the regulatory authorities in an open and cooperative manner.

(i) A Platform Operator should ensure that client assets are promptly and properly accounted for and adequately safeguarded.

(j) A Platform Operator should maintain proper records.

(k) The senior management[52] of a Platform Operator should bear primary responsibility for ensuring the maintenance of appropriate standards of conduct and adherence to proper procedures by the Platform Operator.

---

[51] Except for clients which are institutional and qualified corporate professional investors.

[52] In determining where responsibility lies, and the degree of responsibility of a particular individual, regard shall be had to that individual's apparent or actual authority in relation to the particular business operations, levels of responsibility within the Platform Operator, any supervisory duties he or she may perform, and the ~~levels~~ degree of control or knowledge he or she may have concerning any failure by the Platform Operator or persons under his or her supervision to follow these Guidelines. ~~The SFC is generally of the view that senior management of a Platform Operator includes, amongst others, directors, responsible officers and individuals appointed by a Platform Operator to be principally responsible, either alone or with others, for management core functions of the Platform Operator.~~

VI. Financial Soundness

Financial resources and soundness

6.1 A Platform Operator should maintain in Hong Kong at all times assets which it beneficially owns and are sufficiently liquid, for example, cash, deposits, treasury bills and certificates of deposit (but not virtual assets), equivalent to at least 12 months of its actual operating expenses calculated on a rolling basis.

6.2 A Platform Operator ~~shall~~ must at all times maintain paid-up share capital of not less than HK$ 5,000,000 (referred to as "minimum paid-up share capital").

6.3 A Platform Operator must at all times maintain liquid capital which is not less than its required liquid capital. The Platform Operator, for the purposes of calculating its liquid capital and required liquid capital, should account for all its assets, liabilities and transactions in accordance with Part 4 of the Financial Resources Rules[53] and follow the computation basis prescribed in Division 2 of Part 4 of the Financial Resources Rules. Specifically:

(a) liquid capital means the amount by which the Platform Operator's liquid assets exceeds its ranking liabilities, where:

(i) liquid assets means the aggregate of the amounts required to be included in the Platform Operator's liquid assets under the provisions of Division 3 of Part 4 of the Financial Resources Rules; and

(ii) ranking liabilities means the aggregate of the amounts required to be included in the Platform Operator's ranking liabilities under the provisions of Division 4 of Part 4 of the Financial Resources Rules; and

(b) required liquid capital means the higher of HK$ 3,000,000 and the basic amount as defined in section 2 of the Financial Resources Rules.

6.4 For the purposes of ~~this~~ Part VI of these Guidelines, a Platform Operator must account for all assets and liabilities:

(a) in accordance with generally accepted accounting principles, unless otherwise specified in the Financial Resources Rules; and

(b) in a way ~~that~~ which recognises the substance of a transaction, arrangement or position.

The Platform Operator must not, without notifying the SFC under paragraph 6.10~~9~~, change any of its accounting principles, other than those referred to in subparagraph (a), in a way that may materially affect the paid-up share capital or liquid capital ~~that~~ which it maintains or is required to maintain under paragraphs 6.2 and 6.3 respectively.

---

[53] For the purposes of ~~this~~ Part VI of these Guidelines, any reference to a licensed corporation in the Financial Resources Rules should be read to mean a Platform Operator, except for (b)(ii)(D) of the definition of marketable debt securities and sections 9(6)(b)(i)(D) and 19(2)(a)(iii) of the Financial Resources Rules.

Financial returns

6.5 A Platform Operator shall, in respect of each month at the end of which it remains licensed, submit to the SFC, no later than three weeks after the end of the month concerned, a return which is in the form specified by the SFC and includes~~, amongst other things, the Platform Operator's liquid capital computation and required liquid capital computation as at the end of the month.~~ :

(a) the Platform Operator's liquid capital computation, as at the end of the month;

(b) the Platform Operator's required liquid capital computation, as at the end of the month;

(c) a summary of bank loans, advances, credit facilities and other financial accommodation available to the Platform Operator, as at the end of the month;

(d) an analysis of the Platform Operator's client assets, as at the end of the month; and

(e) an analysis of the Platform Operator's profit and loss account.

The Platform Operator shall sign and submit the return to the SFC in the manner specified by the SFC.

6.6 A Platform Operator may elect to submit the return required under paragraph 6.5 above, in respect of periods of not less than 28 days but not more than 35 days, each of which ending not more than seven days before or after the end of a month~~,~~. The Platform Operator must determine~~d by it~~such periods ~~on a basis according to which~~so that the ending date of each period ~~so determined~~ is predictable~~, and~~. ~~where~~ Where ~~it~~ the Platform Operator ~~so~~ elects to ~~and~~ submit~~s~~ the return ~~concerned~~in this manner, it is deemed to have submitted the return concerned in respect of ~~the~~ that period ~~required~~.

6.7 A Platform Operator shall, in respect of each financial year, submit to the SFC, no later than four months after the end of that financial year, a return which is in the form specified by the SFC that is made up to the last day of the financial year and includes the information specified under paragraphs 6.5(a) to 6.5(d) above.

Notifications

~~6.7~~6.8 If a Platform Operator becomes aware of its inability to maintain, or to ascertain whether it maintains, sufficient assets, the paid-up share capital or liquid capital ~~that~~ which it is required to maintain under paragraphs 6.1, 6.2 and 6.3 respectively, it shall as soon as reasonably practicable notify the SFC by notice in writing of that fact, including the full details of the matter and the reason therefor ~~and~~ as well as any steps it is taking, has taken or proposes to take to redress the inability.

~~6.8~~6.9 A Platform Operator must notify the SFC in writing as soon as reasonably practicable and in any event within one business day of becoming aware of any of the following matters:

(a) its liquid capital falls below 120% of its required liquid capital;

(b) its liquid capital falls below 50% of the liquid capital stated in its last return submitted to the SFC under paragraph 6.5 above;

(c) any information contained in any of its previous returns submitted to the SFC ~~pursuant to~~under paragraph 6.5 above has become false or misleading in a material particular;

(d) the aggregate of the amounts it has drawn down on any loan, advance, credit facility or other financial accommodation provided to it by banks exceeds the aggregate of the credit limits thereof;

(e) it has been or will be unable, for three consecutive business days, to meet in whole or in part any calls or demands for payment or repayment (as the case may be), from any of its lenders, credit providers or financial accommodation providers;

(f) any of its lenders or any person who has provided credit or financial accommodation to it (lending person) has exercised, or has informed it that the lending person will exercise, the right to liquidate security provided by ~~it~~ the Platform Operator to the lending person in order to reduce its liability or indebtedness to the lending person under any outstanding loan, advance, credit facility balance or other financial accommodation provided to it by the lending person;

(g) the aggregate of the maximum amounts ~~that~~ which can be drawn down against it under any guarantee, indemnity or any other similar financial commitment provided by it~~—~~:

  (i) exceeds HK$ 5,000,000; or

  (ii) would, if deducted from its liquid capital, cause its liquid capital to fall below 120% of its required liquid capital;

(h) the aggregate of the amounts of any outstanding claims made in writing by it or against it (whether disputed or not) exceeds or is likely to exceed HK$ 5,000,000; and

(i) the aggregate of the amounts of any outstanding claims made in writing by it or against it (whether disputed or not) would, if deducted from its liquid capital, cause its liquid capital to fall below 120% of its required liquid capital.

Where the Platform Operator notifies the SFC of any of the abovementioned matters, it must include in the notice full details of the matter and the reasons therefor and, in the case of a notification under subparagraph (a), (b), (d), (e), or (f), include in the notice full details of any steps it is taking, has taken or proposes to take to prevent its liquid capital from falling below its required liquid capital or to improve its liquidity.

6.96.10 Where a Platform Operator intends to change any of its accounting principles in a way that may materially affect the paid-up share capital or liquid capital ~~that~~ it maintains or is required to maintain under paragraphs 6.2 and 6.3 respectively, it must notify the SFC in writing of the details of, and the reasons for, the intended change not less than five business days prior to effecting the change.

6.106.11 A Platform Operator which makes an election under any provision of the Financial Resources Rules for the purpose of complying with Part VI of these Guidelines is bound by the election until withdrawal of the election. If the Platform Operator wishes to withdraw from any election, it must notify the SFC in writing of the details of, and the reasons for, the withdrawal not less than five business days prior to the withdrawal.

6.116.12 For the avoidance of doubt, in addition to the requirements under ~~this~~ Part VI of these Guidelines, an SFO-licensed Platform Operator should also comply with the Financial Resources Rules which are applicable to licensed corporations[54]. Where there are any inconsistencies between such requirements and those under these Guidelines, the more stringent requirement should prevail.

[54] "Licensed corporation" has the meaning as defined in section 1 of Part 1 of Schedule 1 to the SFO.

VII. Operations

Token admission and review committee

7.1 A Platform Operator should set up a token admission and review committee which will be responsible for:

(a) establishing, implementing and enforcing the criteria for a virtual asset to be admitted for trading (ie, the token admission criteria), taking into account factors specified in paragraphs 7.65 to 7.1012 below, and the application procedures if applicable;

(b) establishing, implementing and enforcing the criteria for halting, suspending and withdrawing a virtual asset from trading, and the options available to clients holding that virtual asset;

(c) making the final decision as to whether to admit, halt, suspend and withdraw a virtual asset for clients to trade based on the criteria;

(d) establishing, implementing and enforcing the rules which set out the obligations of and restrictions on virtual asset issuers (for example, the obligation to notify the Platform Operator of any proposed voting, hard fork or airdrop, any material change in the issuer's business or any regulatory action taken against the issuer), if applicable; and

(e) reviewing regularly the criteria and rules mentioned under subparagraphs (a), (b) and (d) above to ensure they remain appropriate, as well as the virtual assets admitted for trading to ensure they continue to satisfy the token admission criteria.

7.2 A Platform Operator should ensure that the criteriadecision-making process of for includingadmitting or removing, suspending and withdrawing a virtual asset for or from trading virtual assets is transparent and fair and disclose such criteria on its website (see paragraph 9.27 below), and is properly documented.

7.3 The token admission and review committee should at least consist of members from senior management who are principally responsible for managing the key business line, compliance, risk management and information technology functions of the Platform Operator.

7.4 A Platform Operator should ensure that the decisions (and the reasons thereof) made by the token admission and review committee are properly documented.

7.47.5 The token admission and review committee should:

(a) report to the Bboard of Ddirectors at least monthly, and its report should, at a minimum, cover the details of the virtual assets made available to retail clients for trading and other issues noted; and

(b) promptly escalate to the board of directors critical matters such as the suspension and withdrawal of virtual assets from trading.

Due diligence on virtual assets

~~7.5~~7.6 A Platform Operator should act with due skill, care and diligence when selecting virtual assets to be made available for trading. The Platform Operator should perform all reasonable due diligence on all virtual assets before including them for trading (irrespective of whether they are made available to retail clients or not), and ensure that they continue to satisfy ~~the~~ all the admission criteria established by the token admission and review committee ~~at all times~~. Set out below is a non-exhaustive list of factors which a Platform Operator must consider, where applicable:

(a) the background of the management or development team of a virtual asset or any of its known key members (if any);

(b) the regulatory status of a virtual asset in Hong Kong ~~each jurisdiction in which the Platform Operator provides trading services~~ and whether its regulatory status would also affect the regulatory obligations of the Platform Operator;

(c) the supply, demand, maturity and liquidity of a virtual asset, including its ~~market capitalisation, average daily trading volume,~~ track record, where the virtual asset (except for a security token) should be ~~(for example,~~ issued for at least 12 months ~~except for security tokens), whether other Platform Operators also provide trading for the virtual asset, the availability of trading pairs (for example, fiat currency to virtual asset), and the jurisdictions where the virtual assets have been made available for trading~~;

(d) the technical aspects of a virtual asset~~, including the security infrastructure of its blockchain protocol, the size of the blockchain and network, and especially how resistant it is to common attacks (for example, a 51% attack[55]), the type of consensus algorithm, and the risk relating to code defects, breaches and other threats relating to the virtual asset and its supporting blockchain, or the practices and protocols that apply to them~~;

~~(e) the marketing materials for a virtual asset issued by the issuer, which should be accurate and not misleading;~~

~~(f)~~(e) the development of a virtual asset ~~including the outcomes of any projects associated with it as set out in its Whitepaper (if any) and any previous major incidents associated with its history and development~~;

~~(g)~~(f) the market and governance risks of a virtual asset~~, including concentrations of virtual asset holdings or control by a small number of individuals or entities, price manipulation, and fraud, and the impact of the virtual asset's wider or narrower adoption on market risks~~;

~~(h)~~(g) the legal risks associated with the virtual asset and its issuer (where applicable)~~, including any pending or potential civil, regulatory, criminal, or enforcement action relating to its issuance, distribution, or use~~; ~~and~~

~~[55] This refers to an attack on a blockchain by a group of miners controlling more than 50% of the network's mining hash rate or computing power.~~

~~(i)~~(h) whether the utility offered, the novel use cases facilitated, ~~or~~ technical, structural or cryptoeconomic innovation, or the administrative control exhibited by the virtual asset clearly appears to be fraudulent or ~~scandalous~~illegal, or whether the continued viability of the virtual asset depends on attracting continuous inflow into the virtual asset;~~.~~

(i) the enforceability of any rights extrinsic to the virtual asset (for example, rights to any underlying assets) and the potential impact of the virtual asset's trading activity on the underlying markets; and

(j) the money laundering and terrorist financing risks associated with the virtual asset.

7.7 Before making any virtual asset available for trading by retail clients, in addition to ensuring that the virtual asset fulfils all the token admission criteria established by the token admission and review committee, a Platform Operator should take all reasonable steps to ensure that the virtual asset:

(a) does not fall within the definition of "securities" under the SFO, unless the offering of such virtual asset to the retail clients complies with the prospectus requirements for offering of shares and debentures under the Companies (Winding Up and Miscellaneous Provisions) Ordinance (Cap. 32) (C(WUMP)O)[56] and does not breach the restrictions on offers of investments under Part IV of the SFO; and

(b) is of high liquidity.

~~7.6~~7.8 In assessing the liquidity of a specific virtual asset for trading by retail clients,~~Where~~ a Platform Operator ~~intends to make a specific virtual asset available for trading by its retail clients, it~~ should, at a minimum, ~~also~~ ensure that the virtual asset is an eligible large-cap virtual asset, ie, the specific virtual asset should have been included in ~~at least~~a minimum of two acceptable indices issued by at least two different index providers~~, before admitting the virtual asset for retail clients to trade~~.

Note 1: An acceptable index refers to an index which has a clearly defined objective to measure the performance of the largest virtual assets in the global market, and should fulfil the following criteria:

(a) The index should be investible, meaning the constituent virtual assets should be sufficiently liquid.

(b) The index should be objectively calculated and rules-based.

(c) The index provider should possess the necessary expertise and technical resources to construct, maintain and review the methodology and rules of the index.

(d) The methodology and rules of the index should be well documented, consistent and transparent.

[56] Parts II and XII of the C(WUMP)O.

Note 2: The two index providers should be separate and independent from each other, the issuer of the virtual asset (if applicable) and the Platform Operator~~, meaning~~ (for example, they are not within the same group of companies). Further, at least one of the indices should be issued by an index provider which complies with the IOSCO Principles for Financial Benchmarks and has experience in publishing indices for the conventional securities market.

Note 3: If a Platform Operator intends to make a specific virtual asset available for trading by its retail clients and such virtual asset fulfils all the token admission criteria under ~~this~~ Part VII of these Guidelines except for this paragraph, the Platform Operator may submit a detailed proposal on the virtual asset for the SFC's consideration on a case-by-case basis.

~~7.7~~7.9 A Platform Operator should ensure that its internal controls and systems, technology and infrastructure (for instance, its anti-money laundering monitoring and market surveillance tools) could support and manage any risks specific to the virtual assets which it intends to make available to its clients for trading.

~~7.8~~7.10 Before admitting any virtual assets for trading, a Platform Operator should exercise due skill, care and diligence in selecting and appointing an independent assessor to conduct a smart contract audit for smart-contract based virtual assets, unless the Platform Operator demonstrates that it would be reasonable to rely on a smart contract audit conducted by an independent ~~auditor~~ assessor engaged by a third party. The smart contract audit should focus on reviewing ~~whether~~ that the smart contract is not subject to any contract vulnerabilities or security flaws to a high level of confidence.

~~7.9 Before making any virtual assets available for trading by retail clients, a Platform Operator should obtain and submit to the SFC written legal advice in the form of a legal opinion or memorandum confirming that each of the virtual assets made available for trading by retail clients does not fall within the definition of "securities" under the SFO.~~

~~7.10~~7.11 A Platform Operator should conduct ongoing monitoring of each virtual asset admitted for trading and consider whether to continue to allow it for trading (for example, whether in respect of a particular segment of its clients or whether a virtual asset continues to satisfy all the token admission criteria). Regular review reports should be submitted to the token admission and review committee. Where the committee decides to ~~halt,~~ suspend ~~and~~ or withdraw a virtual asset from trading, the Platform Operator should as soon as practicable notify clients of its decision and its rationale~~as soon as practicable~~, inform clients holding that virtual asset~~them~~ of the options available ~~to clients holding that virtual asset~~, and ensure that clients~~they~~ are fairly treated.

Note: As an example, where an admitted virtual asset falls outside the constituent virtual assets of an acceptable index as provided in paragraph 7.~~6~~ 8 above, the Platform Operator is not required to automatically suspend or withdraw a virtual asset from trading. However, the Platform Operator should evaluate whether to continue to allow trading of this virtual asset by retail clients. Factors which the Platform Operator may consider include why the virtual asset was removed from an acceptable index and whether there ~~are~~ is any material adverse news ~~or~~ (including those relating to underlying liquidity

issues) for the virtual asset. Where such factors would unlikely be resolved in the near future, the Platform Operator should consider whether the trading of the virtual asset should be ~~halted~~ suspended or whether retail clients should be restricted to the selling of their positions only.

7.12 Given that the specific features of a virtual asset may change throughout its life cycle, a Platform Operator should have appropriate monitoring procedures in place to keep track of any changes to a virtual asset being traded by its clients through its platform that may cause the virtual asset's legal status to change such that the virtual asset falls within or ceases to fall within the definition of "securities" under the SFO. Should a virtual asset traded by its retail clients subsequently falls within the definition of "securities" under the SFO, the Platform Operator should cease to offer that virtual asset for trading by retail clients.

Offering of virtual assets

~~7.11~~7.13 A Platform Operator should note in particular, but without limitation, the following offer of investments requirements:

(a) prospectus requirements for offering of shares and debentures under ~~the Companies (Winding Up and Miscellaneous Provisions) Ordinance (Cap. 32) (~~the C(WUMP)O~~)~~[57];

(b) restrictions on offers of investments under Part IV of the SFO, in particular the restrictions on offering of unauthorised collective investment schemes (CIS) and structured products (for example, overseas exchange-traded exchange traded funds, unauthorised CIS and structured products) notwithstanding the offer is made by or on behalf of an intermediary licensed or registered for Type 1 (dealing in securities), Type 4 (advising on securities) or Type 6 (advising on corporate finance) regulated activity under the SFO[58]; and

(c) relevant requirements relating to the offering of CIS on the internet as set out in the Guidance Note for Persons Advertising or Offering Collective Investment Schemes on the Internet issued by the SFC.

~~7.12~~7.14 A Platform Operator should implement appropriate access rights and controls such that the public (including retail clients) would not be able to invest in or view materials relating to virtual assets in circumstances that would constitute a breach of the C(WUMP)O or Part IV of the SFO.

Order recording and handling

~~7.13~~7.15 A Platform Operator should record the particulars of all order instructions received from clients.

~~7.14~~7.16 Where order instructions are received from clients through the telephone, a Platform Operator should use a telephone recording system to record the instructions and maintain telephone recordings as part of its records for at least six months.

---

57 Parts II and XII of the C(WUMP)O.

58 Sections 103(2)(a) and 103(11) of the SFO.

~~7.15~~7.17 A Platform Operator should prohibit its staff from receiving client order instructions through mobile phones when they are on the trading floor, in the trading room, in the usual place of business where orders are received or in the usual place where business is conducted, and should have a written policy in place to explain and enforce this prohibition.

~~7.16~~7.18 A Platform Operator should take all reasonable steps to promptly execute client orders in accordance with clients' instructions.

~~7.17~~7.19 A Platform Operator should handle orders of clients fairly and in the order in which they are received.

~~7.18~~7.20 A Platform Operator should not withdraw or withhold client orders for its own convenience or for the convenience of any other person. For the avoidance of doubt, this only applies in respect of market orders and limit orders that can be executed on the platform at the relevant price.

~~7.19~~7.21 A Platform Operator when acting for or with clients should execute client orders on the best available terms.

Trading of virtual assets

~~7.20~~7.22 A Platform Operator should establish and maintain policies and procedures in relation to the trading process to prevent or detect errors, omissions, fraud and other unauthorised or improper activities.

~~7.21~~7.23 A Platform Operator should execute a trade for a client only if there are sufficient fiat currencies or virtual assets in the client's account with the Platform Operator to cover that trade except for any off-platform transactions to be conducted by institutional professional investors in respect of virtual assets which are not issued by (a) the Platform Operator and any corporation within the same group of companies as the Platform Operator or (b) the client and any corporation within the same group of companies as the client concerned ~~to be conducted by institutional professional investors which are settled intra-day~~ and except under permitted circumstances specified by the SFC.

~~7.22~~7.24 Except for the circumstances described in paragraph 7.23 above, a~~A~~ Platform Operator should not provide any financial accommodation[59] for its clients to acquire virtual assets. It should ensure, to the extent possible, that no corporation within the same group of companies as the Platform Operator does so unless for exceptional circumstances which ~~are~~ have been approved by the SFC on a case-by-case basis.

~~7.23~~7.25 A Platform Operator should not conduct any offering, trading or dealing activities in virtual asset futures contracts or related derivatives.

~~7.24~~7.26 A Platform Operator should not:

[59] "Financial accommodation" has the meaning as defined in section 1 of Part 1 of Schedule 1 to the SFO~~This term is defined in section 1 of Part 1 of Schedule 1 to the SFO~~.

(a) provide algorithmic trading services[60] to its clients; ~~or~~

(b) make any arrangements with its clients on using the client virtual assets held by the Platform Operator or its Associated Entity with the effect~~for the purpose~~ of generating returns for the clients or any other parties; or

(c) offer any gift, other than a discount of fees or charges, to its client for the trading of a specific virtual asset.

~~7.25~~7.27 A Platform Operator should prepare comprehensive trading and operational rules governing its platform operations for both on-platform trading and off-platform trading (where applicable). These should, at the minimum, cover the following areas:

(a) trading and operational matters;

(b) trading channels (such as website, dedicated application and application programming interface (API));

(c) trading hours;

(d) different types of orders; detailed description of the functionality and their priorities;

(e) order minimum and maximum quantity limits per underlying currency or virtual asset (in the case of virtual asset trading pairs);

(f) order execution conditions and methodology;

(g) situations in which orders can be amended and cancelled;

(h) trade verification procedures;

(i) arrangements during trading suspension, outages and business resumption, including arrangements during restart before entering continuous trading;

(j) rules preventing market manipulative and abusive activities;

(k) clearing and settlement arrangements;

(l) deposit and withdrawal procedures, including the procedures and time required for transferring virtual assets to a client's private wallet and depositing fiat currencies to a client's bank account when returning client assets to the client;

(m) custodial arrangements, risks associated with such arrangements, the internal controls implemented to ensure that client assets are adequately safeguarded, and insurance/compensation arrangements to protect against any losses arising from the custody of client virtual assets (see paragraphs 10.22 to 10.26 below);

[60] For the purpose of this paragraph, algorithmic trading refers to computer generated trading activities created by a predetermined set of rules aimed at delivering specific execution outcomes.

(n) the internal control procedures which have been put in place to ensure the fair and orderly functioning of its market and to address potential conflicts of interest;

(o) prohibited trading activities, including, but not limited to, churning, pump-and-dump schemes, ramping, wash trading and other market manipulation aimed at creating a false representation of price ~~and/or~~, quantity or both; and

(p) actions the Platform Operator might take should it discover that a client is engaged in prohibited trading activities, including suspension of the client's account, ~~and/or~~ termination of the client's account or both.

Market access

~~7.26~~7.28 If the Platform Operator provides programmable access to its platform through one or multiple channels (API access), thorough and detailed documentation should be provided to clients. This includes, but is not limited to, detailed descriptions and examples for all synchronous and asynchronous interactions and events, as well as all potential error messages. A simulation environment, simulating a reasonable amount of market activity, should be provided for clients to test their applications.

Fair and reasonable charges

~~7.27~~7.29 A Platform Operator should adopt a fee structure that is clear, fair and reasonable in the circumstances, and characterised by good faith. In relation to trading, the Platform Operator should clearly set out how different fees may apply based on the type of order (including whether the client is providing or taking liquidity), transaction size and type of virtual asset transacted (if applicable). In relation to admission of virtual assets for trading, the fee structure (if applicable) should be designed to avoid any potential, perceived or actual conflicts of interest (for example, charging all virtual asset issuers a flat rate for admission).

~~Compliance by Associated Entity~~

~~7.28 If any obligations of the Platform Operator under these Guidelines, the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset Service Providers) and any other applicable regulatory requirements can only be performed together with the Associated Entity or solely by the Associated Entity on behalf of the Platform Operator, the Platform Operator should ensure that its Associated Entity observes such obligations.~~

~~7.29 In any event, the Platform Operator remains primarily responsible for compliance with these Guidelines, the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset Service Providers) and other regulatory requirements applicable to the Platform Operator.~~

VIII. Prevention of Market Manipulative and Abusive Activities

Internal policies and controls

8.1 A Platform Operator should establish and implement written policies and controls for the proper surveillance of trading activities on its trading platform in order to identify, prevent and report any market manipulative or abusive trading activities. The policies and controls should, at a minimum, cover the following:

(a) identifying and detecting anomalies, which includes performing periodic independent reviews of suspicious price spikes;

(b) monitoring and preventing any potential use of abusive trading strategies; and

(c) taking immediate steps to restrict or suspend trading upon discovery of manipulative or abusive activities (for example, temporarily ~~freezing~~ suspending accounts).

8.2 Upon becoming aware of any market manipulative or abusive activities, whether actual or potential, on its trading platform, a Platform Operator should notify the SFC of such matter as soon as practicable, provide the SFC with such additional assistance in connection with such activities as it might request and implement appropriate remedial measures.

Market surveillance system

8.3 In addition to internal market surveillance policies and controls referred to in paragraph 8.1 above, a Platform Operator should adopt an effective market surveillance system provided by a reputable and independent provider to identify, monitor, detect and prevent any market manipulative or abusive activities on its trading platform, and provide access to this system for the SFC to perform its own surveillance functions when required.

8.4 A Platform Operator should review the effectiveness of the market surveillance system provided by the independent provider on a regular basis, at least annually, and make enhancements as soon as practicable to ensure that market manipulative or abusive activities are properly identified. The review report should be submitted to the SFC upon request.

IX. Dealing with Clients

9.1 Where a Platform Operator advises or acts on behalf of a client, it should ensure that any representations made and information provided to the client are accurate and not misleading.

9.2 A Platform Operator should ensure that invitations and advertisements in respect of its services do not contain information that is false, disparaging, misleading or deceptive.

Access to trading services

9.3 A Platform Operator should ensure that it complies with the applicable laws and regulations in the jurisdictions in which it provides services. It should establish and implement measures which include:

~~(a) disclosing to its clients the jurisdictions which do not permit the trading of relevant virtual assets;~~

~~(b)~~(a) ensuring its marketing activities are only conducted in permitted jurisdictions without violation of the relevant restrictions on offers of investments; and

~~(c)~~(b) implementing measures to prevent persons from jurisdictions which have banned trading in virtual assets from accessing its services (for example, by checking IP addresses and blocking access). For the avoidance of doubt, a Platform Operator should also implement appropriate measures to detect and prevent persons who are attempting to circumvent the relevant jurisdictions' ban on trading virtual assets (for example, by using a virtual private network to mask their IP addresses) from accessing its services.

9.4 Except for institutional and qualified corporate professional investors, a Platform Operator should assess the knowledge of the investors in virtual assets (including knowledge of relevant risks associated with virtual assets) before opening an account for them. ~~Where an investor does not possess such knowledge, the~~ The Platform Operator may open an account for an investor who does not possess such knowledge or allow such an investor to access its services, ~~that investor~~ only if the Platform Operator has provided adequate training to the investor.

Note ~~1~~: The following are some criteria (which are not exhaustive) for assessing if an investor can be regarded as having knowledge of virtual assets:

(a) whether the investor has undergone training or attended courses on virtual assets;

(b) whether the investor has current or previous work experience related to virtual assets; or

(c) whether the investor has prior trading experience in virtual assets.

~~Note 2: An investor will be considered to have knowledge of virtual assets if he or she has executed five or more transactions in any virtual assets within the past three years.~~

Know your client

9.5 A Platform Operator should take all reasonable steps to establish the true and full identity of each of its clients, and, except for institutional and qualified corporate professional investors, each client's financial situation, investment experience, and investment objectives. Where an account opening procedure other than a face-to-face approach is used, it should be one that satisfactorily ensures the identity of the client.

Note: The Platform Operator should refer to the SFC's website, circulars and FAQs regarding account opening approaches which the SFC would consider to be acceptable for the purpose of this requirement.

9.6 Except for institutional and qualified corporate professional investors, a Platform Operator should assess a client's risk tolerance level ~~and risk profile~~, accordingly determine the client's risk profile and assess whether it is suitable for the client to participate in the trading of virtual assets. The Platform Operator should exercise due skill, care and diligence to ensure the methodology for risk profiling is properly designed and should determine the client's risk profile based on an assessment of the information about the client obtained through its know-your-client process. The methodology adopted for categorising clients and an explanation of the risk profiles of clients should be made available to the client.

Note: Where risk-scoring questionnaires are used to risk profile clients, the Platform Operator should pay particular attention to the design of the questions and the underlying scoring mechanism, which should be properly designed to accurately reflect the personal circumstances of a client. The Platform Operator should also have appropriate processes in place to periodically review the risk profiling methodology and mechanism for clients.

9.7 Except for institutional and qualified corporate professional investors, a Platform Operator should set a limit for each client to ensure that the client's exposure to virtual assets is reasonable, ~~as determined by the Platform Operator,~~ with reference to the client's financial situation (including the client's net worth) and personal circumstances.

Note 1: When assessing the client's exposure to virtual assets, ~~T~~the Platform Operator should take into account the client's overall holdings in virtual assets (held with the Platform Operator or otherwise) on a best effort basis.

Note 2: The Platform Operator should notify the client of the assigned limit and review this limit regularly to ensure that it remains appropriate.

Client identity: origination of instructions and beneficiaries

9.8 A Platform Operator should be satisfied on reasonable grounds about[61]:

[61] ~~A Platform Operator should interpret this paragraph sensibly in accordance with its spirit and not interpret this paragraph technically or literally.~~ The Platform Operator must satisfy itself about and record information that identifies those who are really behind a transaction: those who ultimately originate instructions in relation to a transaction and those who ultimately

(a) the identity, address and contact details of:

(i) the person or entity (legal or otherwise) ultimately responsible for originating the instruction in relation to a transaction;

(ii) the person or entity (legal or otherwise) that stands to gain the commercial or economic benefit of the transaction ~~and/or~~, bear its commercial or economic risk or both gain the benefit and bear its risks; and

(b) the instruction given by the person or entity referred to in subparagraph (a).

9.9 A Platform Operator should not do anything to effect a transaction unless it has complied with paragraph 9.8 above and kept records in Hong Kong of the details referred to in paragraph 9.8 above.

9.10 In relation to a collective investment scheme or discretionary account, the "entity" referred to in paragraph 9.8 above is the collective investment scheme or account, and the manager of that collective investment scheme or account, not those who hold a beneficial interest in that collective investment scheme or account.

Client agreement

9.11 In conducting any Relevant Activities, a Platform Operator should enter into a written client agreement with each and every client[62] before services are provided to the client. The client agreement should include the following provisions:

(a) the full name and address of the client as verified by a retained copy of the identity card, relevant sections of the passport, business registration certificate, corporation documents, or any other official document which uniquely identifies the client;

(b) the full name and address of the Platform Operator's business including the Platform Operator's licensing status with the SFC and the CE number (being the unique identifier assigned by the SFC);

(c) undertakings by the Platform Operator and the client to notify the other in the event of any material change to the information (as specified in subparagraphs (a), (b), (d) and (e)) provided in the client agreement;

(d) a description of the nature of services to be provided to or available to the client;

(e) a description of any remuneration (and the basis for payment) that is to be paid by the client to the Platform Operator;

(f) the risk disclosure statements as specified in paragraph 9.26 below and Schedule 2 to these Guidelines; and

---

benefit from, or bear the risk of, that transaction. The SFC is concerned about the substance of what is going on with a transaction and not the technicalities.

62 Except for institutional and qualified corporate professional investors.

(g) the following clause:

"*In conducting any Relevant Activities, if we [the Platform Operator] solicit the sale of or recommend any product including any virtual assets to you [the client], the product must be reasonably suitable for you having regard to your financial situation, investment experience and investment objectives. No other provision of this agreement or any other document we may ask you to sign and no statement we may ask you to make derogates from this clause.*"

9.12 The client agreement should be in Chinese or English according to the language preference of the client, as should any other agreement, authority, risk disclosure, or supporting document.

9.13 A Platform Operator should provide a copy of the documents referred to under paragraph 9.12 above to the client and draw the relevant risks to the client's attention. Where an account opening procedure other than a face-to-face approach is used, ~~a copy of these documents should be sent to the client by email and~~ the covering correspondence should specifically direct the client's attention to the appropriate risk disclosure statements.

9.14 A Platform Operator should ensure that it complies with its obligations under a client agreement and that a client agreement does not operate to remove, exclude or restrict any rights of a client or obligations of the Platform Operator under the law.

9.15 A client agreement should properly reflect the services to be provided. Where the services to be provided are limited in nature, the client agreement may be limited accordingly.

9.16 A Platform Operator should not incorporate any clause, provision or term in the client agreement or in any other document signed or statement made by the client at the request of the Platform Operator which is inconsistent with its obligations under these Guidelines. No clause, provision, term or statement should be included in any client agreement (or any other document signed or statement made by the client at the request of the Platform Operator) which misdescribes the actual services to be provided to the client.

Note: This paragraph precludes the incorporation in the client agreement (or in any other document signed or statement made by the client) of any clause, provision or term by which a client purports to acknowledge that no reliance is placed on any recommendation made or advice given by the Platform Operator.

Suitability obligations

9.17 A Platform Operator should perform all reasonable due diligence on the virtual assets before making them available to clients (see paragraph 7.6~~5~~ above) and provide sufficient and up-to-date information on the nature, features and risks of these virtual assets (see also paragraph 9.27(d) below) on its website in order to enable clients to understand them before making an investment decision. ~~Where a Platform Operator posts any product-specific materials on the platform, it should ensure that such materials are factual, fair and balanced.~~

9.18 Where a Platform Operator posts any product-specific materials (whether on the platform or off the platform), it should ensure that such materials are factual, fair and balanced. For the avoidance of doubt, the ~~A~~ Platform Operator should not post any advertisement in connection with a specific virtual asset.

9.19 ~~The~~ A Platform Operator may engage in off-platform trading activities as part of its Relevant Activities.

9.20 Except for dealing with institutional and qualified corporate professional investors, a Platform Operator should, when making a recommendation or solicitation, ensure the suitability of the recommendation or solicitation for the client is reasonable in all the circumstances having regard to information about the client of which the Platform Operator is or should be aware through the exercise of due diligence.

Note 1: The question of whether there has been a "solicitation" or "recommendation" triggering the suitability requirement is a question of fact which should be assessed in light of all the circumstances leading up to the point of sale or advice.

A Platform Operator should refer to guidance published by the SFC (which may be updated from time to time) on the circumstances under which the suitability requirement would likely or unlikely be regarded as being triggered.

Note 2: The context (such as the manner of presentation) and content of product-specific materials posted on the platform ~~and/ or~~, its website or both coupled with the design and overall impression created by the content of the platform, ~~/~~ website or both would determine whether the suitability requirement is triggered.

The posting of factual, fair and balanced product-specific materials would not in itself amount to a solicitation or recommendation and would not trigger the suitability requirement. This is so in the absence of other circumstances ~~that~~ which amount to a solicitation or recommendation ~~in~~ of a particular virtual asset. This would occur, for example, where the Platform Operator emphasises some virtual assets over others or there have been interactive one-to-one communications involving solicitations or recommendations through the platform.

A Platform Operator should refer to guidance published by the SFC (which may be updated from time to time) on how the posting of materials on the platform would or would not trigger the suitability requirement.

9.21 In discharging its suitability obligations, a Platform Operator should also note in particular (but not exclusively) the following where applicable:

(a) The Platform Operator should establish a proper mechanism to assess the suitability of virtual assets for clients. Such mechanism should be holistic (ie, all relevant factors concerning the personal circumstances of a client, including concentration risk, should be taken into account).

(b) The Platform Operator should match the risk return profile of the recommended virtual asset with the personal circumstances of the client. This may involve:

(i) rRisk profiling the client (see paragraph 9.6 above). The Platform Operator should have appropriate processes in place to periodically review and update (where appropriate[63]) the individual risk profile of a client; and

(ii) rRisk profiling the virtual asset. The Platform Operator should ascertain the risk return profile of the virtual asset and accordingly assign a risk profile to the virtual asset. The Platform Operator should exercise due skill, care and diligence to ensure the risk profiling methodology it uses is properly designed to take into account both quantitative and qualitative factors and consider all risks involved and should make available on the platform information on about the methodology adopted (including an explanation on the risk profile of the virtual assets) on the platform. The Platform Operator should have appropriate processes in place to periodically review the risk profiling methodology and mechanism for virtual assets and the risk profiles of virtual assets.

NotwithstandingHowever, it should be noted that merely matching a virtual asset's risk rating mechanically with a client's risk tolerance level may not be sufficient to discharge the suitability obligation; .

(c) The Platform Operator should have in place appropriate tools for assessing a client's concentration risk and such an assessment should be based on the information about the client obtained by the Platform Operator; .

(d) The Platform Operator should act diligently and carefully in providing any advice and ensuring that advice and recommendations are based on thorough analysis and take into account available alternatives; and .

(e) The Platform Operator should ensure that any conflicts of interest are properly managed and minimised to ensure that clients are fairly treated, for example, the Platform Operator should not take commission rebates or other benefits as the primary basis for soliciting or recommending a particular virtual asset to clients.

9.22 Except for dealing with institutional and qualified corporate professional investors, subject to paragraph 9.23 below, a Platform Operator should ensure that a transaction in a complex product is suitable for the client in all the circumstances. The Platform Operator should also ensure that there are prominent and clear warning statements to warn clients about a complex product prior to and reasonably proximate to the point of sale or advice.

Note 1: "Complex product" refers to a virtual asset whose terms, features and risks are not reasonably likely to be understood by a retail investor because of its

[63] For example, this may not apply to a dormant client account.

complex structure. The factors to determine whether a virtual asset is complex or not are set out below:

(a) whether the virtual asset is a derivative product;

(b) whether a secondary market is available for the virtual asset at publicly available prices;

(c) whether there is adequate and transparent information about the virtual asset available to retail investors;

(d) whether there is a risk of losing more than the amount invested;

(e) whether any features or terms of the virtual asset could fundamentally alter the nature or risk of the investment or pay-out profile or include multiple variables or complicated formulas to determine the return[64]; and

(f) whether any features or terms of the virtual asset might render the investment illiquid ~~and/or~~, difficult to value or both.

Note 2: The Platform Operator should determine whether a virtual asset may be treated as non-complex or complex with due skill, care and diligence. In making such determination, the Platform Operator should have regard to the factors set out in Note 1 and refer to the guidance issued by the SFC from time to time for examples of complex products.

9.23 For orders in virtual assets (including virtual assets classified as complex products) which are ~~traded~~ placed by the client directly on the platform, ~~where there has been no solicitation or recommendation,~~ a Platform Operator is not required to comply with paragraphs 9.21 and 9.22 above for such transactions if there has been no solicitation or recommendation made by the Platform Operator~~in such products executed on the platform, although it must still comply with paragraphs 9.5 to 9.7 above~~.

Opening of multiple accounts

9.24 A Platform Operator should not allow a single client to open multiple accounts, unless in the form of sub-accounts.

Disclosure

9.25 When posting any information and materials on its platform and providing any information to clients, ~~A~~ a Platform Operator should act with due skill, care and diligence ~~when posting any information and materials on its platform and providing any information to clients. The Platform Operator should~~ to ensure that all information is accurate, presented in a clear and fair manner which is not misleading and communicated in an easily comprehensible manner.

[64] This would include, for example, investments that incorporate a right for the issuer to convert the instrument into a different investment.

9.26 Except for dealing with institutional and qualified corporate professional investors, a Platform Operator should take all reasonable steps to ~~fully~~ disclose, in a prominent manner, the nature and risks that clients may be exposed to in trading virtual assets and using the Platform Operator's virtual asset trading services (including the disclosures set out in Schedule 2 to these Guidelines). ~~The disclosed risks should, amongst other things, include:~~

~~(a) virtual assets are highly risky and investors should exercise caution in relation to the products;~~

~~(b) a virtual asset may or may not be considered "property" under the law, and such legal uncertainty may affect the nature and enforceability of a client's interest in such a virtual asset;~~

~~(c) the offering documents or product information provided by the issuer have not been subject to scrutiny by any regulatory body;~~

~~(d) the protection offered by the Investor Compensation Fund does not apply to transactions involving virtual assets (irrespective of the nature of the tokens);~~

~~(e) a virtual asset is not a legal tender, ie, it is not backed by the government and authorities;~~

~~(f) transactions in virtual assets may be irreversible, and, accordingly, losses due to fraudulent or accidental transactions may not be recoverable;~~

~~(g) the value of a virtual asset may be derived from the continued willingness of market participants to exchange fiat currency for a virtual asset, which means that the value of a particular virtual asset may be completely and permanently lost should the market for that virtual asset disappear. There is no assurance that a person who accepts a virtual asset as payment today will continue to do so in the future;~~

~~(h) the extreme volatility and unpredictability of the price of a virtual asset relative to fiat currencies may result in a total loss of the investment over a short period of time;~~

~~(i) legislative and regulatory changes may adversely affect the use, transfer, exchange and value of virtual assets;~~

~~(j) some virtual asset transactions may be deemed to be executed only when recorded and confirmed by the Platform Operator, which may not necessarily be the time at which the client initiates the transaction;~~

~~(k) the nature of virtual assets exposes them to an increased risk of fraud or cyberattack; and~~

~~(l) the nature of virtual assets means that any technological difficulties experienced by the Platform Operator may prevent clients from accessing their virtual assets.~~

9.27 A Platform Operator should, at a minimum, ~~also~~ make the following information available on its website:

(a) adequate and appropriate information about its business, including contact details and services available to clients;

(b) its trading and operational rules as well as token admission and removal rules and criteria (including the criteria for admitting, suspending and withdrawing a virtual asset for or from trading and the "acceptable indices" referenced by the Platform Operator for admitting a virtual asset for trading by retail clients (if applicable));

(c) its admission (for example, the fees charged to issuers for admitting their virtual assets for trading on the platform as set out in paragraph 7.29 above) and trading fees and charges, including illustrative examples of how the fees and charges are calculated~~, for ease of understanding by clients~~;

(d) the relevant ~~material~~ information for each virtual asset admitted for trading to enable clients to appraise the position of their investments;

(e) the rights and obligations of the Platform Operator and the client under the client agreement (see paragraph 9.11 above);

(f) arrangements for dealing with settlement failures in respect of transactions executed on its platform;

(g) detailed documentation of market models, order types and trading rules as well as deposit and withdrawal processes for fiat currencies and virtual assets (where applicable);

(h) if API access is offered, detailed documentation regarding different connectivity channels, all synchronous and asynchronous requests and responses, market events, error messages and all other messages. The documentation should also include detailed examples for each of these matters;

(i) detailed documentation regarding the simulation environment as well as constant and active simulated quote and order feed into the simulation environment;

(j) client's liability for unauthorised virtual asset transactions;

(k) client's right to stop payment of a preauthorised virtual asset transfer and the procedure for initiating such a stop-payment order;

(l) circumstances under which the Platform Operator may disclose the client's personal information to third parties, including regulators and auditors;

(m) client's right to prior notice of any change in the Platform Operator's rules, procedures or policies;

(n) dispute resolution mechanisms, including complaints procedures;

(o) system upgrades and maintenance procedures and schedules; and

(p) the types of services that would only be available to professional investors.

Where the Platform Operator makes any revisions or updates, it should, as soon as practicable thereafter, publish them on its website and circulate them to its clients. The Platform Operator should also identify the material amendments which have been made and provide an explanation for making them.

9.28 In respect of the posting of information for each virtual asset in paragraph 9.27(d) above, the ~~following~~ types of information which are considered relevant ~~and material~~ include:

(a) ~~P~~price and trading volume of the virtual asset on the platform, for example, in the last 24-hours and since its admission for trading on the platform;

(b) ~~B~~background information about the management or development team ~~management team or developer~~ of the virtual asset or any of its known key members (if any);

(c) ~~I~~issuance date of the virtual asset (if any);

(d) ~~Brief description of the~~ material terms and features of the virtual asset;

(e) affiliation of the Platform Operator with the issuer of the virtual asset and the management or development team (or any of its known key members) of the virtual asset (if any);

~~(e)~~(f) ~~L~~link to the virtual asset's official website and Whitepaper (if any);

~~(f)~~(g) ~~L~~link to the smart contract audit report and other bug reports of the virtual asset (if any); and

~~(g)~~(h) ~~W~~where the virtual asset has voting rights, how those voting rights will be handled by the Platform Operator.

9.29 In respect of posting any product-specific materials and other materials on the platform, a Platform Operator should take all reasonable steps to ensure that the information does not contain information that is false, biased, misleading or deceptive.

9.30 A Platform Operator should, upon request, disclose the financial condition of its business to a client by providing a copy of the latest audited balance sheet and profit and loss account required to be filed with the SFC, and disclose any material changes which adversely affect the Platform Operator's financial condition after the date of the accounts.

Provision of prompt confirmation to clients

9.31 Prior to the execution of each transaction in virtual assets, a Platform Operator should confirm with its clients the following terms:

(a) name of the virtual asset in the proposed transaction;

(b) amount or value of the proposed transaction;

(c) fees and charges to be borne by the client including applicable exchange rates; and

(d) a warning that once executed the transaction may not be undone.

9.32 After a Platform Operator has effected a transaction for a client, it should confirm promptly with the client the essential features of the transaction. The following information should be included:

(a) name of the virtual asset in the transaction;

(b) amount or value of the transaction; and

(c) fees and charges borne by the client including applicable exchange rates.

Provision of contract notes, statements of account and receipts to clients

9.33 A Platform Operator should provide to each client timely and meaningful information about the transactions conducted with the client or on the client's behalf, the client's holdings and movements of client virtual assets and fiat currencies, and other activities in the client's account. Where contract notes, statements of account and receipts are provided by a Platform Operator to a client, the Platform Operator should ensure that the information included in the contract notes, statements of account and receipts is fit for purpose, comprehensive and accurate in respect of the particular type of virtual asset involved. In particular:

Contract notes

(a) Where a Platform Operator enters into a relevant contract with or on behalf of a client, it must prepare and provide a contract note to the client no later than the end of the second business day after entering into the relevant contract. The term "*relevant contract*" means a contract, entered into by ~~a~~ the Platform Operator with or on behalf of a client in the conduct of its businesses which constitute any Relevant Activity, that is a contract for dealing in virtual assets.

(b) Where a Platform Operator enters into more than one relevant contract with or on behalf of a client on the same day, unless the client has given contrary instructions to the Platform Operator, the Platform Operator may prepare a single contract note which:

(i) records all of those relevant contracts; and

(ii) in respect of each of those relevant contracts includes all of the information which would have been required to be included in the contract note.

If such a single contract note is prepared, the Platform Operator should provide it to the client no later than the end of the second business day after entering into those relevant contracts.

(c) A contract note should include, to the extent applicable, the following information:

(i) the name under which the Platform Operator carries on business;

(ii) the name and account number of the client;

(iii) full particulars of the relevant contract including:

(I) the quantity, name, description and such other particulars of the virtual asset involved, as are sufficient to enable it to be identified;

(II) the nature of the dealing;

(III) where the Platform Operator is acting as principal, an indication that it is so acting;

(IV) the date (i) on which the relevant contract is entered into; (ii) of settlement or performance of the relevant contract; and (iii) on which the contract note is prepared;

(V) the price per unit of the virtual asset traded;

(VI) the rate or amount of fees and charges payable in connection with the relevant contract; and

(VII) the amount of consideration payable under the relevant contract.

Monthly statements of account

(d) Where any of the following circumstances applies, a Platform Operator should prepare and provide a monthly statement of account to the client no later than the end of the seventh business day after the end of the monthly accounting period:

(i) during a monthly accounting period, the Platform Operator is required to prepare and provide to the client a contract note or receipt;

(ii) at any time during a monthly accounting period, the client has an account balance that is not nil; or

(iii) at any time during a monthly accounting period, any client virtual assets are held for the account of the client.

(e) Where a Platform Operator is required to prepare a monthly statement of account, it should include the following information:

(i) the name under which the Platform Operator carries on business;

(ii) the name, address and account number of the client to whom the Platform Operator is required to provide the statement of account;

(iii) the date on which the statement of account is prepared; and

(iv) where the client assets of a client to whom the Platform Operator is required to provide the statement of account are held for the client's account by the Associated Entity, the name under which the Associated Entity carries on business.

(f) A Platform Operator should also include, to the extent applicable, the following information in the monthly statement of account:

(i) the address of the Platform Operator's principal place of business in Hong Kong;

(ii) the outstanding balance of that account as at the beginning and as at the end of that monthly accounting period and details of all movements in the balance of that account during that period;

(iii) details of all relevant contracts entered into by the Platform Operator with or on behalf of the client during that monthly accounting period, indicating those initiated by the Platform Operator;

(iv) details of all movements during that monthly accounting period of any client virtual assets held for that account;

(v) the quantity, and, in so far as readily ascertainable, the market price and market value of each client virtual asset held for that account as at the end of that monthly accounting period; and

(vi) details of all income credited to and charges levied against that account during that monthly accounting period.

Duty to provide statements of account upon request

(g) Where a Platform Operator receives a request from a client for a statement of account as of the date of the request, it should:

(i) prepare a statement of account in respect of the client which includes the information required for all statements of account (see subparagraph (e)) and, to the extent applicable, the following information relating to the account of the client as of the date of the request:

(I) the outstanding balance of that account; and

(II) the quantity, and, in so far as readily ascertainable, the market price and market value of each client virtual asset, held for that account~~.~~; and

(ii) provide the statement of account to the client as soon as practicable after the date of the request.

Receipts

(h) On each occasion that a Platform Operator or its Associated Entity receives any client assets from or on behalf of a client, the Platform Operator or its Associated Entity should prepare and provide a receipt to the client no later than the end of the second business day after receiving the client assets.

(i) The requirement under subparagraph (h) is not applicable in the following circumstances:

(i) where client money is deposited directly into the bank account of a Platform Operator or its Associated Entity, by the client or on behalf of the client by any person other than the Platform Operator or its Associated Entity; or

(ii) where a contract note or other trade document provided to the client expressly states that it also serves as a receipt and includes the information specified in subparagraph (j).

(j) A Platform Operator should include the following information in the receipt:

(i) the name under which the Platform Operator or its Associated Entity (as the case may be) carries on business;

(ii) the date on which the receipt is prepared;

(iii) the name and account number of the client; and

(iv) in respect of the client assets received:

(I) the quantity, description and such other particulars of the client assets as are sufficient to enable them to be identified;

(II) the account into which they have been deposited; and

(III) the date on which they were received.

Miscellaneous

(k) Where a Platform Operator or its Associated Entity receives a request from a client for a copy of any contract note, statement of account or receipt that the Platform Operator or its Associated Entity was required to provide to the client, the Platform Operator should, as soon as practicable after receiving the request, provide the copy to the client. A Platform Operator may impose a reasonable charge for a copy of a document provided by it under this subparagraph.

(l) If, on an application made by a client, the SFC so directs, the Platform Operator should make available for inspection by the client during the ordinary business hours of the Platform Operator a copy of any contract note, statement of account or receipt, except for those dated after the expiration of the period for which the Platform Operator or its Associated Entity is required to retain them.

(m) Where a Platform Operator is required to prepare any contract note, statement of account or receipt, the Platform Operator should prepare it in the Chinese or English language as preferred by the client to whom it is intended to be provided.

(n) Any contract note, statement of account or receipt (or any copy of any such document) required to be provided to a client should for all purposes be regarded as duly provided to the client if it is served on:

(i) the client; or

(ii) any other person (except an officer or employee of the Platform Operator or the Associated Entity which is required to provide the document to the client) designated by the client for the purposes of this subparagraph by notice in writing to the Platform Operator or the Associated Entity that is required to provide the document to the client~~.~~,

and it is:

(I) delivered to the person by hand;

(II) left at (where applicable), or sent by post to the person's address;

(III) sent by facsimile transmission to the person's last known facsimile number;

(IV) sent by electronic mail transmission to the person's last known electronic mail address; or

(V) provided to the person by access through the Platform Operator's website.

~~(o) A Platform Operator should ensure that it has obtained consent from its clients and put in place adequate operational safeguards if any contract note, statement of account or receipt required to be provided to a client is provided by accessing its website.~~

X. Custody of Client Assets

Handling of client virtual assets and client money

10.1 A Platform Operator should only hold client assets on trust for its clients through ~~the~~ its Associated Entity. The Associated Entity should not conduct any business other than that of receiving or holding client assets on behalf of the Platform Operator.

10.2 In the handling of client transactions and client assets (ie, client money and client virtual assets), a Platform Operator should act to ensure that client assets are accounted for properly and promptly. Where the Platform Operator or its Associated Entity is in possession or control of client assets, the Platform Operator should ensure that client assets are adequately safeguarded.

10.3 A Platform Operator should have, and should also ensure that its Associated Entity has, appropriate and effective procedures to protect the client assets from theft, fraud and other acts of misappropriation. In particular, the Platform Operator and its Associated Entity should ensure that the authority of the Platform Operator, its Associated Entity and their staff to acquire, dispose of and otherwise move or utilise ~~its~~ client assets is clearly defined and followed.

10.4 A Platform Operator should have, and should also ensure that its Associated Entity has, a robust process to prepare, review and approve reconciliations of client assets in a timely and efficient manner to identify and highlight for action any errors, omissions or misplacements of client assets. Reconciliations should be checked and reviewed by appropriate staff members, and material discrepancies and long outstanding differences should be escalated to senior management on a timely basis for appropriate action.

Client virtual assets

10.5 A Platform Operator should ensure that all client virtual assets are properly safeguarded and held in wallet address(es) which are established by its Associated Entity and are designated for the purpose of holding client virtual assets. The Platform Operator should ensure that client virtual assets are segregated from the assets of the Platform Operator ~~or~~ and its Associated Entity. The Platform Operator should ensure the Associated Entity's compliance with this requirement.

10.6 A Platform Operator should establish and implement, and should also ensure that its Associated Entity establishes and implements, written internal policies and governance procedures which include, but are not limited to, the following:

(a) The Platform Operator and its Associated Entity should hold virtual assets that are the same as those virtual assets which are owed to or held on behalf of its clients and in the same amount~~Virtual assets are held of the same type and amount as those which are owed or belong to its client;~~.

(b) Subject to paragraph 7.26(b) above, t~~T~~he Platform Operator and its Associated Entity should not deposit, transfer, lend, pledge, repledge or otherwise deal with or create any encumbrance over the virtual assets of a client except for the settlement of transactions, and fees and charges owed by the client to the Platform Operator in respect of the Relevant Activities carried

out by the Platform Operator on behalf of the client or in accordance with the client's ~~written instructions (including~~ standing authorities (see paragraph 10.17 below) or one-off written directions~~);~~.

(c) The Platform Operator and its Associated Entity should store 98% of client virtual assets in cold storage (such as Hardware Security Module (HSM)-based cold storage) except under limited circumstances permitted by the SFC on a case-by-case basis to minimise exposure to losses arising from a compromise or hacking of the platform~~);~~.

(d) The Platform Operator and its Associated Entity should minimise transactions out of the cold storage in which a majority of client virtual assets are held~~;~~.

(e) The Platform Operator and its Associated Entity should have detailed specifications for how access to cryptographic devices or applications is to be authorised and validated, covering key generation, distribution, storage, use and destruction~~;~~.

(f) The Platform Operator and its Associated Entity should document in detail the mechanism for the transfer of virtual assets between hot, cold and other storages. The scope of authority of each function designated to perform any non-automated process in such transfers should be clearly specified~~; and~~.

(g) The Platform Operator and its Associated Entity should have detailed procedures for how to deal with events such as voting, hard forks or airdrops from an operational and technical point of view.

10.7 A Platform Operator should not conduct any deposits and withdrawals of client virtual assets through any wallet address other than an address which belongs to the client and is whitelisted by the Platform Operator, except under permitted circumstances specified by the SFC. The Platform Operator should ensure the Associated Entity's compliance with this requirement.

10.8 A Platform Operator should establish and implement strong internal controls and governance procedures for private key management to ensure all cryptographic seeds and private keys are securely generated, stored and backed up. The Platform Operator should ensure that the Associated Entity establishes and implements the same controls and procedures. These will include the following:

(a) The generated seeds and private keys must be sufficiently resistant to speculation or collusion. The seeds and private keys should be generated in accordance with applicable international security standards and industry best practices so as to ensure that the seeds (where Hierarchical Deterministic Wallets, or similar processes, are used) or private keys (if seeds are not used) are generated in a non-deterministic manner which ensures randomness and thus are not reproducible. Where practicable, seeds and private keys should be generated offline and kept in a secure environment~~-~~, such as a ~~Hardware Storage Module (~~HSM~~)~~, with appropriate certification for the lifetime of the seeds or private keys.

(b) Detailed specifications for how access to cryptographic devices or applications is to be authorised and validated, covering key generation, distribution, use, ~~and~~ storage and destruction, as well as the immediate revocation of a

signatory's access as required. Where practicable, multi-factor authentication is used to authenticate authorised personnel for access to applications governing the use of private keys.

(c) Access to seeds and private keys relating to client virtual assets is tightly restricted amongst authorised personnel who have undergone appropriate screening and training, no single person has possession of information on or access to the entirety of the seeds, private keys or backup passphrases, and controls are implemented to mitigate the risk of collusion amongst authorised personnel.

(d) Distributed backups of seeds or private keys are kept so as to mitigate any single point of failure. The backups need to be distributed in a manner such that an event affecting the primary location of the seeds or private keys does not affect the backups. The backups should be stored in a protected form on external media (preferably HSM with appropriate certification). Distributed backups should be stored in a manner that ensures seeds or private keys cannot be re-generated based solely on the backups stored in the same physical location. Access control to the backups needs to be as stringent as access control to the original seeds or private keys.

(e) Seeds and private keys are securely stored in Hong Kong.

10.9 A Platform Operator should assess the risks posed to each storage method in view of the new developments in security threats, technology and market conditions and implement appropriate storage solutions to ensure the secure storage of client virtual assets. The Platform Operator should also ensure that its Associated Entity implements the same. In particular, the Platform Operator should keep, and should ensure that its Associated Entity keeps, the wallet storage technology up-to-date and in line with international best practices or standards. Wallet storage technology and any upgrades should be fully tested before deployment to ensure reliability and security. The Platform Operator should implement, and should ensure that its Associated Entity implements, measures to deal with any compromise or suspected compromise of all or part of any seed or private key without undue delay, including the transfer of all client virtual assets to a new storage location as appropriate.

10.10 A Platform Operator should have, and should ensure that its Associated Entity has, adequate processes in place for handling deposit and withdrawal requests for client virtual assets to guard against losses arising from theft, fraud and other dishonest acts, professional misconduct or omissions:

(a) ~~T~~the Platform Operator should continuously monitor ~~major~~ developments (such as technological changes or the evolution of security threats) relevant to all virtual assets included for trading. Clear processes should be in place to evaluate the potential impact and risks of these developments, as well as for handling fraud attempts specific to distributed ledger technology (such as 51% attacks), and these processes should be proactively executed;

(b) ~~T~~the Platform Operator and its Associated Entity should monitor ~~ensure that~~ client IP addresses to identify and follow up on potential deposit or withdrawal instructions that are not originated from the client;

(c) the Platform Operator and its Associated Entity should also ensure that ~~as well as~~ wallet addresses used for deposit and withdrawal are whitelisted, using appropriate ~~confirmation~~ methods (for example, verify a client owns a wallet address via proof of ownership test such as message signing or micropayment test~~such as two-factor authentication and separate email confirmation~~);

~~(c)~~(d) ~~T~~the Platform Operator and its Associated Entity should have clear processes in place to minimise the risks involved with handling deposits and withdrawals, including whether deposits and withdrawals are performed using hot ~~or~~, cold or other storages, whether withdrawals are processed ~~constantly~~real time or only at certain cut-off times, whether there are transaction size limits and hourly/daily velocity limits, ~~and~~ whether the withdrawal process is automatic or involves manual authorisation, and when to suspend irregular deposits and withdrawals to conduct investigations;

~~(d)~~(e) ~~T~~the Platform Operator and its Associated Entity should ensure that any decision to suspend the withdrawal of client virtual assets is made on a transparent and fair basis, and the Platform Operator will inform the SFC and all its clients without delay; and

~~(e)~~(f) ~~T~~the Platform Operator and its Associated Entity should ensure that the above processes include safeguards against fraudulent requests or requests made under duress as well as controls to prevent one or more officers or employees from transferring assets to wallet addresses other than the client's designated wallet address. The Platform Operator and its Associated Entity should ensure that destination addresses of client withdrawal instructions cannot be modified before the transactions are signed and broadcasted to the respective blockchain.

Client money

10.11 A Platform Operator should properly handle and safeguard client money and ensure that its Associated Entity does the same. This includes but is not limited to the following:

(a) Establishing one or more segregated accounts by the Associated Entity with an authori~~s~~zed financial institution in Hong Kong or another bank in another jurisdiction as agreed by the SFC from time to time.

(b) Within one business day after the Platform Operator or its Associated Entity receives any client money, the Platform Operator or its Associated Entity should:

(i) ~~P~~pay it into a segregated account maintained with an authori~~s~~zed financial institution in Hong Kong ~~if the client money is received in Hong Kong or in any other jurisdiction~~;

(ii) ~~P~~pay it into a segregated account maintained with another bank in another jurisdiction as agreed by the SFC from time to time if the client money is received outside Hong Kong;

(iii) ~~P~~pay it to the client from whom or on whose behalf it has been received; or

(iv) ~~P~~pay it in accordance with the client's ~~written instructions (including a~~ standing authority (see paragraph 10.17 below) or ~~a~~ one-off written ~~instruction~~direction~~)~~.

(c) No client money should be paid, or permitted to be paid, to:

(i) any officers or employees of the Platform Operator or its Associated Entity; or

(ii) any officer or employee of any corporation with which the Platform Operator is in a controlling entity relationship or in relation to which its Associated Entity is a linked corporation[65],

unless that officer or employee is the client of the Platform Operator from whom or on whose behalf such client money has been received or is being held.

(d) No client money should be paid out of a segregated account other than for (i) paying the client on whose behalf it is being held; (ii) meeting the client's settlement obligations in respect of dealings in virtual assets carried out by the Platform Operator for the client, being the client on whose behalf it is being held; (iii) paying money that the client, being the client on whose behalf it is being held, owes to the Platform Operator in respect of the conduct of Relevant Activities; or (iv) paying in accordance with the client's ~~written instructions, including~~ standing authority~~ies~~ (see paragraph 10.17 below) or one-off written direction~~s~~.

10.12 Subject to paragraph 10.13 below, any amount of interest derived from the holding of client money in a segregated account should be dealt with in accordance with paragraph 10.11 above.

10.13 A Platform Operator should ensure that any amount of interest retained in a segregated account which the Platform Operator or its Associated Entity is entitled to retain under an agreement in writing with a client of the Platform Operator, being the client on whose behalf the client money is being held, should be paid out of the account within one business day after:

(a) the interest is credited to the account; or

(b) the Platform Operator or its Associated Entity becomes aware that the interest has been credited to the account,

whichever is later.

10.14 A Platform Operator or its Associated Entity which becomes aware that it is holding an amount of money in a segregated account that is not client money shall, within

[65] "Linked corporation", in relation to the Associated Entity, means a corporation: (a) of which the Associated Entity is a controlling entity; (b) which is a controlling entity of the Associated Entity; or (c) which has as its controlling entity a person which is also a controlling entity of the Associated Entity.

one business day of becoming so aware, pay that amount of money out of the segregated account.

10.15 A Platform Operator should not deposit and withdraw client money through any bank account other than the account which is opened in the name of the client and designated by the client for this purpose, except under permitted circumstances specified by the SFC. The Platform Operator should ensure the Associated Entity's compliance with this requirement.

10.16 A Platform Operator should use, and should also ensure that its Associated Entity uses, its best endeavours to match any unidentified receipts in its bank accounts (including segregated accounts) with all relevant information in order to establish the nature of any receipt and the identity of the person who has made it.

(a) Upon ascertaining that a receipt represents client money, the amount should be transferred into a segregated account within one business day, even if it has not been able to identify which specific client has made the payment.

(b) Where the receipt is not client money, within one business day of becoming so aware, that amount of money should be paid out of the segregated account.

Standing authority to deal with client assets

10.17 A ~~Standing~~ standing authority is a written instruction that is given to a Platform Operator or its Associated Entity which:

(a) authorises the Platform Operator or its Associated Entity to deal with client assets from time to time received from or on behalf of or held on behalf of the client, in one or more specified ways;

(b) specifies a period not exceeding 12 months during which it is valid. This does not apply to a standing authority which is given to the Platform Operator or its Associated Entity by a client of the Platform Operator who is a professional investor; and

(c) specifies the manner in which it may be revoked.

10.18 A standing authority which is not revoked prior to its expiry:

(a) may be renewed for one or more further periods:

(i) not exceeding 12 months, if the client of the Platform Operator who gave it is not a professional investor; or

(ii) of any duration, if the client of the Platform Operator who gave it is a professional investor,

at any one time, with the written consent of the client of the Platform Operator who gave it; or

(b) shall be deemed to have been renewed if:

(i) at least 14 days prior to the expiry of the standing authority, the Platform Operator or its Associated Entity to which it was given gives a written notice to the client of the Platform Operator who gave the standing authority, reminding the client of its impending expiry, and informing the client that unless the client objects, it will be renewed upon expiry upon the same terms and conditions as specified in the standing authority and for:

(I) an equivalent period to that specified in the standing authority;

(II) any period not exceeding 12 months specified by the Platform Operator or its Associated Entity, if the client of the Platform Operator is not a professional investor; or

(III) a period of any duration specified by the Platform Operator or its Associated Entity, if the client of the Platform Operator is a professional investor; and

(ii) the client does not object to the renewal of the standing authority before its expiry.

Where a standing authority is deemed to have been renewed in accordance with subparagraph (b), the Platform Operator or its Associated Entity (as the case may be) shall give a written confirmation of the renewal of the standing authority to the client of the Platform Operator within one week after the date of expiry.

Disclosure to clients

10.19 A Platform Operator should fully disclose to its clients the custodial arrangements in relation to client assets held on their behalf, including the rights and obligations of each party and how client assets are stored. This should include:

(a) Client virtual assets may not enjoy the same protection as that conferred on "securities" under the SFO, the Securities and Futures (Client Securities) Rules (Cap. 571H) and the Securities and Futures (Client Money) Rules (Cap. 571I)~~;~~;

(b) Where the client money is received or held overseas, such assets may not enjoy the same protection as that conferred on client money received or held in Hong Kong~~;~~;

(c) How the Platform Operator and its Associated Entity will compensate its clients in the event of hacking or any other loss of client virtual assets caused by the default of the Platform Operator or its Associated Entity~~; and~~;

(d) The treatment of client virtual assets and their respective rights and entitlements when events such as, but not limited to, voting, hard forks and airdrops occur. Upon becoming aware of such events, the Platform Operator should notify its clients as soon as practicable.

Ongoing monitoring

10.20 A Platform Operator should assign designated staff member(s) to conduct regular internal audits to monitor its compliance with the requirements for custody of client assets, and its established policies and procedures in respect of handling of these assets. The designated staff member(s) should report to the senior management of the Platform Operator as soon as practicable upon becoming aware of any non-compliance.

10.21 A Platform Operator should closely monitor account activities to check if there are inactive or dormant accounts. It should establish internal procedures as to how deposits and withdrawals of client assets in these accounts should be handled.

Insurance ~~/~~ compensation arrangement

10.22 A Platform Operator should have in place a compensation arrangement approved by the SFC to cover potential loss[66] of 50% of client virtual assets in cold storage and 100% of client virtual assets in hot and other storages ~~provide an appropriate level of coverage for risks associated with the custody of client virtual assets~~ held by its Associated Entity (referred to as the "Compensated Amount")~~(for example, hacking incidents on the platform or default on the part of the Platform Operator or its Associated Entity)~~. The arrangement should include any or a combination of the options below:

(a) ~~T~~third-party insurance; ~~and~~

(b) ~~F~~funds (held in the form of a demand deposit or time deposit which will mature in ~~6~~six months or less) or virtual assets of the Platform Operator or any corporation within the same group of companies as the Platform Operator which are set aside on trust and designated for such a purpose~~.~~; and

(c) bank guarantee provided by an authorized financial institution in Hong Kong.

Any subsequent changes in the compensation arrangement should be pre-approved by the SFC.

10.23 A Platform Operator should establish, implement and enforce internal controls and procedures to monitor on a daily basis the total value of client virtual assets under custody and ascertain whether the compensation arrangement continues to comply with paragraph 10.22 above.

10.24 Where a Platform Operator becomes aware that the total value of the Compensated Amount ~~client virtual assets under custody~~ exceeds the covered amount under the compensation arrangement and the Platform Operator anticipates such a situation to persist, the Platform Operator should notify the SFC, and take prompt remedial measures to ensure compliance with the requirement under paragraph 10.22 above.

10.25 Where a Platform Operator adopts the option of setting aside ~~funds to satisfy the requirement under paragraph 10.22 above, :~~

[66] Potential loss may arise from, amongst other things, hacking incidents on the platform, theft, fraud, or default on the part of the Platform Operator or its Associated Entity (whether or not as a result of its acts, errors, omissions, or gross negligence).

(a) funds, it should ensure that such funds are set aside appropriately, including ~~held on trust and designated for such a purpose~~:

(i) where the funds are held in a manner controlled by the Platform Operator or its Associated Entity,~~.~~ ~~The~~ the funds should ~~also~~ be held in an segregated account with an authorized financial institution and segregated from ~~the~~ any assets of the Platform Operator, its Associated Entity and any corporation within the same group of companies as the Platform Operator and any client assets; and ~~of the Platform Operator or its Associated Entity or any corporation within the same group of companies as the Platform Operator.~~

(ii) where the funds are held in a manner controlled by an independent third party (for example, a trust or company service provider licensed under the AMLO), the Platform Operator should provide the SFC with such party's written acknowledgement of the designated purpose of such funds and such party should disclose information relating to such funds at the SFC's request.

(b) virtual assets, it should ensure that such virtual assets are set aside appropriately, including:

(i) the virtual assets should be held by its Associated Entity in cold storage and segregated from any virtual assets of the Platform Operator, its Associated Entity and any corporation within the same group of companies as the Platform Operator and any client virtual assets; and

(ii) the virtual assets should be the same as those client virtual assets which are covered under the compensation arrangement.

10.26 When selecting an insurance company to provide insurance coverage, a~~A~~ Platform Operator should base its choice of insurance company on verifiable and quantifiable criteria. These include a valuation schedule of assets insured, maximum coverage per incident and overall maximum coverage, as well as any excluding factors. The insurance company may be a captive insurer as defined in the Insurance Ordinance (Cap. 41).

XI. Management, Supervision and Internal Control

Responsibilities of senior management

11.1 Senior management of a Platform Operator should assume full responsibility for the Platform Operator's operations and its Associated Entity's operations to ensure that the operations are conducted in a sound, efficient, effective and compliant manner, including:

(a) the development and implementation of the Platform Operator's internal controls and its Associated Entity's internal controls and ensuring the ongoing effectiveness of these controls and adherence thereto by employees; and

(b) the establishment and maintenance of proper and effective policies and procedures for the identification and management of the risks associated with the Platform Operator's business and its Associated Entity's business.

11.2 Senior management of a Platform Operator should understand the nature of the business of the Platform Operator, its internal control procedures and its policies on the assumption of risk.

11.3 Senior management of a Platform Operator should clearly understand their own authority and responsibilities. In respect of that authority and those responsibilities:

(a) they should have access to all relevant information about the business on a timely basis to ensure that they are continually and timely appraised of the Platform Operator's operations and its Associated Entity's operations; and

(b) they should have available to them and seek where appropriate all necessary advice on that business and on their own responsibilities.

11.4 Senior management of a Platform Operator should establish and maintain an effective management and organisation structure and clear reporting lines for the Platform Operator and its Associated Entity, with supervisory and management responsibilities assigned to qualified and experienced individuals. The senior management should also ensure that detailed policies and procedures pertaining to authorisations and approvals, as well as the authority of key positions are clearly defined and communicated to and followed by employees.

Segregation of duties

11.5 A Platform Operator should ensure that it and its Associated Entity's key duties and functions are appropriately segregated, particularly those duties and functions which, when performed by the same individual, may result in potential conflicts of interest or undetected errors or may be susceptible to abuses which may expose the Platform Operator, its Associated Entity or its clients to inappropriate risks. In particular:

(a) ~~F~~front office functions (which include sales staff, staff responsible for handling client orders) and back office functions (which include staff responsible for handling client assets, settlement and accounting) should be carried out by different staff with separate reporting lines; and

(b) ~~C~~compliance and internal audit functions should be (i) segregated from and independent of the operational functions mentioned in subparagraph (a); and (ii) separated from each other. In addition, these functions should report directly to the senior management of the Platform Operator.

Capabilities

11.6 A Platform Operator should have and employ effectively the resources and procedures which are needed for the proper performance of its and its Associated Entity's business activities and to minimise the risk of loss due to the absence or departure of key staff members.

11.7 A Platform Operator should ensure that any person it or its Associated Entity employs or appoints to conduct business is fit and proper and otherwise qualified to act in the capacity so employed or appointed (including having relevant professional qualification, training or experience).

11.8 A Platform Operator should ensure that it and its Associated Entity have adequate resources to supervise diligently and do supervise diligently persons employed or appointed by them to conduct business on their behalf. The Platform Operator and its Associated Entity should be responsible for the acts or omissions of these employees and persons.

11.9 A Platform Operator should establish appropriate training policies with adequate consideration given to training needs to ensure compliance with the Platform Operator's and its Associated Entity's operational and internal control policies and procedures, and all applicable legal and regulatory requirements to which the Platform Operator, its Associated Entity and their employees are subject. A Platform Operator should ensure that it and its Associated Entity provide adequate training suitable for the specific duties which their employees perform both initially and on an ongoing basis.

Internal controls

11.10 A Platform Operator should have internal control procedures and financial and operational capabilities which can be reasonably expected to protect its and its Associated Entity's operations, clients and assets~~, and other licensed or registered persons~~ from financial losses arising from theft, fraud, and other dishonest acts, professional misconduct or omissions.

Risk management

11.11 A Platform Operator should establish and maintain appropriate and effective policies and procedures to identify, quantify, monitor and manage the risks, whether financial or otherwise, to which the Platform Operator, its Associated Entity and its clients are exposed. The Platform Operator should ensure its and its Associated Entity's risks of suffering losses are maintained at acceptable and appropriate levels, and take appropriate and timely action to contain and otherwise adequately manage such risks. In particular, the Platform Operator and its Associated Entity should only take on positions which they have the financial and management capacity to assume.

11.12 A Platform Operator should establish and maintain an effective and independent risk management function. The risk management function, together with the senior management of the Platform Operator, should:

(a) clearly define the Platform Operator's and its Associated Entity's risk policies and establish and maintain risk measures commensurate with their business strategies, size, complexity of its operations and risk profile; and

(b) monitor the implementation of the risk management policies and procedures of the Platform Operator and its Associated Entity and regularly review these policies and procedures to ensure that they remain appropriate and effective.

The senior management should be provided with exposure reports on a regular basis and promptly alerted to any material exposures and significant variances.

11.13 A Platform Operator should put in place effective risk management and supervisory controls for the operation of its trading platform. These controls should include:

(a) system controls to enable the Platform Operator to:

(i) prevent "fat finger" errors such as input limits or thresholds for order price and quantity;

(ii) immediately prevent the platform from accepting suspicious client orders; and

(iii) cancel any unexecuted orders on the platform.

(b) automated pre-trade controls that are reasonably designed to:

(i) prevent the entry of any orders that would exceed the limits prescribed for each client, including exposure limit referred to under paragraph 9.7 above;

(ii) alert the user to the entry of potential erroneous orders and prevent the entry of erroneous orders; and

(iii) prevent the entry of orders that are not in compliance with regulatory requirements.

(c) regular post-trade monitoring to reasonably identify any:

(i) suspicious market manipulative or abusive activities. Upon the identification of any suspected manipulative or abusive trading activities, the Platform Operator should take immediate steps to prevent such activities from continuing; and

(ii) market events or system deficiencies, such as unintended impact on the market, which call for further risk control measures.

11.14 Where institutional professional investors are allowed to conduct off-platform transactions without sufficient fiat currencies or virtual assets in the client's account with a Platform Operator (see paragraph 7.~~21~~ 23 above), the Platform Operator

should, based on its operational model, establish appropriate limits to ensure that the Platform Operator's risks of suffering losses, as a consequence of client defaults or changing market conditions, are maintained at acceptable and appropriate levels. These limits should be checked and reviewed for effectiveness on a regular basis.

Compliance

11.15 A Platform Operator should comply with, and implement and maintain measures appropriate to ensure its and its Associated Entity's compliance with the law, rules, regulations and codes administered or issued by the SFC, the requirements of any regulatory authority which apply to the Platform Operator and its Associated Entity, and the Platform Operator's and its Associated Entity's internal policies and procedures.

11.16 A Platform Operator should establish and maintain an effective and independent compliance function. The compliance function, together with the senior management of the Platform Operator, should:

(a) establish, maintain and enforce clear and effective compliance policies and procedures which cover all relevant aspects of the Platform Operator's and its Associated Entity's operations; and

(b) ensure that regular compliance reviews are conducted to detect potential violations or non-compliance by the Platform Operator, its Associated Entity or its staff with legal and regulatory requirements and the Platform Operator's and its Associated Entity's internal policies and procedures.

11.17 A Platform Operator should implement proper measures to ensure that all occurrences of material non-compliance by the Platform Operator, its Associated Entity or its staff with legal and regulatory requirements, as well as with the Platform Operator's and its Associated Entity's own policies and procedures, are promptly reported to its senior management and the relevant regulatory authorities, such as the SFC, where applicable.

11.18 A Platform Operator and its Associated Entity, as a firm, should not, without reasonable excuse, prohibit persons it employs from performing expert witness services for the SFC ~~and the Hong Kong Monetary Authority~~.

Internal audit

11.19 A Platform Operator should establish and maintain an independent audit function to objectively examine, evaluate and report on the adequacy, effectiveness and efficiency of the Platform Operator's and its Associated Entity's management, operations and internal controls. The audit function should:

(a) be free from operating responsibilities, with a direct line of communication to the senior management or the audit committee of the Platform Operator, as applicable;

(b) follow clearly defined terms of reference which set out the scope, objectives, approach and reporting requirements;

(c) adequately plan, control and record all audit and review work performed; and

(d) report to the senior management of the Platform Operator the findings, conclusions and recommendations noted in the audit and ensure that all matters and risks highlighted in the audit reports are followed up and resolved satisfactorily in a timely manner.

Complaints

11.20 A Platform Operator should ensure that:

(a) clients are provided with the Platform Operator's contact details for handling client complaints;

(b) written policies and procedures are established and maintained to ensure that complaints are properly handled and appropriate remedial action is promptly taken;

(c) complaints from clients relating to its business are handled independently by staff who are not involved in the subject matter of complaint and in a timely and appropriate manner;

(d) steps are taken to investigate and respond promptly to the complaints;

(e) where a complaint is not remedied promptly, the client is advised of any further steps which may be available to the client under the regulatory system; and

(f) where a complaint has been received, the subject matter of the complaint is properly reviewed. If the subject matter of the complaint relates to other clients, or raises issues of broader concern, the Platform Operator should take steps to investigate and remedy such issues, notwithstanding that the other clients may not have filed complaints with the Platform Operator.

Anti-bribery

11.21 A licensed person and all directors and staff of a Platform Operator, its Associated Entity or both should be familiar with the Prevention of Bribery Ordinance (Cap. 201) (PBO) and follow related guidance issued by the Independent Commission Against Corruption. The PBO may prohibit an agent (normally an employee) from soliciting or accepting an advantage without the permission of the principal (normally the employer) when conducting the principal's business. A person who offers the advantage may also commit an offence.

XII. Cybersecurity

12.1 A Platform Operator should ensure that the platform (including the trading system and custody infrastructure) is properly designed and operated in compliance with all applicable laws and regulations. The Platform Operator should ensure that all systems and processes underpinning the operation of the platform are robust and properly maintained such that the risk of theft, fraud, and other dishonest acts, professional misconduct, errors and omissions, interruptions or other operational or control failures is minimised and appropriately managed.

12.2 A Platform Operator should ensure that there are robust governance arrangements in place for overseeing the operation of its platform as well as adequate human, technology and financial resources available to ensure that the operations of its platform are carried out properly.

12.3 A Platform Operator should effectively manage and adequately supervise the design, development, deployment, ~~and~~ operation and modification of the platform ~~(which includes its trading system and custody infrastructure)~~. It should establish and implement written internal policies and procedures for the design, development, deployment, ~~and~~ operation and modification of the platform, to ensure the following:

(a) The key personnel of a Platform Operator should possess the necessary professional qualifications, management and technical experience to ensure the proper and continued provision of the virtual asset trading services offered by it. A Platform Operator should identify key personnel (such as the founder or chief developer of the platform) and have plans in place to mitigate the associated key man risks.

(b) A Platform Operator should have at least one responsible officer responsible for the overall management and supervision of its ~~trading~~ platform and for defining a cybersecurity management framework and setting out key roles and responsibilities. These responsibilities include:

(i) ~~R~~reviewing and approving policies and procedures relating to the design, development, deployment, operation, modification and cybersecurity risk management matters of the platform;

(ii) ~~R~~reviewing and approving the budget and spending on resources for the platform and cybersecurity risk management;

(iii) ~~A~~arranging to conduct a technology audit (see paragraph 12.7) and an independent cybersecurity assessment (see paragraph 12.13) on a periodic basis;

(iv) ~~R~~reviewing significant issues arising from emergencies, disruptions and cybersecurity incidents relating to the platform;

(v) ~~R~~reviewing major findings identified from internal and external audits and cybersecurity reviews; endorsing and monitoring the completion of remedial actions;

(vi) ~~M~~monitoring and assessing ~~the latest~~ cybersecurity threats and attacks, including maintaining up-to-date knowledge of the cyber threat landscape, new vulnerabilities, bugs and attack vectors, gathering cyber threat intelligence and performing vulnerability scans regularly with automated tools;

Note: The requirement to perform vulnerability scans regularly with automated tools does not include performing penetration tests based on attack simulations.

(vii) ~~R~~reviewing and approving the contingency plan developed for the platform; and

(viii) ~~R~~reviewing and approving the initial and ongoing due diligence of, and the service level agreement and contract with a third-party service provider relating to the provision of outsourced services to the platform, where applicable.

These responsibilities can be delegated, in writing, to a designated committee or operational unit, but overall accountability remains with the responsible officer(s).

(c) There should be a formalised governance process with input from the dealing, risk and compliance functions.

(d) There should be clearly identified reporting lines with supervisory and reporting responsibilities assigned to appropriate staff members.

(e) There should be managerial and supervisory controls which are designed to manage the risks associated with the use of the ~~trading system~~platform by clients.

12.4 A Platform Operator should conduct regular reviews to ensure that these internal policies and procedures are in line with changing market conditions, the cyber threat landscape and regulatory developments and promptly remedy any deficiencies identified.

12.5 A Platform Operator should assign adequately qualified staff, expertise, technology and financial resources to the design, development, deployment, ~~and~~ operation and modification of the platform.

12.6 Where the platform or any activities associated with the platform is provided by or outsourced to a third party service provider, a Platform Operator should perform appropriate due diligence, conduct ongoing monitoring and make appropriate arrangements to ensure that the Platform Operator meets the requirements in these Guidelines (including ~~this~~ Part XII of these Guidelines and Part XIV (Record Keeping) below[67]). In particular, the Platform Operator or its Associated Entity should enter into a formal service-level agreement with the service provider which specifies the terms of services and responsibilities of the provider. This service-level

[67] In response to a request for information made by the SFC, information in possession of a third party service provider that is proprietary in nature may be provided to the SFC directly from the service provider.

agreement should be regularly reviewed and revised, where appropriate, to reflect any changes to the services provided, outsourcing arrangements or regulatory developments. Whenever possible, such agreements should provide sufficient levels of maintenance and technical assistance with quantitative details.

12.7 A Platform Operator should arrange a periodic (at least annual) technology audit by a suitably qualified independent professional so as to be satisfied that the Platform Operator and its Associated Entity have fully complied with ~~this~~ Part XII of these Guidelines. A Platform Operator should exercise due skill, care and diligence in the selection and appointment of the independent professional and should have regard to their experience and track record in reviewing virtual asset related technology. It should take, and should ensure its Associated Entity takes, prompt rectification measures upon the identification of any non-compliance.

Adequacy of platform

12.8 A Platform Operator should ensure the integrity of the platform, maintain a high degree of reliability, security and capacity in respect of its systems, and have appropriate contingency measures in place.

Reliability of platform

12.9 A Platform Operator should have standard operating procedures (SOP) in writing for performing system upgrades and maintenance. The SOP need to contain:

(a) the method(s) of communication, as well as how pending orders still in the order book are dealt with;

(b) information on how long orders can be entered, amended or cancelled after a system downtime, and before continuous trading resumes; and

(c) the process applicable for unexpected and unplanned system failures which affect an orderly market.

12.10 A Platform Operator should ensure that its ~~trading system~~platform and all modifications to the ~~system~~platform, such as implementing a new system or upgrading an existing system, are tested before deployment and are regularly reviewed to ensure that the ~~system~~ platform and modifications are reliable. Specifically, a Platform Operator should at least conduct the following before deployment:

(a) reviewing and signing off on the test results by senior management;

(b) fully backing up the system and data; and

(c) devising a contingency plan to switch back to the previous version of the ~~trading system~~platform in the event of any critical and unrecoverable errors in the new version.

A Platform Operator should maintain a clear audit trail for all modifications made to the ~~trading system~~platform.

12.11 Where a Platform Operator plans to have ~~trading system~~ outages to perform updates and testing of its platforms or systems, it should inform its clients as far in advance as practicable if such outages may affect them.

Security of platform

12.12 A Platform Operator should employ adequate, up-to-date and appropriate security controls to protect the platform from being abused. The security controls should at least include:

(a) robust authentication and authorisation methods and technology to ensure that access to the platform is restricted to authorised persons only on a need-to-have basis. Specifically:

(i) only permit members of its staff to have access to trading information concerning orders placed, or transactions conducted, on its platform and only to the extent necessary to enable the platform to operate properly and efficiently, and at all times keep the senior management informed as to:

(I) the identity of each such staff member (by title and department) and the information to which he or she has access;

(II) the basis upon which it is necessary, in each case, for such access to be permitted; and

(III) any change made in relation to the staff members to whom such access is permitted and the basis for such change;

(ii) adopt appropriate user authentication method to enable the relevant user to be uniquely identified;

~~(ii)~~(iii) review, at least on a yearly basis, the user access list of the platform and databases to ensure that access to or use of the platform and databases remain restricted to persons approved to use them on a need-to-have basis, and revoke unnecessary user access and privileges (for example, for departed staff) on a timely basis;

~~(iii)~~(iv) maintain an adequate access log which records the identity and role of the staff members who have access to its platform, the information accessed, the time of access, any approval given for such access and the basis upon which such access was permitted in each case, and have adequate protections in place to prevent tampering or erasure of the log; and

~~(iv)~~(v) have adequate and effective policies, systems and controls in place to guard against, and detect the occurrence of errors, omissions or unauthorised insertion, alteration or deletion of data (including clients' information and trading information), information leakage or abuse by members of its staff in relation to the trading information concerning

orders placed ~~and/or~~, transactions conducted on its platform or both to which they have access;

(b) two-factor authentication[68] for login to clients' accounts;

(c) effective policies and procedures to ensure that a client login password is generated and delivered to a client in a secure manner during the account activation and password reset processes. A client login password should be randomly generated by the system and sent to a client through a channel of communication which is free from human intervention and from tampering by staff of the Platform Operator. In a situation where a client login password is not randomly generated by the system, the Platform Operator should implement adequate compensating security controls such as compulsory change of password upon the first login after client account activation;

(d) stringent password policies and session timeout controls on its platform, which include:

(i) ~~M~~minimum password length;

(ii) ~~P~~periodic reminders for those clients who have not changed their passwords for a long period;

(iii) ~~M~~minimum password complexity (ie, alphanumeric) and history;

(iv) avoidance of passwords that contain values known to be commonly-used, expected, or compromised;

~~(iv)~~(v) ~~A~~appropriate controls on invalid login attempts; and

~~(v)~~(vi) ~~S~~session timeout after a period of inactivity~~.~~;

(e) prompt notification to clients after certain client activities have taken place in their accounts. These activities should at least include:

(i) ~~S~~system login;

(ii) ~~P~~password reset;

(iii) ~~T~~trade execution; and

(iv) ~~C~~changes to client and account-related information~~.~~;

The channel of notification to clients should be different from the one used for system login (as outlined in subparagraph (b)). Clients may choose to opt out from "trade execution" notifications only. Under such circumstances, except for dealing with institutional and qualified corporate professional investors, adequate risk disclosures should be provided by the Platform Operator to the

[68] Two-factor authentication refers to an authentication mechanism which utilises any two of the following factors: what a client knows, what a client has, and who a client is.

client and an acknowledgement should be executed by the client confirming that the client understands the risks involved in doing so.

(f) adequate security controls over the infrastructure of the platform. Specifically, the Platform Operator should:

(i) deploy a secure network infrastructure through proper network segmentation, ie, a Demilitarised Zone (DMZ) with multi-tiered firewalls, to protect critical systems and client data against cyber-attacks;

(ii) grant ~~remote~~ access (including remote access) to its internal network and different segments of it on a need-to-have basis and implement security controls over such access;

(iii) monitor and evaluate security patches or hotfixes released by software provider(s) on a timely basis and, subject to an evaluation of the impact, conduct testing as soon as practicable and implement the security patches or hotfixes within one month following the completion of testing;

(iv) implement and update anti-virus and anti-malware solutions as well as endpoint detection and response technology on a timely basis to detect malicious applications and malware on critical system servers and workstations;

(v) implement Intrusion Prevent System (IPS), Intrusion Detection System (IDS) and System Information and Event Management (SIEM) solutions to detect and generate alerts on any intrusion or unauthorised access to critical system servers and workstations on a real time basis;

Note: the detection rules of the endpoint detection and response technology and SIEM solutions mentioned in subparagraphs (iv) and (v) above should be updated as and when necessary such as when there are new attack or threat scenarios that require additional detection rules.

(vi) establish a Security Operations Center (SOC) or equivalent function with sufficient resources to take charge of all security monitoring processes and technologies and act as a coordinator for efficient incident detection and handling;

~~(v)~~(vii) implement security controls to prevent unauthorised installation of hardware and software, and ensure that only authorised storage media and devices are used to store and transfer critical data; and

~~(vi)~~(viii) establish physical security policies and procedures to protect critical platform components (for example, the HSM, the authorised storage media and devices used to store and transfer critical data, system servers and network devices) in a secure environment and to prevent unauthorised physical access to the facilities hosting the platform as well as the critical platform~~system~~ components, and where applicable, apply segregation of duty or privilege separation to the access to critical platform components;

(g) up-to-date data encryption and secure transfer technology, in accordance with industry best practices and international standards, to protect the confidentiality and integrity and assure source authenticity of information stored on the platform and during transmission between internal and external networks. In particular, the Platform Operator should use a strong encryption algorithm to:

(i) encrypt sensitive information such as client login credentials (ie, user ID and password) and trade data during transmission between internal networks and client devices; ~~and~~

(ii) protect client login passwords stored on the platform;

(iii) protect critical data transferred between components of the Platform Operator's system infrastructure; and

(iv) protect the backup copies of the platform's critical data;

(h) up-to-date security tools to detect, prevent and block any potential unauthorised intrusion, security breach and cyberattack attempts. In particular, the Platform Operator should implement an effective monitoring and surveillance mechanism to detect unauthorised access to clients' accounts or the Platform Operator's accounts (if any); and

(i) adequate internal procedures and training for the Platform Operator's staff at least on a yearly basis and regular alerts and educational materials for its clients to raise awareness of the importance of cybersecurity and the need to strictly observe security measures when using the platform.

12.13 A Platform Operator should perform a stringent independent cybersecurity assessment, before the launch or deployment of modifications to ~~of~~ its ~~trading~~ platform ~~and any major enhancement to existing services~~, and periodically thereafter. The scope of the cybersecurity assessment should at least cover:

(a) user application security (ie, desktop/web-based/mobile app);

(b) wallet security;

(c) physical security; and

(d) network and system security (including penetration testing, source code review of the custody system and other systems which interface or connect with the custody system[69], and vulnerability scanning).

[69] In relation to the source code review of the custody system and other systems which interface or connect with the custody system, whilst the assessment prior to the launch of the platform and the ongoing periodic assessments should be performed by an independent third party, the review in relation to modifications prior to their deployment can be performed by either an independent third party or by the Platform Operator itself. For the avoidance of doubt, if no changes have been made to the custody system or the other systems which interface or connect with the custody system after the platform's initial launch, then no source code review needs to be performed.

The Platform Operator should maintain sufficient documentation on the cybersecurity assessment, including the testing scope and methodology and the assessment results.

12.14 A Platform Operator should establish written policies and procedures specifying the manner in which a suspected or actual cybersecurity incident should be escalated internally and externally (for example, the clients, the SFC and other regulatory authorities, where appropriate).

Capacity of platform

12.15 A Platform Operator should ensure that:

(a) the usage capacity of the platform is regularly monitored and appropriate capacity planning is developed. As part of the capacity planning, a Platform Operator should determine and keep a record of the required level of spare capacity;

(b) the capacity of the platform is regularly stress tested to establish system behaviour under different simulated market conditions, and the results of the stress tests and any actions taken to address the findings of the stress tests are documented;

(c) the platform has sufficient capacity to handle any foreseeable increase in the volume of business and market turnover; and

(d) there are contingency arrangements to:

(i) handle clients' orders when the capacity of the platform is exceeded; and

(ii) inform clients about the arrangements and ensure alternative means of executing orders are available and offered to clients.

System and data backup

12.16 A Platform Operator should back up business records, client and transaction databases, servers and supporting documentation in an offline medium at least on a daily basis. Off-site storage is generally expected to be subject to proper security measures. A Platform Operator should also implement proper measures to ensure the availability and integrity of the backup copies.

Contingencies

12.17 A Platform Operator should identify and manage the associated risks (including any unintended consequences) prudently with appropriate contingency arrangements in place. Such arrangement should include a written contingency plan to cope with emergencies and disruptions (including cybersecurity situations) related to the platform, including checking and ensuring data integrity after system recovery and ensuring that trading can be conducted in a fair and orderly manner after resumption.

12.18 The contingency plan should at least include:

(a) the potential disruptive scenarios, including cyber-attack scenarios, such as distributed denial-of-service attacks and total loss of business records and client data resulting from cyber-attacks, and the corresponding procedures for activating the contingency plan;

(b) a suitable backup facility which will enable the Platform Operator to continue providing its trading services or alternative arrangements for order execution in the event of an emergency; and

(c) the availability of trained staff to deal with clients' and regulators' enquiries.

12.19 A Platform Operator should ensure that the backup facility and the contingency plan are reviewed, updated and tested for viability and adequacy at least on a yearly basis.

12.20 In the event of material system delay or failure, a Platform Operator should, in a timely manner:

(a) rectify the situation; and

(b) inform clients about the situation as soon as practicable and how their pending orders, deposits and withdrawals will be handled.

XIII. Conflicts of Interest

13.1 A Platform Operator should avoid, and should also ensure that its Associated Entity, its associates[70] and its Associated Entity's associates avoid~~s~~, any material interest in a transaction with or for a client or a relationship which gives rise to an actual or potential conflict of interest. Where the Platform Operator ~~or~~, its Associated Entity, its associates and its Associated Entity's associates cannot avoid acting in any actual or potential conflict of interest situation, ~~it~~ the Platform Operator should make appropriate prior disclosure to the client, where applicable, and take all reasonable steps to manage the conflict and ensure fair treatment of the client.

13.2 A Platform Operator should not engage in proprietary trading in virtual assets for its own account or any account in which it has an interest, except for off-platform back-to-back transactions entered into by the Platform Operator and other ~~limited~~ circumstances permitted by the SFC on a case-by-case basis.

Note: ~~——~~For the purpose of this paragraph, ~~:~~

~~(a) *"proprietary trading"* refers to trading activities conducted for:~~

~~(i) the account of the Platform Operator, trading as principal;~~

~~(ii) the account of any client which is a company within the same group of companies as the Platform Operator, trading as principal; or~~

~~(iii) any account in which the Platform Operator, or any client which is a company within the same group of companies as the Platform Operator, has an interest.~~

~~(b)~~ ~~——~~off-platform b~~B~~ack-to-back transactions refer to those transactions where a Platform Operator, after receiving: ~~—~~

(a) ~~(i)~~ a purchase order from a client, purchases a virtual asset from a third party and then sells the same virtual asset to the client; or

(b) ~~(ii)~~ a sell order from a client, purchases a virtual asset from the client and then sells the same virtual asset to a third party,

and no market risk is taken by the Platform Operator.

13.3 A Platform Operator should ensure that any corporation within the same group of companies as the Platform Operator does not conduct any proprietary trading in virtual assets through the Platform Operator (whether on-platform or off-platform) except for circumstances permitted by the SFC on a case-by-case basis.

~~13.3~~13.4 A Platform Operator should not engage in market making activities on a proprietary basis.

[70] "Associate" has the meaning as defined in section 1 of Part 1 of Schedule 1 to the SFO.

~~13.4~~13.5 A Platform Operator should establish, and ensure that its Associated Entity establishes, clear policies which set out the circumstances under which the acceptance of gifts, rebates or benefits from clients or other counterparties by the Platform Operator, its Associated Entity or their staff members are allowed and the corresponding approval required.

Employee dealings

~~13.5~~13.6 A Platform Operator should have, and should also ensure that its Associated Entity has, a policy which has been communicated to employees in writing governing employees' dealings in virtual assets and virtual asset-related products to eliminate, avoid, manage or disclose actual or potential conflicts of interests which may arise from such dealings. For purposes of ~~this~~ Part XIII of these Guidelines, the term:

(a) *"employees"* includes directors (other than non-executive directors) of a Platform Operator or its Associated Entity; and

(b) *"related accounts"* refer to accounts of the employee's minor children and accounts in which the employee holds any beneficial interest.

~~13.6~~13.7 Where employees of a Platform Operator or its Associated Entity are permitted to deal in virtual assets and virtual asset-related products for their own accounts and related accounts:

(a) the written policy should specify the conditions under which employees may deal in virtual assets and virtual asset-related products for their own accounts and related accounts (in particular, those who possess non-public information should be prohibited from dealing in the relevant virtual asset);

(b) the employees should generally be required to deal through the Platform Operator;

~~(b)~~(c) where these accounts have been set up with the Platform Operator's trading platform~~:~~ , ~~(i)~~ employees should be required to identify them as such and report them to the Platform Operator's senior management and any transactions for employees' own accounts and related accounts should be separately recorded and clearly identified in the records of the Platform Operator; and

~~(ii) employees should generally be required to deal through the Platform Operator;~~

~~(iii) any transactions for employees' own accounts and related accounts should be separately recorded and clearly identified in the records of the Platform Operator.~~

(d) ~~Where the Platform Operator's or its Associated Entity's employees are permitted to deal in virtual assets and virtual asset-related products for their own accounts or related accounts through a person other than the Platform Operator~~where these accounts have been set up with a person other than the Platform Operator, the Platform Operator and the employee should arrange for

duplicate trade confirmations and statements of account to be provided to the Platform Operator's senior management.

~~13.7~~13.8 Senior management of a Platform Operator should actively monitor all virtual asset and virtual asset-related products transactions for employees' own accounts and related accounts. The senior management should not have any beneficial or other interest in these transactions and should maintain procedures to detect irregularities.

~~13.8~~13.9 A Platform Operator should have, and should also ensure its Associated Entity has, procedures in place to ensure that orders of clients have priority over orders for the account of their employees and their employees do not deal (for the benefit of the Platform Operator, its Associated Entity, the employee or a client) in virtual assets where the employee concerned effects the dealing in order to *"front-run"* pending transactions for or with clients. The procedures should also ensure that the employees of the Platform Operator and its Associated Entity do not deal in virtual assets on the basis of other non-public information, which could materially affect the prices of those virtual assets, until the information becomes public.

~~13.9~~13.10 A Platform Operator should not knowingly deal in virtual assets for an employee of another ~~P~~platform ~~O~~operator unless it has received written consent from that ~~P~~platform ~~O~~operator.

XIV. Record keeping

General record keeping requirements for Platform Operators and its Associated Entity

14.1 A Platform Operator should establish, and should also ensure that its Associated Entity establishes, policies and procedures to ensure the integrity, security, availability, reliability and completeness of all information, both in physical and electronically stored form, in relation to the Relevant Activities.

14.2 A Platform Operator should, in relation to the Relevant Activities:

(a) keep, where applicable, such accounting, trading and other records as are sufficient to:

(i) explain, and reflect the financial position and operation of, such businesses;

(ii) enable profit and loss accounts and balance sheets which give a true and fair view of its financial affairs to be prepared from time to time;

(iii) account for all client assets it receives or holds;

(iv) enable all movements of such client assets to be traced through its accounting systems;

(v) reconcile, on a monthly basis, any differences in its balances or positions with other persons, including its Associated Entity and banks, and show how such differences were resolved;

(vi) demonstrate compliance with, and that it has systems of control in place to ensure compliance with, Part X (Custody of Client Assets) above; and

(vii) enable it readily to establish whether it has complied with Part VI (Financial Soundness) above;

(b) keep those records in such a manner as will enable an audit to be conveniently and properly carried out; and

(c) make entries in those records in accordance with generally accepted accounting principles.

The records required to be kept are specified in paragraphs 14.7 to 14.9 below.

14.3 A Platform Operator should, and should also ensure that its Associated Entity will, in respect of the client assets that its Associated Entity receives or holds:

(a) keep, where applicable, such accounting and other records as are sufficient to:

(i) account for all client assets;

(ii) enable all movements of the client assets to be traced through its accounting systems;

(iii) show separately and account for all receipts, payments, deliveries and other uses or applications of the client assets effected by it, or on its behalf, and on whose behalf such receipts, payments, deliveries or other uses or applications of the client assets have been effected;

(iv) reconcile, on a monthly basis, any differences in its balances or positions with other persons, including the Platform Operator and banks, and show how such differences were resolved; and

(v) demonstrate compliance with, and that it has systems of control in place to ensure compliance with, Part X (Custody of Client Assets) above;

(b) keep those records in such a manner as will enable an audit to be conveniently and properly carried out; and

(c) make entries in those records in accordance with generally accepted accounting principles.

The records required to be kept are specified in paragraph 14.7 below.

Form and premises in which records are to be kept

14.4 A Platform Operator should keep, and should also ensure that its Associated Entity keeps, all the required records:

(a) in writing in the Chinese or English language; or

(b) in such a manner as to enable them to be readily accessible and readily convertible into written form in the Chinese or English language.

14.5 A Platform Operator should adopt, and should also ensure that its Associated Entity adopts, all reasonably necessary procedures to guard against the falsification of any of the required records, to ~~and~~ facilitate the discovery of any such falsification, and to ensure the security, authenticity, reliability, integrity, confidentiality and timely availability of required records.

14.6 A Platform Operator should keep, and should also ensure that its Associated Entity keeps, all the required records at the premises used by the Platform Operator which have been approved under section 130(1) of the SFO and/or section 53ZRR of the AMLO. If the Platform Operator wishes to keep any required records exclusively with an electronic data storage provider, it should obtain prior written approval from the SFC.

Records to be kept

14.7 A Platform Operator should retain, and should also ensure that its Associated Entity retains, the following records for a period of not less than seven years:

(a) Records showing particulars of:

(i) all money received by it, whether or not such money belongs to it, or is paid into accounts maintained by it or on its behalf, and disbursed by it;

(ii) all income received by it, whether the income relates to charges made by it for the provision of services, commissions, brokerage, remuneration, interest or otherwise;

(iii) all expenses, commissions and interest incurred or paid by it;

(iv) all disposals of client virtual assets initiated by it, showing in the case of each disposal:

(I) the name of the client;

(II) the date on which the disposal was effected;

(III) the charges incurred for effecting the disposal; and

(IV) the proceeds of the disposal and how such proceeds were dealt with;

(v) its assets and liabilities, including financial commitments and contingent liabilities;

(vi) all virtual assets belonging to it, identifying:

(I) with whom such virtual assets are deposited; and

(II) the date on which they were so deposited;

(vii) all virtual assets held by it but not belonging to it, identifying:

(I) for whom such virtual assets are held and with whom they are deposited;

(II) the date on which they were so deposited; and

(III) virtual assets which are deposited with another person for safe custody;

(viii) all wallet addresses from which deposits of virtual assets were received, and to which withdrawals of virtual assets were made;

(ix) all bank accounts held by it, including segregated accounts maintained;

(x) all other accounts held by it; and

(xi) all off-balance sheet transactions or positions.

(b) Records of all contracts (including written agreements with clients) entered into by it.

(c) Records evidencing:

(i) any standing authority given to it by a client, and any renewal of such authority; and

(ii) any one-off written direction given to it by a client.

(d) In respect of a client who is a professional investor:

(i) records showing particulars sufficient to establish that the client is a professional investor; and

(ii) any notice given by it to the client.

(e) Records in respect of transactions conducted in its systems, as particularised below:

(i) details of the clients, including their registered names and addresses, dates of admission and cessation, and client agreements;

(ii) details of any restriction, suspension or termination of the access of any clients to its systems, including the reasons for this;

(iii) all notices and other information, whether written or communicated through electronic means, provided by the Platform Operator to the users of its systems, whether individually or generally;

(iv) routine daily and monthly summaries of trading in its systems, including:

(I) the virtual assets in respect of which transactions have been executed; and

(II) the transaction volume, expressed in numbers of trades, numbers of virtual assets traded and total settlement value.

(f) Records relating to the inclusion of virtual assets on its platform (as provided in Part VII (Operations) above), including the due diligence plan, procedures, assessment and results of due diligence performed, legal opinions and all relevant correspondences~~;~~.

(g) Records of knowing your clients, including the process and outcomes of any risk profiling~~;~~.

(h) Records of suitability assessments conducted~~;~~.

(i) Records of reconciliation between a distributed ledger and an internal ledger on client virtual assets~~;~~.

(j) A copy of each monthly statement of account prepared in accordance with ~~Part IX (Dealing with Clients)~~paragraph 9.33 above~~;~~.

(k) Records of all client complaints relating to client assets and details of follow-up actions, including the substance and resolution of each complaint~~;~~.

(l) Records regarding client identity for confirmation on origination of instructions and beneficiaries and details of the instructions as prescribed in paragraph 9.8 above~~; and~~.

(m) To the extent not already covered elsewhere in this paragraph, records evidencing the Platform Operator's and the Associated Entity's compliance with these Guidelines.

14.8 A Platform Operator, and its Associated Entity (where applicable), should retain the following for a period of not less than two years:

(a) A copy of each contract note and receipt prepared in accordance with paragraph 9.33~~Part IX (Dealing with Clients)~~ above~~;~~.

(b) A copy of each statement of account prepared upon request by the client in accordance with paragraph 9.33(g) above~~;~~.

(c) Time-sequenced records of orders and instructions that the Platform Operator receives or initiates, containing particulars including, but not limited to, the following:

(i) the date and time that any order or instruction was received, executed, modified, cancelled or expired (where applicable);

(ii) the identity, address and contact details of the client initiating an entry, modification, cancellation or execution of an order or instruction;

(iii) the particulars of any subsequent modification and execution of any order or instruction (where applicable), including but not limited to, the virtual assets involved, the size and side (buy or sell) of the order, the order type and any order designation, time and price limit or other conditions specified by the client originating the order;

(iv) the particulars of the allocation and re-allocation (where applicable) of an execution;

(v) the particulars of each transaction entered into by it or on its behalf to implement any such order or instruction;

(vi) the particulars identifying with whom or for whose account it has entered into such a transaction; and

(vii) the particulars which enable the transaction to be traced through its accounting, trading and settlement systems~~;~~.

(d) To the extent not already covered in subparagraph (c) above, time-sequenced records of all off-platform transactions.

~~(d)~~(e) Audit logs for the activities of its systems including but not limited to audit trails and access logs referred to in Part XII (Cybersecurity) above~~; and~~.

~~(e)~~(f) Incident reports for all material system delays or failures.

Details of the requirements for the recording of audit logs and incident reports referred to in subparagraphs (~~ed~~) and (~~fe~~) are set out in ~~the~~ Schedule ~~32~~ to these Guidelines.

Records to be kept for not less than two years after the platform or system ceases to be used

14.9 A Platform Operator should keep the following records for a period of not less than two years after the Platform Operator's platform or system ceases to be used:

(a) ~~C~~comprehensive documentation of the design, development, deployment and operation of its platform or system, including any testing, reviews, modifications, upgrades or rectifications of its system; and

(b) ~~C~~comprehensive documentation of the risk management controls of its platform or system.

14.10 A Platform Operator should give the SFC access to the required records upon request. Given the nature of the technology behind the virtual assets, a Platform Operator should, at all times, maintain proper access to the platform or system nodes for the full records of the Relevant Activities.

XV. Auditors

15.1 A Platform Operator should exercise due skill, care and diligence in the selection and appointment of the auditors[71] to perform an audit of the financial statements of the Platform Operator and its Associated Entity, and should have regard to their experience and track record auditing virtual asset-related business and their capability in acting as auditors of the Platform Operator and its Associated Entity.

15.2 For the purpose of matters reportable by auditors under sections 53ZSD(4)(a)(i) and 53ZSD(4)(b)(i) of the AMLO, such matters ~~mean~~are:

(a) ~~i~~in relation to an auditor of a Platform Operator, a matter that constitutes, on the part of the Platform Operator, a failure to comply with any requirements in Part VI (Financial Soundness), Part X (Custody of Client Assets) and Part XIV (Record Keeping) above; and

(b) ~~i~~in relation to an auditor of an Associated Entity of a Platform Operator, a matter that constitutes, on the part of the Associated Entity of the Platform Operator, a failure to comply with any requirements Part X (Custody of Client Assets) and Part XIV (Record Keeping) above.

[71] "Auditor" is defined in section 1 of Part 1 of Schedule 1 to the SFO and section 53ZR of the AMLO.

XVI. Ongoing Reporting ~~/~~ and Notification Obligations

16.1 Pursuant to section 128(1) of the SFO and/or sections 53ZTI(1) and (2) of the AMLO, applicants should provide any information that the SFC reasonably requires to enable it to consider the applications made under Part V of the SFO and/or Part 5B of the AMLO, including but not limited to the following information:

	Information specified in	Type of applications
(a)	Part 1 of Schedule 4	Applications by Platform Operators
(b)	Part 2 of Schedule 4	Applications by licensed representatives
(c)	Part 3 of Schedule 4	Other applications

~~16.1~~16.2 Where there is a change in the information specified in relevant part of Schedule ~~4~~3 to these Guidelines that has been provided to the SFC under any provision of Part V of the SFO and Divisions 3, 4 and ~~6~~ 7 of Part 5B of the AMLO[72], a notice in writing of the change containing a full description of it shall, within ~~7~~seven business days after the change takes place, be given to the SFC by the following persons:

	Information specified in~~:~~	Changes to be notified by~~:~~
(a)	Part ~~1~~ 4 of Schedule ~~4~~3	Platform Operator
(b)	Part 5 of Schedule 4	Associated Entity
(~~b~~c)	Part ~~2~~ 6 of Schedule ~~4~~3	Licensed representative
(~~c~~d)	Part ~~3~~ 7 of Schedule ~~4~~3	Substantial shareholder and ultimate owner

~~16.2~~16.3 Nothing in Schedule ~~4~~3 to these Guidelines shall require disclosure of information concerning an ongoing criminal investigation by a regulatory body or criminal investigatory body if such disclosure is prohibited by any statutory provision in Hong Kong or elsewhere, but the person shall notify the SFC of the results of the investigation within ~~7~~ seven business days after the person becomes aware of the completion of the investigation.

~~16.3~~16.4 A Platform Operator should obtain the SFC's prior written approval for any plan or proposal to include any virtual asset for trading by retail clients, or suspend trading of, or remove any virtual asset which is made available to retail clients.

~~16.4~~16.5 A Platform Operator should notify the SFC in writing in advance of any plan or proposal to include any virtual asset for trading by professional investors only, or suspend trading of or remove any virtual asset which is made available to professional investors only.

[72] This also applies to applications that have not been withdrawn or granted or otherwise finally disposed of. In this respect, a reference to "Platform Operator, "Associated Entity", "licensed representative", "substantial shareholder" and "ultimate owner" would mean a person applying to be a Platform Operator, Associated Entity, licensed representative, substantial shareholder and ultimate owner respectively.

~~16.5~~16.6 A Platform Operator should submit such information as may be specified and requested by the SFC from time to time, and this includes but is not limited to:

(a) the monthly volume of virtual asset transactions conducted through the Platform Operator (whether on or off-platform), with a breakdown by type of virtual asset (as specified by the SFC) traded by clients;

(b) its operating expenses in the past 12 months and the amount of assets maintained in accordance with paragraph 6.1 above as at the end of the month; and

(c) other statistics on trading, custody and other incidental activities, as applicable, in Hong Kong.

~~16.6~~16.7 A Platform Operator, and its Associated Entity (where applicable), should also notify the SFC immediately of matters specified under other Parts of these Guidelines and upon the occurrence of the following:

(a) any proposed change to the following which might affect the Platform Operator's or its Associated Entity's~~its~~ operations, with an explanation for the proposed change, prior to its implementation:

(i) the trading rules, admission and removal rules or criteria, trading sessions and operating hours, hardware, software and other technology of its systems, and, where applicable, all system interfaces between its own platform and other platforms;

(ii) the Platform Operator's or its Associated Entity's contractual responsibilities in relation to its clients; and

(iii) the contingency and business recovery plan in relation to its ~~trading system~~platform;

(b) any causes, or possible causes, impact analysis and recovery measures to be taken in respect of material service interruptions or other significant issues related to ~~its~~ the Platform Operator's or its Associated Entity's platform or systems;

(c) any material failure, error or defect in the operation or functioning of the Platform Operator's or its Associated Entity's~~its~~ trading, custody, accounting, clearing and settlement systems or equipment; ~~and~~

Note: The Platform Operator, and its Associated Entity (where applicable), should submit the incident report (see Schedule 3 to these Guidelines) in relation to the notification in subparagraphs (b) and (c) above without undue delay to the SFC.

(d) any material breach or infringement of or non-compliance with these Guidelines, any applicable law (including the SFO and the AMLO), rules, regulations,~~the SFO and the applicable subsidiary legislation made under them, the AMLO, the~~ codes, ~~and~~ guidelines, ~~or any relevant~~ circulars or ~~frequently asked question~~FAQs administered or issued by the SFC, or where the Platform Operator or its Associated Entity~~it~~ suspects any such breach,

infringement or non-compliance ~~whereby~~ whether by itself or persons the Platform Operator or its Associated Entity ~~it~~ employs or appoints to conduct business with clients;

Note: The Platform Operator, and its Associated Entity (where applicable), should give particulars of the breach, infringement or non-compliance, or suspected breach, infringement or non-compliance, and relevant information and documents.

(e) the passing of any resolutions, the initiation of any proceedings, or the making of any order which may result in the appointment of a receiver, provisional liquidator, liquidator or administrator or the winding-up, re-organisation, reconstruction, amalgamation, dissolution or bankruptcy of the Platform Operator or its Associated Entity or any of the Platform Operator's~~its~~ substantial shareholders, ultimate owners or the making of any receiving order or arrangement or composition with creditors;

(f) the bankruptcy of any of the Platform Operator's or its Associated Entity's ~~its~~ directors; and

(g) the exercise of any disciplinary measure against the Platform Operator or its Associated Entity~~it~~ by any regulatory or other professional or trade body or the refusal, suspension or revocation of any regulatory licence, consent or approval required in connection with the Platform Operator's or its Associated Entity's~~its~~ business.

Schedule 1 Professional Investors

Overview of professional investor ~~and~~ terminology

For the purposes of setting out exemptions and for ease of reference under these Guidelines, a "professional investor" is referred to in the Guidelines in the following terms:

"*Institutional professional investor*" means a person falling under paragraphs (a) to (i) of the definition of "professional investor" in section 1 of Part 1 of Schedule 1 to the SFO.

"*Corporate professional investor"* means a trust corporation, corporation or partnership falling under sections 4, 6 and 7 of the Securities and Futures (Professional Investor) Rules (Cap. 571D) (Professional Investor Rules).

"*Qualified corporate professional investor*" means a corporate professional investor which has passed the assessment requirements under paragraph 1 below and gone through the procedures under paragraph 2 below.

~~"*Individual professional investor*" means an individual falling under section 5 of the Professional Investor Rules.~~

Determination of whether corporate professional investors are qualified

1. Assessment requirements for corporate professional investors

   (a) In making the assessment on a corporate professional investor in relation to virtual assets, the Platform Operator should assess whether or not it is reasonably satisfied that the corporate professional investor satisfies all of the following three criteria:

      (i) the corporate professional investor has the appropriate corporate structure and investment process and controls (ie, how investment decisions are made, including whether the corporation has a specialised treasury or other function responsible for making investment decisions);

      (ii) the person(s) responsible for making investment decisions on behalf of the corporate professional investor has(have) sufficient investment background (including the investment experience of such person(s)); and

      (iii) the corporate professional investor is aware of the risks involved, which is considered in terms of the person(s) responsible for making investment decisions.

   (b) The above assessment should be in writing. Records of all relevant information and documents obtained in the assessment should be kept by the Platform Operator so as to demonstrate the basis of the assessment.

   (c) A Platform Operator should undertake a new assessment where a corporate professional investor has ceased to trade in virtual assets for more than ~~2~~ two years.

2. Procedures for dis-applying certain requirements when dealing with corporate professional investors

(a) Prior to dis-applying certain requirements[73] in these Guidelines, a Platform Operator should also:

(i) obtain a written and signed declaration from the client that the client has given consent; and

(ii) fully explain to the client the consequences (ie, all relevant regulatory exemptions that the Platform Operator is entitled to) of being treated as a professional investor and that the client has the right to withdraw from being treated as such at any time.

(b) A Platform Operator should carry out a confirmation exercise annually to ensure that the client continues to fulfil the requisite requirements under the Professional Investor Rules. In carrying out the annual confirmation exercise, a Platform Operator should remind the client in writing of:

(i) the risks and consequences (ie, all relevant regulatory exemptions that the Platform Operator is entitled to) of being treated as a professional investor, in particular, the Platform Operator is not required to comply with the regulatory requirements; and

(ii) the right for the client to withdraw from being treated as a professional investor.

[73] The following requirements are dis-applied for qualified corporate professional investors:
- The need to conduct virtual asset knowledge assessment (paragraph 9.4)
- The need to establish a client's financial situation, investment experience and investment objectives (paragraphs 5.1(d) and 9.5)
- The need to assess a client's risk tolerance level and risk profile (paragraph 9.6)
- The need to set an exposure limit (paragraph 9.7)
- The need to enter into a written agreement and the provision of relevant risk disclosure statements (paragraphs 9.11 and 9.26)
- The need to ensure the suitability of a recommendation or solicitation (paragraph 9.20)
- The need to ensure the suitability of a transaction in a complex product, to provide sufficient information about a complex product and to provide warning statements (paragraph 9.22)
- The need to provide adequate risk disclosures for opting out from "trade execution" notifications (paragraph 12.12(e))

Schedule 2 Risk Disclosure Statements

The following risk disclosures should be made to clients (where applicable):

(a) virtual assets are highly risky and investors should exercise caution in relation to the products;

(b) a virtual asset may or may not be considered "property" under the law, and such legal uncertainty may affect the nature and enforceability of a client's interest in such a virtual asset;

(c) the offering documents or product information provided by the issuer have not been subject to scrutiny by any regulatory body;

(d) the protection offered by the Investor Compensation Fund does not apply to transactions involving virtual assets (irrespective of the nature of the tokens);

(e) a virtual asset is not a legal tender, ie, it is not backed by the government and authorities;

(f) transactions in virtual assets may be irreversible, and, accordingly, losses due to fraudulent or accidental transactions may not be recoverable;

(g) the value of a virtual asset may be derived from the continued willingness of market participants to exchange fiat currency for a virtual asset, which means that the value of a particular virtual asset may be completely and permanently lost should the market for that virtual asset disappear. There is no assurance that a person who accepts a virtual asset as payment today will continue to do so in the future;

(h) the extreme volatility and unpredictability of the price of a virtual asset relative to fiat currencies may result in a total loss of the investment over a short period of time;

(i) legislative and regulatory changes may adversely affect the use, transfer, exchange and value of virtual assets;

(j) some virtual asset transactions may be deemed to be executed only when recorded and confirmed by the Platform Operator, which may not necessarily be the time at which the client initiates the transaction;

(k) the nature of virtual assets exposes them to an increased risk of fraud or cyberattack; and

(l) the nature of virtual assets means that any technological difficulties experienced by the Platform Operator may prevent clients from accessing their virtual assets.

Schedule ~~2~~3 Audit Logs and Incident Reports

Requirements for Audit Logs and Incident Reports

A Platform Operator should make arrangements to keep the audit logs and incident reports referred to in paragraphs 14.8(~~d~~e) and (~~e~~f) of these Guidelines. The logs and reports should be made available to the SFC upon request. It is important that the logs and reports be reviewed regularly for detecting potential problems and planning preventive measures.

1. Audit logs

   Audit logs should document the order process and transaction flow through the trading platform, where applicable. This should at a minimum include:

   (a) order placement/cancellation/modification/execution (with time stamping and the assignment of unique reference number);

   (b) system login attempts including login details such as user identity, date and time of the login attempts;

   (c) trading limits/-position limits/-cash limits validation exceptions - which for example, may include the logging of instances where the trading limits/ position limits/-cash limits have been exceeded, thereby causing the client to have exceeded the trading/-position limit or traded without cash upfront;

   (d) compliance validation exceptions – which for example may include logging exceptions where the client does not have sufficient holdings of virtual assets to actually sell them;

   (e) the assigning of hierarchical user access – where different levels of access are allocated to different job responsibilities within the Platform Operator;

   (f) details of the changes to critical system parameters and master files; and

   (g) erroneous order inputs – which for example may include order prices which materially deviated from the prevailing order prices or last traded prices, order sizes exceeding the client's trading limits, and orders in a virtual asset which do not accord to client instructions.

2. Incident reports

   Incident reports should document instances where the Platform Operator's platform or system experiences a material delay or failure that renders it unusable by clients. At a minimum, it should include:

   (a) a clear explanation of the problem, including the root cause analysis;

   (b) the time of outage or delay;

   (c) the duration of outage or delay;

   (d) the platforms or systems affected during outage or delay and subsequently;

(e) whether this problem or a related problem has occurred before;

(f) the number of clients affected at the time and the impact on these clients;

(g) the steps taken to rectify the problem; and

(h) steps taken to ensure that the problem does not occur again.

Schedule ~~43~~ Required Information and Notifications

~~A.~~ Terminology

"*Applicant*" means the person making an application under the SFC and/or the AMLO to the SFC.

"*CE number*" means the central entity identification number assigned by the SFC.~~;~~

"~~c~~*Complaints officer*", in relation to a Platform Operator, means a person appointed by the intermediary to handle complaints made to the Platform Operator.~~;~~

"~~c~~*Controlling person*", in relation to a corporation, means each of the directors, substantial shareholders and ultimate owners of the corporation.~~;~~

"~~c~~Criminal investigatory body" means the Hong Kong Police Force and the Independent Commission Against Corruption established under section 3 of the Independent Commission Against Corruption Ordinance (Cap. 204), and public bodies in Hong Kong or elsewhere carrying out criminal investigations.~~;~~

"*~~m~~Minor offence"* means an offence punishable by a fixed penalty under the Fixed Penalty (Traffic Contraventions) Ordinance (Cap. 237), the Fixed Penalty (Criminal Proceedings) Ordinance (Cap. 240) or the Fixed Penalty (Public Cleanliness and Obstruction) Ordinance (Cap. 570), or offence of a similar nature committed outside Hong Kong.~~;~~

"*~~p~~Permanent identity card"* has the meaning assigned to it by section 1A of the Registration of Persons Ordinance (Cap. 177).~~;~~

"*~~r~~Regulatory body"* includes the SFC, the Monetary Authority, a recognised exchange company, any professional body or association, an examination authority, an inspector appointed under any enactment, and other equivalent bodies or persons in Hong Kong or elsewhere~~; and~~.

"~~v~~*Valid business registration certificate*" has the meaning assigned to it by section 2(1) of the Business Registration Ordinance (Cap. 310).

In this Schedule, the terms "*basic information*" and "*relevant information*" shall be construed as follows:

Basic information

1. Basic information, in relation to an individual, means, in so far as applicable, the following particulars of the individual—

   (a) the title and the full personal name and surname in Chinese and English;

   (b) the date and place of birth;

   (c) gender;

   (d) the Chinese commercial code and the number on his or her identity card issued under the Registration of Persons Ordinance (Cap. 177), and, if he or she is not the holder of a permanent identity card, the number, the name of

the issuing agency and the date of expiry, of his or her passport, travel or other document issued by a competent government agency providing proof of identity;

(e) nationality;

(f) the business, residential and correspondence addresses; and

(g) the contact telephone and facsimile numbers and electronic mail~~email~~ address.

2. Basic information, in relation to a corporation, means, in so far as applicable, the following particulars of the corporation—

(a) the corporate name and business name in Chinese and English;

(b) former names and periods during which those names were used;

(c) the date and place of incorporation;

(d) the number of its valid business registration certificate;

(e) in the case of a corporation incorporated outside Hong Kong, the date of the certificate of registration issued in respect of the corporation under Part XI of the Companies Ordinance (Cap. 32) before it was repealed or section 777 of Part 16 of the Companies Ordinance (Cap. 622);

(f) the address of its registered office;

(g) the addresses of its places of business;

(h) the correspondence address; and

(i) the telephone and facsimile numbers, electronic mail ~~email~~ address and website address.

Relevant ~~Information~~information

3. Relevant information, in relation to an individual, means information on whether or not the individual is or has been, in Hong Kong or elsewhere—

(a) convicted of or charged with any criminal offence (other than a minor offence) whether or not evidence of such conviction is admissible in proceedings in Hong Kong or elsewhere;

(b) subject to any disciplinary action or investigation by a regulatory body or criminal investigatory body (as the case may be);

(c) subject to any order of the court or other competent authority for fraud, dishonesty or misfeasance;

(d) a substantial shareholder, ultimate owner or director of a corporation or business that is or has been subject to any disciplinary action or investigation by a regulatory body or criminal investigatory body (as the case may be), or involved in the management of such a corporation or business;

(e) a substantial shareholder, ultimate owner or director of a corporation or business that is or has been subject to any order of the court or other competent authority for fraud, dishonesty or misfeasance, or involved in the management of such a corporation or business;

(f) engaged in any judicial or other proceedings;

(g) a party to a scheme of arrangement, or any form of compromise, with his or her creditors;

(h) in default of compliance with any judgement or court order;

(i) a substantial shareholder, ultimate owner or director of a corporation or business that was wound up otherwise than by way of a members' voluntary winding up, or involved in the management of such a corporation or business;

(j) a partner of a firm which was dissolved other than with the consent of all the partners;

(k) bankrupt or aware of the existence of any matters that might render him or her insolvent or lead to the appointment of a provisional trustee of his or her property under the Bankruptcy Ordinance (Cap. 6);

(l) refused or restricted from the right to carry on any trade, business or profession for which a specific licence, registration or other authorisation is required by law;

(m) a substantial shareholder, ultimate owner or director of a corporation that has been refused or restricted from the right to carry on any trade, business or profession for which a specific licence, registration or other authorisation is required by law, or involved in the management of such corporation; and

(n) disqualified from holding the office of director.

4. Relevant information, in relation to a corporation, means information on whether or not the person is or has been, in Hong Kong or elsewhere —

(a) convicted of or charged with any criminal offence (other than a minor offence) whether or not evidence of such conviction is admissible in proceedings in Hong Kong or elsewhere;

(b) subject to any disciplinary action or investigation by a regulatory body or criminal investigatory body (as the case may be);

(c) subject to any order of the court or other competent authority for fraud, dishonesty or misfeasance;

(d) a substantial shareholder~~, ultimate owner~~ or director of a corporation or business that is or has been subject to any disciplinary action or investigation by a regulatory body or criminal investigatory body (as the case may be), or involved in the management of such a corporation or business;

(e) a substantial shareholder~~, ultimate owner~~ or director of a corporation or business that is or has been subject to any order of the court or other competent authority for fraud, dishonesty or misfeasance, or involved in the management of such a corporation or business;

(f) engaged in any judicial or other proceedings;

(g) a party to a scheme of arrangement, or any form of compromise, with its creditors;

(h) in default of compliance with any judgement or court order;

(i) a substantial shareholder~~, ultimate owner~~ or director of a corporation or business that was wound up otherwise than by way of a members' voluntary winding up, or involved in the management of such a corporation or business;

(j) a partner of a firm which was dissolved other than with the consent of all the partners;

(k) in the case of a corporation other than a registered institution, insolvent or aware of the existence of any matters that might render it insolvent or lead to the appointment of a liquidator;

(l) refused or restricted from the right to carry on any trade, business or profession for which a specific licence, registration or other authorisation is required by law; and

(m) a substantial shareholder~~, ultimate owner~~ or director of a corporation that has been refused or restricted from the right to carry on any trade, business or profession for which a specific licence, registration or other authorisation is required by law, or involved in the management of such corporation.

Applications

Part 1 – Applications by Platform Operators[74]

1. Basic information in respect of—

(a) the applicant;

(b) each controlling person of the applicant;

(c) each person who is, or is proposed to be, a responsible officer of the applicant;

(d) each subsidiary of the applicant that carries on any regulated activity or Relevant Activities; and

[74] Applications by Platform Operators include:
- an application under section 116 of the SFO and/or section 53ZRK of the AMLO by a corporation for a licence;
- an application under section 127 of the SFO and/or section 53ZRN of the AMLO by a Platform Operator for variation of the regulated activity and/or the VA service for which a Platform Operator is licensed; and
- an application under section 134 of the SFO by a Platform Operator for the grant of a modification or waiver, in relation to the Platform Operator, in respect of any conditions imposed on its licence.

(e) each related corporation of the applicant that carries on any regulated activity or Relevant Activities.

2. Basic information in respect of—

(a) any corporation that is, or is proposed to be, an Associated Entity of the applicant; and

(b) any person who is, or is proposed to be, an executive officer of an Associated Entity referred to in paragraph (a).

3. The name, correspondence address, contact telephone and facsimile numbers and electronic mail address of—

(a) each contact person appointed by the applicant as the person whom the SFC may contact in the event of market emergency or other urgent need; and

(b) each person who is, or is proposed to be, a complaints officer of the applicant.

4. In the case of an application for—

(a) variation, under section 127 of the SFO and/or section 53ZRN of the AMLO, of the regulated activity and/or the VA service for which the person is licensed; and

(b) the grant of a modification or waiver under section 134 of the SFO,

a statement setting out the nature of the application and the reasons for the application.

5. The details of any authorisation (however described) to carry on any regulated activity or Relevant Activities by an authority or regulatory organisation in Hong Kong or elsewhere in respect of each of the persons referred to in item 1.

6. The relevant information in respect of each of the persons referred to in item 1.

7. In so far as applicable, the employment record in respect of each of the persons referred to in item 1 stating, in relation to each employer—

(a) the name of his or her employer;

(b) the position in which he or she is, or was, employed; and

(c) the dates of such employment.

8. The nature of the business carried on or to be carried on and types of services provided or to be provided by the applicant.

9. Information relating to the human and technical resources, operational procedures and organisational structures of the applicant showing that it is capable of carrying on its Relevant Activities, and its proposed Relevant Activities, competently.

10. The business history (if any) of the applicant and a business plan of the applicant covering internal controls, organisational structure, contingency plans and related matters.

11. The capital and shareholding structure of the applicant and the basic information in respect of any person in accordance with whose directions or instructions it is, or its directors are, accustomed or obliged to act.

12. Whether any assets of the applicant are subject to any charge (including pledge, lien or encumbrance), and if so, the following particulars—

(a) the date on which the assets are subject to the charge;

(b) a description of the assets; and

(c) the amount secured under the charge.

13. The particulars in respect of wallet addresses of the Platform Operator or its Associated Entity relating to the conduct of Relevant Activities stating—

(a) whether a wallet address has been created or is active or has become dormant or ordered to be frozen by a competent authority;

(b) the full wallet address along with the name of its associated blockchain protocol; and

(c) whether the wallet address is or was designated for holding client virtual assets or assets belonging to the Platform Operator.

14. In the case of a person applying to be licensed as a Platform Operator, the following particulars in respect of any bank account that the person has opened for the purpose of carrying on Relevant Activities—

(a) the name of the bank with which the account is opened;

(b) the number of the account; and

(c) whether the account is or was a trust account.

15. The name of the auditor of the applicant and the date of his or her appointment.

16. The address of each of the premises where—

(a) the business of the applicant is, or is to be, conducted; and

(b) records or documents of the applicant are, or are to be, kept.

17. In the case of a person applying to be licensed as a Platform Operator, whether any substantial shareholder of the Platform Operator, ultimate owner of the Platform Operator or both that is an individual has ever been a patient as defined in section 2 of the Mental Health Ordinance (Cap. 136).

18. In the case of a person applying to be licensed as a Platform Operator, the financial information in respect of the person showing that the person is capable of meeting its obligations under Part VI (Financial Soundness) above.

Part 2 – Applications by licensed representatives[75]

1. Basic information and CE number (if any) in respect of—

   (a) the applicant; and

   (b) the Platform Operator to which the applicant is accredited or seeks to be accredited.

2. In the case of an application for—

   (a) variation, under section 127 of the SFO and/or section 53ZRN of the AMLO, of the regulated activity and/or the VA service for which the person is licensed; and

   (b) the grant of a modification or waiver of conditions under section 134 of the SFO,

   a statement setting out the nature of the application and the reasons for the application.

3. The details of any authorisation (however described) to carry on any regulated activity or Relevant Activities of the applicant by an authority or regulatory organisation in Hong Kong or elsewhere, and whether the applicant's travel document is endorsed with a condition of stay prohibiting him or her from taking employment in Hong Kong.

4. The types of services provided or to be provided by the applicant on behalf of the Platform Operator to which the applicant is accredited or seeks to be accredited.

5. A description of any current directorship, partnership or proprietorship of the applicant and the dates of appointment, or commencement, of any such directorship, partnership or proprietorship (as the case may be).

6. The relevant information in respect of the applicant.

7. In so far as applicable, the following details in respect of each of the persons referred to in item 1—

[75] Applications by licensed representatives include:
- an application under section 120(1) or of the SFO and/or sections 53ZRL(1) and (2) of the AMLO by an individual for a licence;
- an application under section 122(1) of the SFO and/or section 53ZRM(1) of the AMLO by a licensed representative for approval of his or her accreditation, or under section 122(2) of the SFO and/or section 53ZRM(2) of the AMLO for approval of the transfer of his or her accreditation to another Platform Operator;
- an application under section 126 of the SFO and/or section 53ZRP of the AMLO by a licensed representative for approval as a responsible officer of a Platform Operator to which he or she is accredited;
- an application under section 127 of the SFO and/or section 53ZRN of the AMLO by a licensed representative for variation of the regulated activity and/or the VA service for which the representative is licensed; and
- an application under section 134 of the SFO by a licensed representative for the grant of a modification or waiver in respect of any condition imposed on the representative's licence.

(a) his or her academic record stating—

(i) the names of post secondary educational or vocational establishments that he or she has attended;

(ii) the courses completed at such establishments and the dates when those courses were attended;

(iii) the examinations passed to obtain any post secondary educational or vocational qualification; and

(iv) in the case of a person who has not obtained a post secondary educational or vocational qualification, whether or not he or she has obtained passes in the Hong Kong Certificate of Education Examination, or equivalent examinations, in the following subjects—

(I) Chinese or English language; and

(II) Mathematics;

(b) his or her professional record stating—

(i) the names of educational or vocational establishments that he or she has attended;

(ii) the courses completed at such establishments and the dates when those courses were attended; and

(iii) the details of any professional qualifications obtained; and

(c) his or her employment record stating, in relation to each employer—

(i) the name of his or her employer;

(ii) the position in which he or she is, or was, employed; and

(iii) the dates of such employment.

8. Whether the applicant has ever been a patient as defined in section 2 of the Mental Health Ordinance (Cap. 136).

Part 3 – Other applications[76]

1. Basic information in respect of—

(a) the applicant;

(b) each controlling person of the applicant;

(c) each person who is, or is proposed to be, a responsible officer of the applicant;

(d) each subsidiary of the applicant that carries on any regulated activity or Relevant Activities; and

(e) each related corporation of the applicant that carries on any regulated activity or Relevant Activities.

2. Basic information in respect of—

(a) any corporation that is, or is proposed to be, an Associated Entity of the applicant; and

(b) any person who is, or is proposed to be, an executive officer of an Associated Entity referred to in paragraph (a).

3. In the case of an application for—

(a) any matter requiring the approval of the SFC under Part V of the SFO (other than those matters referred to in sections 128(1)(a), (b), (c), (d), (e), (f), (g) and (h) of the SFO) and/or under Part 5B of the AMLO (other than those matters referred to in sections 53ZTI(a), (b), (c), (d), (e) and (f) of the AMLO); and

(b) the grant of a modification or waiver under section 134 of the SFO,

a statement setting out the nature of the application and the reasons for the application.

4. In the case of a person applying for approval of premises under section 130(1) of the SFO and/or section 53ZRR(2) of the AMLO—

(a) the address of each of the premises where records or documents required under the SFO and/or the AMLO are to be kept by the applicant; and

[76] Other applications include:
- an application under section 130(1) of the SFO and/or section 53ZRR(2) of the AMLO by a person for approval of premises to be used by a Platform Operator for keeping records or documents required;
- an application under section 132 of the SFO, section 53ZRQ of the AMLO or both sections by a person for approval to become or continue to be (as the case may be) a substantial shareholder of a Platform Operator, an ultimate owner of a Platform Operator or both;
- an application under section 134 of the SFO by a person (other than a Platform Operator or a licensed representative) for the grant of a modification or waiver in respect of any condition imposed on that person; and
- an application by a person under any matter requiring the SFC's approval under Part V of the SFO and/or Part 5B of the AMLO.

(b) evidence that the premises are suitable for being used for the purpose of keeping records or documents required under the SFO and/or the AMLO.

5. The relevant information in respect of each of the persons referred to in item 1.

6. In the case of a person applying for approval to become or continue to be (as the case may be) a substantial shareholder of a Platform Operator, an ultimate owner of a Platform Operator or both, under section 132 of the SFO, section 53ZRQ of the AMLO or both sections—

(a) the financial information in respect of the applicant showing that the person is a fit and proper person to be a substantial shareholder of the Platform Operator, an ultimate owner of the Platform Operator or both;

(b) the details of any authorisation (however described) to carry on any regulated activity or Relevant Activities by an authority or regulatory organisation in Hong Kong or elsewhere in respect of each of the persons referred to in item 1;

(c) in so far as applicable, the employment record in respect of each of the persons referred to in item 1 stating, in relation to each employer—

(i) the name of his or her employer;

(ii) the position in which he or she is, or was, employed; and

(iii) the dates of such employment.

7. In the case of an individual applying to be approved as a substantial shareholder of a Platform Operator, an ultimate owner of a Platform Operator or both, whether he or she has ever been a patient as defined in section 2 of the Mental Health Ordinance (Cap. 136).

~~B.~~ Notifications of changes

Part ~~1~~ 4 – Changes to be notified by Platform Operators

1. Changes in the basic information in respect of—

(a) the Platform Operator;

(b) each controlling person of the Platform Operator;

(c) each person who is a responsible officer of the Platform Operator; and

(d) each subsidiary of the Platform Operator that carries on any Relevant Activities.

2. Changes in the persons who are controlling persons, responsible officers or subsidiaries of the Platform Operator that carry on a business in any Relevant Activities.

3. Changes in the following particulars of any corporation that is, or becomes, or ceases to be, an Associated Entity of the Platform Operator—

~~(a) in the case where the corporation is licensed by or registered with the SFC—~~

~~(i) the basic information in respect of the corporation;~~

~~(ii) its CE number;~~

~~(iii) the date of its becoming, or ceasing to be, an Associated Entity;~~

~~(iv) whether it has any executive officers; and~~

~~(v) the basic information in respect of its executive officers (if any); and~~

~~(b) in any other case—~~

(a) ~~(i)~~ the basic information in respect of the corporation;

(b) ~~(ii)~~ the date of its becoming, or ceasing to be, an Associated Entity;

(c) ~~(iii)~~ whether it has any executive officers;

(d) ~~(iv)~~ the basic information in respect of its executive officers (if any);

(e) ~~(v)~~ in the case of a corporation becoming an Associated Entity, the facts that gave rise to the corporation becoming an Associated Entity; and

(f) ~~(vi)~~ in the case of a corporation ceasing to be an Associated Entity, the facts that gave rise to the corporation ceasing to be an Associated Entity and confirmation that all client assets of the Platform Operator that are received or held by the corporation prior to its ceasing to be an Associated Entity have been fully accounted for and properly disposed of and, if not, the particulars of any such client assets of the Platform Operator that have not been fully accounted for and properly disposed of.

4. Changes in the name, correspondence address, contact telephone and facsimile numbers and electronic mail ~~email~~ address of—

(a) each contact person appointed by the Platform Operator as the person whom the SFC may contact in the event of market emergency or other urgent need; and

(b) each person who is, or is proposed to be, a complaints officer of the Platform Operator.

5. Changes in the status of any authorisation (however described) to carry on any regulated activity or Relevant Activities by an authority or regulatory organisation in Hong Kong or elsewhere in respect of each of the persons referred to in item 1.

6. Changes in the relevant information in respect of each of the persons referred to in item 1.

7. Significant changes in the scope and nature of the business carried on or to be carried on and types of services provided or to be provided by the Platform Operator.

8. Significant changes in the business plan of the Platform Operator covering internal controls, organisational structure, contingency plans and related matters.

9. Changes in the capital and shareholding structure of the Platform Operator and the basic information in respect of any person in accordance with whose directions or instructions the Platform Operator is, or its directors are, accustomed or obliged to act.

10. Changes in the information in respect of any assets of the Platform Operator that are subject to any charge (including pledge, lien or encumbrance).

11. Changes in the particulars in respect of wallet addresses of the Platform Operator or its Associated Entity relating to the conduct of Relevant Activities stating—

    (a) whether a wallet address has been created or is active or has become dormant or ordered to be frozen by a competent authority;

    (b) the full wallet address along with the name of its associated blockchain protocol; and

    (c) whether the wallet address is or was designated for holding client virtual assets or assets belonging to the Platform Operator.

12. Changes in the particulars in respect of bank accounts of the Platform Operator relating to the conduct of Relevant Activities stating—

    (a) whether an account has been opened or closed or has become dormant or ordered to be frozen by a competent authority;

    (b) the name of the bank with which the account has been opened or closed or has become dormant or ordered to be frozen by a competent authority;

    (c) the number of the account;

    (d) the date of opening or closing any such account; and

    (e) whether the account is or was a trust account.

13. Changes in the name of the auditor of the Platform Operator and the reasons for the change in the auditor.

14. Changes in the address of each of the premises where the business of the Platform Operator is, or is to be, conducted.

15. The address of each of the premises where records or documents of the Platform Operator are no longer kept.

Part 5 – Changes to be notified by Associated Entities

1. Changes in the following particulars of any corporation that becomes an Associated Entity—

    (a) the name of the Platform Operator;

(b) the date of its becoming an Associated Entity;

(c) its name and business name (if different);

(d) the date and place of its incorporation;

(e) its telephone and facsimile number, electronic mail address and website address (if any);

(f) each of the following addresses, together with its effective date—

(i) the address of its principal place of business in Hong Kong (if any);

(ii) the address of its registered office;

(iii) its correspondence address; and

(iv) the address of each of the premises where books and records relating to client assets of the Platform Operator, received or held by it in Hong Kong, are kept;

(g) the details of its bank account for holding client assets of the Platform Operator received or held in Hong Kong, including—

(i) the name of the bank with which the account is opened; and

(ii) the number of the account;

(h) whether it is aware of the existence of any matter that might render it insolvent or lead to the appointment of a liquidator;

(i) the facts that gave rise to its becoming such an Associated Entity; and

(j) in relation to each of its executive officers who are its directors responsible for directly supervising the receiving or holding of the client assets of the Platform Operator—

(i) the executive officer's name;

(ii) the executive officer's Hong Kong identity card number, or details of documents issued by a competent government agency providing proof of identity; and

(iii) the executive officer's contact details, including residential address in Hong Kong (if any) and correspondence address.

2. Changes in the following particulars of any corporation that ceases to be an Associated Entity—

(a) the date of ceasing to be such an Associated Entity;

(b) the name of the Platform Operator;

(c) whether all client assets of the Platform Operator received or held by it before it ceases to be such an Associated Entity have been fully accounted for and properly disposed of and, if not, the particulars of any such client assets that have not been fully accounted for and properly disposed of; and

(d) the facts that gave rise to its ceasing to be such an Associated Entity.

Part ~~2~~ 6 – Changes to be notified by licensed representatives

1. Changes in the basic information in respect of the licensed representative.

2. Changes in the status of any authorisation (however described) to carry on any regulated activity or Relevant Activities by an authority or regulatory organisation in Hong Kong or elsewhere in respect of the licensed representative.

3. Significant changes in the types of services provided or to be provided by the licensed representative on behalf of the Platform Operator to which the licensed representative is accredited or seeks to be accredited.

4. Changes in the relevant information in respect of the licensed representative.

5. Changes in whether the licensed representative has ever been a patient as defined in section 2 of the Mental Health Ordinance.

6. Changes in the status of any directorships, partnerships or proprietorships of the licensed representative.

Part ~~3~~ 7 – Changes to be notified by substantial shareholders and ultimate owners

1. Changes in the basic information in respect of the substantial shareholder or ultimate owner.

2. Changes in the relevant information in respect of the substantial shareholder or ultimate owner.

3. Significant changes in the capital and shareholding structure of the substantial shareholder ~~or ultimate owner~~.

4. Changes in whether the substantial shareholder or ultimate owner has ever been a patient as defined in section 2 of the Mental Health Ordinance (if applicable).

App B to Consultation Conclusions

SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset Service Providers)

~~September~~June 202~~3~~1

April 2012 first edition
July 2012 second edition
April 2015 third edition
March 2018 fourth edition
November 2018 fifth edition
September 2021 sixth edition
June 2023 seventh edition

Published by
Securities and Futures Commission
54/F, One Island East
18 Westlands Road
Quarry Bay
Hong Kong
Tel : (852) 2231 1222
Fax : (852) 2521 7836
E-mail : enquiry@sfc.hk
SFC website : www.sfc.hk

Content

Chapter 1 – OVERVIEW

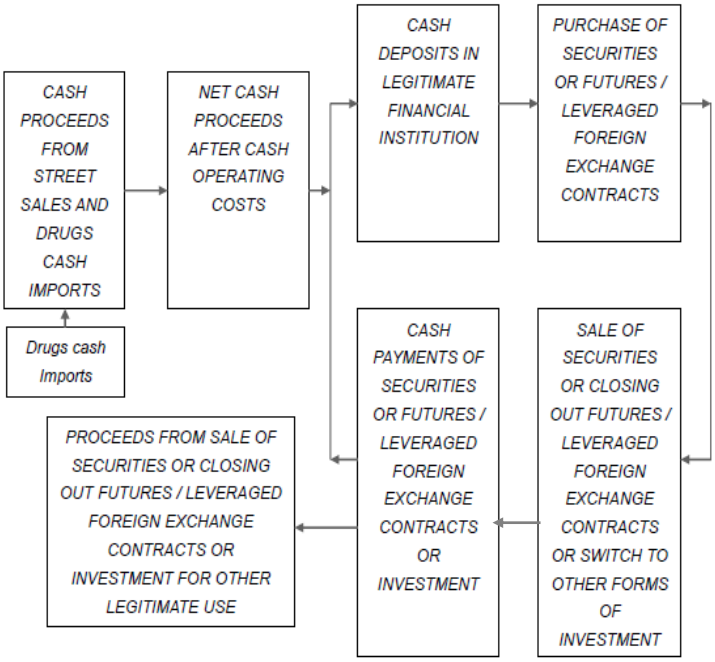
Introduction		
	1.1	This Guideline is published under sections 7 and 53ZTK of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap. 615 (the AMLO), and section 399 of the Securities and Futures Ordinance, Cap. 571 (the SFO).
	1.2	Terms and abbreviations used in this Guideline shall be interpreted by reference to the definitions set out in the Glossary part of this Guideline.
	1.3	Where applicable, interpretation of other words or phrases should follow those set out in the AMLO or the SFO. Unless the context otherwise requires, the term financial institutions (FIs) refers to licensed corporations (LCs) and virtual asset service providers licensed by the Securities and Futures Commission (SFC) under the AMLO (SFC-licensed VAS Providers).
	1.4	This Guideline is issued by the ~~Securities and Futures Commission (~~SFC~~)~~ 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 LCs and SFC-licensed VAS Providers should meet in order to comply with the statutory requirements under the AMLO and the SFO. Compliance with this Guideline is enforced through the AMLO and the SFO. LCs and SFC-licensed VAS Providers which fail to comply with this Guideline may be subject to disciplinary or other actions under the AMLO and/or the SFO for non-compliance with the relevant requirements.
	1.5	This Guideline is intended for use by FIs 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 FIs 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.
	1.6	In addition to the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) issued by the Hong Kong Monetary Authority (HKMA) for use by authorized institutions, registered institutions (RIs) are required to have regard to paragraph 4.1.6 of this Guideline for the definition of "customer" for the securities, futures and leveraged foreign exchange businesses (hereafter collectively referred to as "securities sector" or "securities businesses"), paragraphs 4.20 of this Guideline for the provisions on cross-border correspondent relationships applicable to the securities sector, Chapter 12 of this Guideline for the provisions in relation to virtual assets, and Appendix B to this Guideline for illustrative indicators of suspicious transactions and activities in the securities sector.
	1.7	The relevance and usefulness of this Guideline will be kept under review and it may be necessary to issue amendments from time to time.
	1.8	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. Given the significant differences that exist in the organisational and legal structures of different FIs as well as the nature and scope of the business

		activities conducted by them, there exists no single set of universally applicable implementation measures. The content of this Guideline is not intended to be an exhaustive list of the means of meeting the statutory and regulatory requirements. FIs therefore should use this Guideline as a basis to develop measures appropriate to their structure and business activities.
	1.9	This Guideline also provides guidance in relation to the operation of the provisions of Schedule 2 to the AMLO (Schedule 2).
s.7, & s.53ZTK(5) & (6)(b), AMLO, s.399(6), SFO	1.10	A failure by any person to comply with any provision of this Guideline does not by itself render the person liable to any judicial or other proceedings but, in any proceedings under the AMLO or the SFO before any court, this Guideline is admissible in evidence; and if any provision set out in this Guideline appears to the court to be relevant to any question arising in the proceedings, the provision must be taken into account in determining that question. In considering whether a person has contravened a provision of Schedule 2, the SFC must have regard to any relevant provision in this Guideline.
s.193 & s.194, SFO, s.53ZTK (6)(a), AMLO	1.11	In addition, a failure to comply with any of the requirements of this Guideline by LCs or SFC-licensed VAS Providers and (where applicable) licensed representatives may reflect adversely on their fitness and properness and may be considered to be misconduct.
s.193 & s.196, SFO	1.12	Similarly, a failure to comply with any of the requirements of the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) issued by the HKMA for use by authorized institutions or to have regard to paragraphs 4.1.6 and 4.20 of, Chapter 12 of, and Appendix B to this Guideline by RIs may reflect adversely on their fitness and properness and may be considered to be misconduct.

The nature of money laundering and terrorist financing		
s.1, Sch. 1, AMLO	1.13	The term "money laundering" is defined in section 1 of Part 1 of Schedule 1 to the AMLO and 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.
	1.14	There are three common stages in the laundering of money, and they frequently involve numerous transactions. An FI 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 into the financial system; (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.
Potential uses of the securities sector in the money laundering process		
	1.15	Since the securities businesses are no longer

		predominantly cash based, they are less conducive to the initial placement of criminally derived funds than other financial industries, such as banking. Where, however, the payment underlying these transactions is in cash, the risk of these businesses being used as the placement facility cannot be ignored, and thus due diligence must be exercised.
	1.16	The securities businesses are more likely to be used at the second stage of money laundering, i.e. the layering process. Unlike laundering via banking networks, these businesses provide a potential avenue which enables the launderer to dramatically alter the form of funds. Such alteration may not only allow conversion from cash in hand to cash on deposit, but also from money in whatever form to an entirely different asset or range of assets such as securities or futures contracts, and, given the liquidity of the markets in which these instruments are traded, with potentially great frequency.
	1.17	Investments that are cash equivalents, e.g. bearer bonds and similar investments in which ownership can be evidenced without reference to registration of identity, may be particularly attractive to the money launderer.
	1.18	As mentioned, transactions in the securities sector may prove attractive to money launderers due to the liquidity of the reference markets. The combination of the ability to readily liquidate investment portfolios procured with both licit and illicit proceeds, the ability to conceal the source of the illicit proceeds, the availability of a vast array of possible investment mediums, and the ease with which transfers can be effected between them, offers money launderers attractive ways to effectively integrate criminal proceeds into the general economy.
	1.19	The chart set out below illustrates the money laundering process relevant to the securities sector

		in detail.  Other examples of money laundering methods and characteristics of financial transactions that have been linked with terrorist financing can be found on the websites of the Joint Financial Intelligence Unit (JFIU) (www.jfiu.gov.hk) and the Financial Action Task Force (FATF) (www.fatf-gafi.org).
s.1, Sch. 1, AMLO	1.20	The term “terrorist financing” is defined in section 1 of Part 1 of Schedule 1 to the AMLO and 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); or (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.
	1.21	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 ML, TF, financing of proliferation of weapons of mass destruction (PF) and financial sanctions		
	1.22	The FATF is an inter-governmental body established 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, 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 AML/CFT requirements as promulgated by the FATF, which include the latest FATF Recommendations[1] 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.
	1.23	The main pieces of legislation in Hong Kong that are concerned with ML, TF, PF and financial sanctions are the AMLO, the Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP), the Organized and Serious Crimes Ordinance (OSCO), 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). It is very important that FIs and their officers and staff fully understand their respective responsibilities under the different legislation.
<u>AMLO</u>		
s.23, Sch. 2	1.24	The AMLO imposes requirements relating to customer due diligence (CDD) and record-keeping on FIs and provides relevant authorities (RAs) with the powers to supervise compliance with these requirements and other requirements under the AMLO. In addition, section 23 of Schedule 2 requires FIs to take all reasonable measures (a) to ensure that proper safeguards exist to prevent a contravention of any requirement under Parts 2 and 3 of Schedule 2; and (b) to mitigate ML/TF risks.
s.5, AMLO	1.25	The AMLO makes it a criminal offence if an FI (1) knowingly; or (2) with the intent to defraud any RA, contravenes a specified provision of the AMLO. The "specified provisions" are listed in section 5(11) of the AMLO. If the FI knowingly contravenes a specified

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

		provision, it is liable to a maximum term of imprisonment of 2 years and a fine of $1 million upon conviction. If the FI contravenes a specified provision with the intent to defraud any RA, it is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.
s.5, AMLO	1.26	The AMLO also makes it a criminal offence if a person who is an employee of an FI or is employed to work for an FI or is concerned in the management of an FI (1) knowingly; or (2) with the intent to defraud the FI or any RA, causes or permits the FI to contravene a specified provision in the AMLO. If the person who is an employee of an FI or is employed to work for an FI or is concerned in the management of an FI knowingly contravenes a specified provision, he is liable to a maximum term of imprisonment of 2 years and a fine of $1 million upon conviction. If that person does so with the intent to defraud the FI or any RA, he is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.
s.21 ~~&~~ s.53ZSP, AMLO	1.27	RAs may take disciplinary actions against FIs for any contravention of a specified provision in the AMLO. The disciplinary actions that can be taken include publicly reprimanding the FI; ordering the FI to take any action for the purpose of remedying the contravention; and ordering the FI to pay a pecuniary penalty not exceeding the greater of $10 million or 3 times the amount of profit gained, or costs avoided, by the FI as a result of the contravention.
DTROP		
	1.28	The DTROP contains provisions for the investigation of assets that are suspected to be derived from drug trafficking activities, the freezing of assets on arrest and the confiscation of the proceeds from drug trafficking activities upon conviction.

OSCO		
	1.29	The OSCO, among other things: (a) gives officers of the Hong Kong Police Force 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 ML 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		
	1.30	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	1.31	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 $5 million.
s.6, s.7, s.8, s.8A,	1.32	The UNATMO, among other things, criminalises the

s.13 & s.14, UNATMO		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 & s.14, UNATMO	1.33	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 $50,000 upon conviction.
s.25A, DTROP & OSCO, s.12 & s.14, UNATMO	1.34	"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		
	1.35	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. Most UNSCRs are implemented in Hong Kong under the UNSO.
WMD(CPS)O		
s.4, WMD(CPS)O	1.36	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 2 – RISK-BASED APPROACH

Introduction		
	2.1	Applying an AML/CFT risk-based approach (RBA) is recognised as an effective way to combat ML/TF. The RBA to AML/CFT means that countries, competent authorities and FIs should identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures that are commensurate with those risks in order to mitigate them effectively. The use of an RBA allows an FI to allocate its resources in the most efficient way in accordance with priorities so that the greatest risks receive the highest attention. Therefore, FIs should have in place a process to identify, assess and understand the ML/TF risks to which they are exposed (hereafter referred to as "institutional risk assessment"), so as to facilitate the design and implementation of adequate and appropriate internal AML/CFT policies, procedures and controls (hereafter collectively referred to as "AML/CFT Systems"[2]) that are commensurate with the ML/TF risks identified in order to properly manage and mitigate them. FIs should also assess the ML/TF risks associated with a customer or proposed business relationship (hereafter referred to as "customer risk assessment") to determine the degree, frequency or extent of CDD measures and ongoing monitoring conducted which should vary in accordance with the assessed ML/TF risks associated with the customer or business relationship[3].

[2] Guidance on AML/CFT Systems is provided in Chapter 3.

[3] Illustrative examples of possible simplified and enhanced measures are set out in paragraphs 1 and 2 of Appendix C respectively.

Institutional risk assessment		
	2.2	An institutional risk assessment enables an FI to understand how, and to what extent, it is vulnerable to ML/TF.
	2.3	An FI should take appropriate steps to identify, assess, and understand its ML/TF risks which should include: (a) considering all relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigating measures to be applied (see paragraphs 2.6 –to 2.8); (b) keeping the risk assessment up-to-date (see paragraph 2.9); (c) documenting the risk assessment (see paragraph 2.10); (d) obtaining the approval of senior management of the risk assessment results (see paragraph 2.11); and (e) having appropriate mechanisms to provide risk assessment information to RAs upon request.
	2.4	In conducting the institutional risk assessment, an FI should consider quantitative and qualitative information obtained from relevant internal and external sources to identify, manage and mitigate the risks. This may include consideration of relevant risk assessments and guidance issued by the FATF, inter-governmental organisations, governments and authorities from time to time, including Hong Kong's jurisdiction-wide ML/TF risk assessment and any higher risks notified to the FIs by the SFC.
	2.5	The nature and extent of institutional risk assessment procedures should be commensurate with the nature, size and complexity of the business of an FI. For FIs whose businesses are smaller in size or less complex in nature (for example, where the range of products and services offered by the FI are very

		limited or its customers have a homogeneous risk profile), a simpler risk assessment approach might suffice. Conversely, where the FI's products and services are more varied and complex, or the FI's customers have more diverse risk profiles, a more sophisticated risk assessment process will be required.
<u>Considering relevant risk factors</u>		
	2.6	An FI should holistically take into account relevant risk factors including country risk, customer risk, product/service/transaction risk, delivery/distribution channel risk and, where applicable, other risks that the FI is exposed to, depending on its specific circumstances. While there is no complete set of risk indicators, the list of illustrative risk indicators set out in Appendix A may help identify a higher or lower level of risk associated with the risk factors stated above that may be present in the business operations of an FI or its customer base and should be taken into account holistically whenever relevant in the institutional risk assessment.
	2.7	In determining the level of overall risk that the FI is exposed to, an FI should holistically consider a range of factors, including: (a) country risk, for example, the jurisdictions in which the FI is operating or otherwise exposed to, either through its own activities or the activities of customers, especially jurisdictions with greater vulnerability due to contextual and other risk factors such as: (i) the prevalence of crime, corruption, or financing of terrorism; (ii) the general level and quality of the jurisdiction's law enforcement efforts related to AML/CFT; (iii) the regulatory and supervisory regime and controls; and

		(iv) transparency of beneficial ownership[4]; (b) customer risk, for example, the proportion of customers identified as high risk; (c) product/service/transaction risk, for example, (i) the characteristics of the products and services that it offers and transactions it executes, and the extent to which these are vulnerable to ML/TF abuse; (ii) the nature, diversity and complexity of its business, products and target markets; and (iii) whether the volume and size of transactions are in line with the usual activity of the FI and the profile of its customers; (d) delivery/distribution channel risk, for example, the distribution channels through which the FI distributes its products, including: (i) the extent to which the FI deals directly with the customer, the extent to which it relies on third parties to conduct CDD or other AML/CFT obligations and the extent to which the delivery/distribution channels are vulnerable to ML/TF abuse; and (ii) the complexity of the transaction chain (e.g. layers of distribution and sub-distribution); and (e) other risks, for example, the review results of compliance, internal and external audits, as well as regulatory findings.
	2.8	An FI should also 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 (especially those that may lead to misuse of technological developments or facilitate anonymity in ML/TF schemes); and (b) the use of new or developing technologies for

[4] For example, the availability of adequate, accurate and timely information on the beneficial ownership of legal persons and legal arrangements that can be obtained or accessed in a timely fashion by competent authorities in the country.

		both new and pre-existing products, prior to the launch of the new products, new business practices or the use of new or developing technologies. The FI should take appropriate measures to mitigate and manage the risks identified.
Keeping risk assessment up-to-date		
	2.9	An FI should review the institutional risk assessment at least every 2 years, or more frequently upon trigger events with material impact on the firm's business and risk exposure (e.g. a significant breach of the FI's AML/CFT Systems, the acquisition of new customer segments or delivery channels, the launch of new products and services by the FI, or a significant change of the FI's operational processes).
Documenting risk assessment		
	2.10	An FI should maintain records and relevant documents of the institutional risk assessment, including the risk factors identified and assessed, the information sources taken into account, and the evaluation made on the adequacy and appropriateness of the FI's AML/CFT Systems.
Obtaining senior management approval		
	2.11	The institutional risk assessment should be communicated to, reviewed and approved by the senior management of the FI.
Other considerations		
	2.12	A Hong Kong incorporated FI with overseas branches and subsidiary undertakings that carry on the same business as an FI as defined in the AMLO should conduct a group-wide ML/TF risk assessment, to facilitate the FI to design and implement group-wide AML/CFT Systems as referred to in paragraph 3.13.

		If an FI 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 the ML/TF risks posed to the FI in the local context.
Customer risk assessment		
	2.13	An FI should assess the ML/TF risks associated with a customer or a proposed business relationship. The information obtained in the initial stages of the CDD process should enable an FI to conduct a customer risk assessment, which would determine the level of CDD measures[5] to be applied. The measures must however comply with the legal requirements of the AMLO[6]. The general principle is that the amount and type of information obtained, and the extent to which this information is verified, should be increased where the risk associated with the business relationship is higher, or may be decreased where the associated risk is lower.
	2.14	Based on a holistic view of the information obtained in the course of performing CDD measures, an FI should be able to finalise the customer risk assessment, which determines the level and type of ongoing monitoring (including keeping customer information up-to-date and transaction monitoring), and supports the decision of the FI whether to enter into, continue or terminate the business relationship. While a customer risk assessment should always be

[5] Illustrative examples of possible simplified and enhanced measures are set out in paragraphs 1 and 2 of Appendix C respectively.

[6] FIs should have regard, in particular, to section 4 of Schedule 2 which permits FIs not to identify and take reasonable measures to verify the identities of the beneficial owners of specific types of customers, or in relation to specific types of products related to the transactions of the customers; and sections 8 to 15 of Schedule 2 which require FIs to comply with some special requirements in relation to specific types of customers, products, transactions or other high risk situations. Further guidance is set out in Chapter 4.

		performed at the inception of a business relationship with a customer, a comprehensive risk profile for some customers may only become evident through time or based upon information received from a competent authority after establishing the business relationship. Therefore, an FI may have to periodically review and, where appropriate, update its risk assessment of a particular customer and adjust the extent of the CDD and ongoing monitoring to be applied to the customer.
	2.15	An FI should keep its policies and procedures under regular review and assess that its risk mitigation procedures and controls are working effectively.
<u>Conducting risk assessment</u>		
	2.16	An FI may assess the ML/TF risks of a customer by assigning a ML/TF risk rating to its customers.
	2.17	Similar to other parts of the AML/CFT Systems, an FI should adopt an RBA in the design and implementation of its customer risk assessment framework, and the framework should be designed taking into account the results of the institutional risk assessment of the FI and commensurate with the risk profile and complexity of its customer base. The customer risk assessment should holistically take into account relevant risk factors of a customer including the country risk, customer risk, product/service/transaction risk, and delivery/distribution channel risk. While there is no agreed upon set of indicators, the list of illustrative risk indicators set out in Appendix A may identify a higher or lower level of risk associated with the risk factors stated above and should be taken into account holistically whenever relevant in determining the ML/TF risk rating of a customer.

Documenting risk assessment		
s.20(1)(b)(ii), Sch. 2	2.18	An FI should keep records and relevant documents of the customer risk assessment so that it can demonstrate to the RAs, among others: (a) how it assesses its 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.

Chapter 3 – AML/CFT SYSTEMS

Introduction		
s.23(a) & (b), Sch. 2	3.1	An FI must take all reasonable measures to ensure that proper safeguards exist to mitigate the risks of ML/TF and to prevent a contravention of any requirement under Part 2 or 3 of Schedule 2. To ensure compliance with this requirement, an FI should implement appropriate AML/CFT Systems that are commensurate with the risks identified in its risk assessments.
	3.2	An FI should: (a) have AML/CFT Systems, which are approved by senior management, to enable the FI to manage and mitigate the risks that have been identified; (b) monitor the implementation of the AML/CFT Systems and make enhancements if necessary; and (c) implement enhanced AML/CFT Systems to manage and mitigate the risks where higher risks are identified[7].
	3.3	An FI may implement simplified AML/CFT Systems to manage and mitigate the risks if lower risks are identified, provided that: (a) the FI complies with the statutory requirements set out in Schedule 2; (b) the lower ML/TF risk assessment is supported by an adequate analysis of risks having regard to the relevant risk factors and risk indicators; (c) the simplified AML/CFT Systems are commensurate with the lower ML/TF risks

[7] Depending on the assessed ML/TF risks, RBA may be applied on a specific customer segment, a specific line of business, or a specific product or service offered. For example, where a line of business is assessed to carry higher ML/TF risks, the FI should implement enhanced AML/CFT Systems with respect to the specific line of business (e.g. more frequent internal audit review or more frequent reporting to senior management).

		identified; and (d) the simplified AML/CFT Systems, which are approved by senior management, are subject to review from time to time. For the avoidance of doubt, an FI must not implement simplified AML/CFT Systems whenever there is any suspicion of ML/TF.
AML/CFT Systems		
	3.4	Having regard to the nature, size and complexity of its businesses and the ML/TF risks arising from those businesses, an FI should implement adequate and appropriate AML/CFT Systems which should include: (a) compliance management arrangements; (b) independent audit function; (c) employee screening procedures; and (d) an ongoing employee training programme (see Chapter 9).
Compliance management arrangements		
	3.5	An FI should have appropriate compliance management arrangements that facilitate the FI 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 FI's senior management, and appointment of a Compliance Officer (CO) and a Money Laundering Reporting Officer (MLRO)[8].
Senior management oversight		
	3.6	The senior management of an FI is responsible for implementing effective AML/CFT Systems that can adequately manage the ML/TF risks identified. In

[8] The role and functions of an MLRO are detailed in paragraphs 3.9, 7.9, 7.13- to 7.25. Depending on the size of an FI, the functions of the CO and the MLRO may be performed by the same staff member. The Manager-In-Charge of Core Function responsible for managing the Anti-Money Laundering and Counter-Terrorist Financing function of the FI (i.e. MIC of AML/CFT) can be the CO provided that the requirements set out in paragraphs 3.7 and 3.8 are met.

		particular, the senior management should: (a) appoint a CO at the senior management level to have the overall responsibility for the establishment and maintenance of the FI's AML/CFT Systems; and (b) appoint a senior staff member as the MLRO to act as the central reference point for suspicious transaction reporting.
	3.7	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 FI, independent of all operational and business functions; (c) normally based in Hong Kong; (d) of a sufficient level of seniority and authority within the FI; (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; (f) fully conversant with the FI's statutory and regulatory requirements and the ML/TF risks arising from the FI'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 RAs); 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		
	3.8	The principal function of the CO is to act as the focal point within an FI 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 FI's AML/CFT Systems, including (where applicable) any group-wide AML/CFT Systems in the case of a Hong Kong-incorporated FI, to ensure they remain up-to-date, meet current statutory and regulatory requirements, and are effective in managing ML/TF risks arising from the FI's business; (b) overseeing all aspects of the FI'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.
	3.9	An FI 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, determination of whether or not it is necessary to make a report to the JFIU; (b) maintenance of records related to such internal reviews; and

		(c) provision of guidance on how to avoid tipping-off.
Independent audit function		
	3.10	Where practicable, an FI should establish an independent audit function which should have a direct line of communication to the senior management of the FI. Subject to appropriate segregation of duties, the function should have sufficient expertise and resources to enable it to carry out an independent review of the FI's AML/CFT Systems.
	3.11	The audit function should regularly review the AML/CFT Systems to ensure effectiveness. This would include evaluating, among others: (a) the adequacy of the FI's AML/CFT Systems, ML/TF risk assessment framework and application of risk-based approach; (b) the effectiveness of the system for recognising and reporting suspicious transactions; (c) whether instances of non-compliance are reported to senior management on a timely basis; and (d) the level of awareness of staff having AML/CFT responsibilities. The frequency and extent of the review should be commensurate with the nature, size and complexity of the FI's businesses and the ML/TF risks arising from those businesses. Where appropriate, the FI should seek a review from external parties.
Employee screening		
	3.12	FIs should have adequate and appropriate screening procedures in order to ensure high standards when hiring employees.
Group-wide AML/CFT Systems		
s.22(1), Sch. 2	3.13	Subject to paragraphs 3.14 and 3.15, a Hong Kong-incorporated FI with overseas branches or subsidiary

		undertakings that carry on the same business as an FI as defined in the AMLO should implement group-wide AML/CFT Systems[9] to apply the requirements set out in this Guideline 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. In particular, a Hong Kong-incorporated FI 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 imposed under Parts 2 and 3 of Schedule 2, to the extent permitted by the laws and regulations of that place.
	3.14	If the AML/CFT requirements in the jurisdiction where the overseas branch or subsidiary undertaking of a Hong Kong-incorporated FI is located (host jurisdiction) differ from those relevant requirements referred to in paragraph 3.13, the FI should require that branch or subsidiary undertaking to apply the higher of the two sets of requirements, to the extent that the host jurisdiction's laws and regulations permit.
s.22(2), Sch. 2	3.15	If the host jurisdiction's laws and regulations do not permit the branch or subsidiary undertaking of a Hong Kong-incorporated FI to apply the higher AML/CFT requirements, particularly the CDD and record-keeping requirements imposed under Parts 2 and 3 of Schedule 2, the FI should: (a) inform the RA of such failure; and (b) take additional measures to effectively mitigate

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

		ML/TF risks faced by the branch or subsidiary undertaking as a result of its inability to comply with the requirements.
	3.16	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 FI should also implement measures, 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 FI'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[10].

[10] This should include information and analysis of transactions or activities which appear unusual (if such analysis was done); and could include a suspicious transaction report, its underlying information, or the fact that a suspicious transaction report has been submitted. Similarly, branches and subsidiaries 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 and when they must be carried out		
General		
s.19(3), Sch. 2	4.1.1	The AMLO defines what CDD measures are (see paragraph 4.1.4) and also prescribes the circumstances in which an FI must carry out CDD (see paragraph 4.1.9). This Chapter provides guidance in this regard. Wherever possible, this Guideline gives FIs a degree of discretion in how they comply with the AMLO and put in place procedures for this purpose. In addition, an FI 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	As stated in Chapter 2, FIs should determine the extent of CDD measures using an RBA, taking into account the higher or lower ML/TF risks identified in the customer risk assessment conducted by the FIs, so that preventive or mitigating measures are commensurate with the risks identified [11]. The measures must however comply with the legal requirements of the AMLO. FIs should also have regard to section 4 of Schedule 2 which permits FIs not to identify and take reasonable measures to verify the identities of the beneficial owners of specific types of customers, or in relation to specific types of products related to the transactions of the customers (see paragraphs 4.8); and sections 8 to 15 of Schedule 2 which require FIs to comply with some special requirements in relation to specific types of customers, products, transactions or other high risk situations (see paragraphs 4.9 to 4.14).

[11] Illustrative examples of possible simplified and enhanced measures are set out in paragraphs 1 and 2 of Appendix C respectively.

<u>What CDD measures are</u>		
	4.1.3	CDD information is a vital tool for recognising whether there are grounds for knowledge or suspicion of ML/TF.
s.2(1), Sch. 2	4.1.4	The following are CDD measures applicable to an FI: (a) identify the customer and verify the customer's identity using documents, data or information provided by a reliable and independent source (see paragraphs 4.2); (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 FI is satisfied that it knows who the beneficial owner is, including, in the case of a legal person or trust, measures to enable the FI to understand the ownership and control structure of the legal person or trust (see paragraphs 4.3); (c) obtain information on the purpose and intended nature of the business relationship (if any) established with the FI unless the purpose and intended nature are obvious (see paragraphs 4.6); and (d) if a person purports to act on behalf of the customer: (i) identify the person and take reasonable measures to verify the person's identity using 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 paragraphs 4.4).
	4.1.5	The term "customer" is defined in the AMLO to include a client. The meaning of "customer" and "client" should be inferred from its everyday meaning and in the context of the industry practice.

	4.1.6	Unless the context otherwise requires, for the securities sector, the term "customer" refers to a person who is a client of an LC and the term "client" is as defined in section 1 of Part 1 of Schedule 1 to the SFO ~~and the~~. For SFC-licensed VAS Providers, the term "customer" refers to a person to whom the SFC-licensed VAS Provider provides services in the course of providing a VA service as defined in section 53ZR of the AMLO. The phrase "potential customer" in the term "business relationship" is to be construed accordingly as meaning "potential client".
	4.1.7	In determining what constitutes reasonable measures to verify the identity of a beneficial owner and reasonable measures to understand the ownership and control structure of a legal person or trust, the FI should consider and give due regard to the ML/TF risks posed by a particular customer and a particular business relationship. Due consideration should also be given to the guidance in relation to customer risk assessment set out in Chapter 2.
	4.1.8	FIs should adopt a balanced and common sense approach with regard to customers connected with jurisdictions posing a higher risk (see paragraphs 4.13). While extra care may well be justified in such cases, unless an RA has, through a "notice in writing", imposed a general or specific requirement (see paragraph 4.14.2), it is not a requirement that FIs should refuse to do any business with such customers or automatically classify them as high risk and subject them to the special requirements set out in section 15 of Schedule 2. Rather, FIs should weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of ML/TF.

When CDD measures must be carried out		
s.3(1)~~,~~ & (1A), Sch. 2	4.1.9	An FI must carry out CDD measures in relation to a customer: (a) ~~at the outset of~~before establishing a business relationship with the customer; (b) before ~~performing any~~carrying out for the customer an occasional transaction[12]: (i) involving an amount equal to or ~~exceeding an aggregate value of~~above $120,000~~, whether carried out in a single operation or several operations that appear to the FI to be linked~~ or an equivalent amount in any other currency[13]; or (ii) that is a wire transfer involving an amount equal to or ~~exceeding an aggregate value of~~above $8,000 or an equivalent amount in any other currency;~~,~~ whether the transaction is carried out in a single operation or in several operations that appear to the FI to be linked[14]; (c) when the FI suspects that the customer or the customer's account is involved in ML/TF[15]; or (d) when the FI 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.
s.1, Sch. 2	4.1.10	"Business relationship" between a person and an FI is defined in the AMLO as a business, professional or commercial relationship: (a) that has an element of duration; or (b) that the FI, at the time the person first contacts it in the person's capacity as a potential customer

[12] Occasional transactions may include for example, wire transfers, currency exchanges, purchase of cashier orders or gift cheques.

[13] ~~For the avoidance of doubt, paragraph 4.1.9(b)(i) applies to FIs that are not SFC-licensed VAS Providers. FIs that are SFC-licensed VAS Providers should also refer to the guidance provided in paragraphs 12.3.1 and 12.3.2.~~

[14] FIs should also refer to the guidance provided in paragraphs 12.3 for occasional transactions in the context of virtual assets.

[15] This criterion applies irrespective of the $120,000 or $8,000 threshold applicable to occasional transactions set out in paragraphs 4.1.9(b)(i) and 4.1.9(b)(ii) respectively.

		of the FI, expects to have an element of duration.
s.1, Sch. 2	4.1.11	The term "occasional transaction" is defined in the AMLO as a transaction between an FI and a customer who does not have a business relationship with the FI[16].
	4.1.12	FIs should be vigilant to the possibility that a series of linked occasional transactions could meet or exceed the CDD thresholds of $8,000 for wire transfers and $120,000 for other types of transactions. Where FIs become aware that these thresholds are met or exceeded, CDD measures must be carried out.
	4.1.13	The factors linking occasional transactions are inherent in the characteristics of the transactions – for example, where several payments are made to the same recipient from one or more sources over a short period, where a customer regularly transfers funds to one or more destinations. In determining whether the transactions are in fact linked, FIs should consider these factors against the timeframe within which the transactions are conducted.
4.2 Identification and verification of the customer's identity		
s.2(1)(a), Sch. 2	4.2.1	The FI must 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 RA or any other RA; (c) an authority in a place outside Hong Kong that performs functions similar to those of the RA or any other RA; ~~(c)~~(d) a digital identification system that is a

[16] It should be noted that FIs that are LCs or SFC-licensed VAS Providers should not carry out "occasional transactions" ~~do not apply to the securities sector~~.

		reliable and independent source that is recognised by the RA[17]; or ~~(d)~~(e) any other reliable and independent source that is recognised by the RA.
Customer that is a natural person[18]		
s.2(1)(a), Sch. 2	4.2.2	For a customer that is a natural person, FIs should identify the customer by obtaining at least the following identification information: (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.
s.2(1)(a), Sch. 2	4.2.3	In verifying the identity of a customer that is a natural person, an FI should verify the name, date of birth, unique identification number and document type of the customer. The FI should do so by reference to documents, data or information provided by a reliable and independent source, examples of such documents, data or information include: (a) Hong Kong identity card or other national identity card bearing the individual's photograph; (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). The FI should retain a copy of the individual's

[17] The SFC recognises iAM Smart, developed and operated by the Hong Kong Government, as a digital identification system that can be used for identity verification of natural persons. The SFC may in future recognise other similar digital identification systems developed and operated by governments in other jurisdictions having regard to market developments and specific circumstances.

[18] For the purposes of this Guideline, the terms "natural person" and "individual" are used interchangeably.

		identification document or record.
	4.2.4	An FI should obtain the residential address information of a customer that is a natural person[19].
<u>Customer that is a legal person</u>[20]		
s.2(1)(a), Sch. 2	4.2.5	For a customer that is a legal person, an FI 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 registered office).
s.2(1)(a), Sch. 2	4.2.6	In verifying the identity of a customer that is a legal person, an FI should normally verify its name, legal form, current existence (at the time of verification), and powers that regulate and bind the legal person. The FI should do so by reference to documents, data or information provided by a reliable and independent source, examples of such documents, data or information include[21]:

[19] For the avoidance of doubt, an FI may, under certain circumstances, further require proof of residential address from a customer for other purposes (e.g. group requirements, paragraph 5.4 of the current Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (a.k.a. Client Identity Rule), and other local or overseas legal and regulatory requirements). In such circumstances, the FI should communicate clearly to the customers the reasons why it requires proof of residential address.

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

[21] In some instances, an FI 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.

		(a) certificate of incorporation; (b) record of companies registry; (c) certificate of incumbency; (d) certificate of good standing; (e) record of registration; (f) partnership agreement or deed; (g) constitutive document; or (h) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body). Illustrative examples of possible measures to verify the name, legal form and current existence of a legal person are set out in paragraph 3 of Appendix C.
	4.2.7	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 provide reliable and independent evidence of the identity of the customer as required in paragraph 4.2.6 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.
	4.2.8	In the case of associations, clubs, societies, charities, religious bodies, institutes, mutual and friendly societies, co-operative and provident societies, an FI should satisfy itself as to the legitimate purpose of the organisation, e.g. by requesting sight of the constitutive document.

Customer that is a trust[22] or other similar legal arrangement[23]		
s.2(1)(a), Sch. 2	4.2.9	In respect of trusts, an FI should identify and verify the trust as a customer in accordance with the requirements set out in paragraphs 4.2.10 and 4.2.11. The FI should also regard the trustee[24] as its customer if the trustee enters into a business relationship or carries out occasional transactions on behalf of the trust, which is generally the case if the trust does not possess a separate legal personality. In such a case, an FI should identify and verify the identity of the trustee in line with the identification and verification requirements for a customer that is a natural person or, where applicable, a legal person.
s.2(1)(a), Sch. 2	4.2.10	For a customer that is a trust or other similar legal arrangement, FIs should identify the customer by obtaining at least the following identification information: (a) the 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).

[22] For the purposes 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.

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

[24] For the avoidance of doubt, the AMLO defines a beneficial owner in relation to a trust to include trustee (see paragraph 4.3.10). Depending on the nature of the roles and activities which the trustee is authorised to conduct (e.g. if a trustee is also regarded as the customer or the person purporting to act on behalf of the customer), an FI should apply the higher of the relevant requirements set out in this Guideline for the purposes of identification and verification of the identity of the trustee.

s.2(1)(a), Sch. 2	4.2.11	In verifying the identity of a customer that is a trust or other similar legal arrangement, an FI 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. The FI should do so by reference to documents, data or information provided by a reliable and independent source, examples of such documents, data or information include: (a) trust deed or similar instrument[25]; (b) record of an appropriate register [26] in the relevant country of establishment; (c) written confirmation from a trustee acting in a professional capacity[27]; (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 FI, if the trust concerned is managed by that trust company.
<u>Connected parties</u>		
	4.2.12	Where a customer is a legal person, a trust or other similar legal arrangement, an FI should identify the connected parties[28] of the customer by obtaining their names.
	4.2.13	A connected party of a customer that is a legal person, a trust or other similar legal arrangement:

[25] Under exceptional circumstance, the FI may choose to retain a redacted copy.

[26] In determining whether a register is appropriate, the FI 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.

[27] "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).

[28] 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 FI has to identify and verify the identity of that person with reference to relevant requirements set out in this Guideline.

		(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.
Other considerations		
	4.2.14	An FI may adopt an RBA in determining the documents, data or information to be obtained for verifying the identity of a customer that is a legal person, trust or other similar legal arrangement. Illustrative examples of relevant simplified and enhanced measures are set out in paragraph 4 of Appendix C.
4.3 Identification and verification of a beneficial owner		
s.1 & s.2(1)(b), Sch. 2	4.3.1	~~A b~~Beneficial owner ~~is normally~~refers to ~~a~~ the natural person(s) who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. An FI must identify any beneficial owner in relation to a customer, and take reasonable measures to verify the beneficial owner's identity so that the FI is satisfied that it knows who the beneficial owner is. ~~However, the verification requirements under the AMLO are different for a customer and a beneficial owner.~~
	4.3.2	While an FI 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 FI may obtain an undertaking or declaration[29] from the customer on the identity of,

[29] For example, an FI may obtain from a corporate customer its register of beneficial owners (i.e. the significant controllers register maintained in accordance with the Companies Ordinance, Cap. 622).

		and the information relating to, its beneficial owner. ~~Where a natural person is identified as~~When identifying a beneficial owner, the FI should endeavour to obtain the same identification information as at paragraph 4.2.2 as far as possible.
	4.3.3 ~~4.3.8~~	The verification requirements under the AMLO are different for a customer and a beneficial owner. An FI may adopt an RBA to determine the extent of reasonable measures in relation to the verification of the identity of a beneficial owner of a customer, having regard to paragraph 4.1.7. ~~While an FI usually can identify who the beneficial owner of a customer is in the course of understanding the ownership and control structure of the customer, t~~The FI may consider whether it is appropriate to, for example, (i) make use of records of a beneficial owner available in the public domain~~obtain an undertaking or declaration~~ [30] ; (ii) request its customers to provide documents or information in relation to the identity of a beneficial owner that is obtained from a reliable and independent source; ~~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 FI should take reasonable measures to verify the identity of the beneficial owner (e.g.~~ or (iii) where an undertaking or declaration is obtained from the customer (see paragraph 4.3.2), corroborat~~ing~~e the customer's undertaking or declaration with publicly available information~~).~~
	4.3.4 ~~4.3.9~~	If the ownership structure of a customer involves different types of legal persons or legal arrangements, in determining who the beneficial owner is, an FI should pay attention to who has ultimate ownership or control over the customer, or who constitutes the controlling mind and

[30] For example, some jurisdictions maintain registers of beneficial owners which can be accessed by the public or FIs.

		management of the customer.
Beneficial owner in relation to a natural person		
	4.3.5 ~~4.3.3~~	In respect of a customer that is a natural person, the customer is the beneficial owner, unless the characteristics of the transactions or other circumstances indicate otherwise. Therefore, there is no requirement on FIs to make proactive searches for beneficial owners of the customer in such a case, but they 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		
s.1, Sch. 2	4.3.6 ~~4.3.4~~	The AMLO defines beneficial owner in relation to a corporation as: (i) an individual who (a) 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; (b) 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 (c) exercises ultimate control over the management of the corporation; or (ii) if the corporation is acting on behalf of another person, means the other person.
s.1, Sch. 2	4.3.7 ~~4.3.5~~	The AMLO defines beneficial owner, in relation to a partnership as: (i) an individual who (a) is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership; (b) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights in the partnership; or (c) exercises ultimate control over the

		management of the partnership; or (ii) if the partnership is acting on behalf of another person, means the other person.
s.1, Sch. 2	4.3.8 ~~4.3.6~~	In relation to an unincorporated body other than a partnership, beneficial owner: (i) means an individual who ultimately owns or controls the unincorporated body; or (ii) if the unincorporated body is acting on behalf of another person, means the other person.
s.2(1)(b), Sch. 2	4.3.9 ~~4.3.7~~	For a customer that is a legal person, an FI 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 4.3.64 to 4.3.~~8~~6), the FI should identify the relevant natural persons who hold the position of senior managing official[31] in the legal person, and take reasonable measures to verify their identities.
	~~4.3.8~~	~~While an FI 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 FI may obtain an undertaking or declaration[32] from the customer on the identity of,~~

[31] Examples of positions of senior managing official include chief executive officer, chief financial officer, managing or executive director, president, or natural person(s) who has significant authority over a legal person's financial relationships (including with FIs that hold accounts on behalf of a legal person) and the ongoing financial affairs of the legal person.

~~[32] 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, Cap. 622). An FI 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, or when the FI considers that the information in a publicly available register is not up-to-date or does not adequately reflect the beneficial ownership (e.g. where the register reflects beneficial ownership only up to an intermediate layer of the ownership and control structure of the customer), the FI may obtain the record directly from its customers (e.g. obtaining the ownership chart), having regard to paragraphs 4.3.13 and 4.3.14 as appropriate.~~

		~~and the information relating to, its beneficial owner. Nevertheless, in addition to the undertaking or declaration obtained, the FI should take reasonable measures to verify the identity of the beneficial owner (e.g. corroborating the undertaking or declaration with publicly available information).~~
	~~4.3.9~~	~~If the ownership structure of a customer involves different types of legal persons or legal arrangements, in determining who the beneficial owner is, an FI 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		
s.1, Sch. 2	4.3.10	The AMLO defines the beneficial owner, in relation to a trust as: (i) ~~an individual who is~~a beneficiary or a class of beneficiaries of the trust 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; (ii) the settlor of the trust; ~~(ii)~~(iii) the trustee of the trust; ~~(iii)~~(iv) a protector or enforcer of the trust; or ~~(iv)~~(v) an individual who has ultimate control over the trust.
s.2(1)(b), Sch. 2	4.3.11	For a customer that is a trust~~s~~, an FI should identify the settlor, the trustee, 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[33] to verify their identities. For a customer that is an other similar legal arrangements, an FI should identify any natural person in equivalent or similar positions to 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 FI does not regard the trustee (or equivalent in the case of other similar legal arrangement) as its customer pursuant to paragraph 4.2.9 (e.g. when a trust appears as part of an intermediate layer referred to in paragraph 4.3.13), the FI should also identify the trustee (or equivalent) and take reasonable measures to verify the identity of the trustee (or equivalent) so that the FI is satisfied that it knows who that person is.~~
	4.3.12	For a beneficiary of a trust designated by characteristics or by class[34], an FI should obtain sufficient information[35] concerning the beneficiary to satisfy the FI 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		
s.2(1)(b), Sch. 2	4.3.13	Where a customer is not a natural person, an FI

[33] An FI may adopt an RBA to determine the extent of reasonable measures in relation to the verification of the identities of the beneficiaries or class of beneficiaries of a customer that is a trust, which should be commensurate with the ML/TF risks associated with the customer or business relationship (see paragraph 4.3.3). For example, where the business relationship with a customer that is a trust is assessed to present a low ML/TF risk, it may be reasonable for the FI to verify the identities of the beneficiaries with reference to the information provided by the trustee that was also regarded as the customer by the FI and whose identity has been verified. Such information includes the identification information of the beneficiaries, and declaration that they are known to the trustee.

[34] For example, a trust may have no defined existing beneficiaries when it is set up but only a class of beneficiaries and objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, or following exercise of trustee discretion in the case of a discretionary trust.

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

		should understand its ownership and control structure, including identification of any intermediate layers (e.g. by reviewing an ownership chart of the customer)[36]. The objective is to follow the chain of ownerships to the beneficial owners of the customer. 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 corporate being part of an intermediate layer.
	4.3.14	Where a customer has a complex ownership or control structure, an FI should obtain sufficient information for the FI to satisfy itself that there is a legitimate reason behind the particular structure employed.
4.4 Identification and verification of a person purporting to act on behalf of the customer		
	4.4.1	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 FI 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 ML/TF risks associated with that person's roles and the activities which the person is authorised to conduct[37], as well as the

[36] Examples of information which may be collected to identify the intermediate layers of the corporate structure of a legal person with multiple layers in its ownership structure are set out in paragraph 5 of Appendix C.

[37] For example, those who carry out transactions on behalf of the customer may be considered as PPTAs. However, dealers and traders in an investment bank or asset manager who are authorised to act on behalf of the investment bank or asset manager would not ordinarily be considered PPTAs. For the avoidance of doubt, the person who is authorised to act on behalf of a customer to establish a business relationship with an FI should always be considered as a PPTA.

		ML/TF risks associated with the business relationship[38]. FIs should implement clear policies for determining who is considered to be a PPTA.
s.2(1)(d), Sch. 2	4.4.2	If a person purports to act on behalf of the customer, FIs must: (i) identify the person and take reasonable measures to verify the person's identity by reference to documents, data or information provided by a reliable and independent source: (A) a governmental body; (B) the RA or any other RA; (C) an authority in a place outside Hong Kong that performs functions similar to those of the RA or any other RA; or (D) any other reliable and independent source that is recognised by the RA; and (ii) verify the person's authority to act on behalf of the customer.
	4.4.3	FI should identify a PPTA in line with the identification requirements for a customer that is a natural person or, where applicable, a legal person. In taking reasonable measures [39] to verify the identity of the PPTA, FI should, as far as possible, follow the verification requirements for a customer that is a natural person or, where applicable, a legal person.
s.2(1)(d)(ii), Sch. 2	4.4.4	FIs should verify the authority of each PPTA by

[38] A list of non-exhaustive illustrative risk indicators which may indicate higher or lower ML/TF risks as the case may be is provided in Appendix A.

[39] An FI may adopt an RBA to determine the extent of reasonable measures in relation to the verification of the identity of the PPTA, which should be commensurate with the ML/TF risks associated with the business relationship. For example, where a business relationship with a legal person customer with many PPTAs is assessed to present low ML/TF risk, an FI could verify the identities of the PPTAs with reference to a list of PPTAs, whose identities and authority to act have been confirmed by a department or person within that legal person customer which is independent to the persons whose identities are being verified (for example, compliance, audit or human resources).

		appropriate documentary evidence (e.g. board resolution or similar written authorisation).
4.5 Reliability of documents, data or information		
	4.5.1	In verifying the identity of a customer, an FI needs not establish accuracy of every piece of identification information collected in paragraphs 4.2.2, 4.2.5 and 4.2.10.
	4.5.2	An FI should ensure that documents, data or information obtained for the purpose of verifying the identity of a customer as required in paragraphs 4.2.3, 4.2.6 and 4.2.11 is current at the time they are provided to or obtained by the FI.
	4.5.3	When using documents for verification, an FI should be aware that some types of documents are more easily forged than others, or can be reported as lost or stolen[40]. Therefore, the FI should consider applying anti-fraud procedures that are commensurate with the risk profile of the person being verified.
	4.5.4	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 FI is physically present during the CDD process, the FI 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 FI should take appropriate measures to ensure the reliability of identification documents obtained.

[40] Please refer to paragraph 6 of Appendix C for illustrative examples of procedures to establish whether the identification documents offered by customers are genuine, or have been reported as lost or stolen.

	4.5.5	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 FI to be reasonably satisfied that the documents in fact provide evidence of the customer's identity[41].
4.6 Purpose and intended nature of business relationship		
s.2(1)(c), Sch. 2	4.6.1	An FI must understand the purpose and intended nature of the business relationship. In some instances, this will be self-evident, but in many cases, the FI may have to obtain information in this regard.
	4.6.2	Unless the purpose and intended nature of the business relationship are obvious, FIs should obtain satisfactory information from all new customers as to the intended purpose and reason for opening the account or establishing the business relationship, and record the information on the account opening documentation. The information obtained by the FIs should be commensurate with the risk profile of the customers and the nature of the business relationships. Information that might be relevant may include: (a) nature and details of the customer's business/occupation/employment; (b) the anticipated level and nature of the activity that is to be undertaken through the business relationship (e.g. what the typical transactions are likely to be); (c) location of customer; (d) the expected source and origin of the funds to be used in the business relationship; and (e) initial and ongoing source(s) of wealth or income.

[41] For example, ensuring that staff assessing such documents are proficient in the language or obtaining a translation from a suitably qualified person.

4.7 Delayed identity verification during the establishment of a business relationship		
s.3(2) & (3), Sch. 2	4.7.1	An FI should verify the identity of a customer and any beneficial owner of the customer before or during the course of establishing a business relationship or conducting transactions for occasional customers. However, FIs may, exceptionally, verify the identity of a customer and any beneficial owner of the customer after establishing the business relationship[42], provided that: (a) any risk of ML/TF arising from the delayed verification of the customer's or beneficial owner's identity can be effectively managed[43]; (b) it is necessary not to interrupt the normal conduct of business with the customer; and (c) verification is completed as soon as reasonably practicable.
	4.7.2	An example of a situation in the securities industry where it may be necessary not to interrupt the normal conduct of business is when companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.
	4.7.3	If an FI allows verification of the identity of a customer and any beneficial owner of the customer after establishing the business relationship, it should adopt appropriate risk management policies and procedures concerning the conditions under which the customer may utilise the business relationship prior to verification. These policies and procedures

[42] ~~Paragraphs 4.7 do not apply to FIs that are SFC-licensed VAS Providers.~~

[43] For FIs that are SFC-licensed VAS Providers, it would be highly unlikely that the ML/TF risks arising from the delayed verification of the customer's or beneficial owner's identity can be effectively managed.

		should include: (a) establishing a reasonable timeframe for the completion of the identity verification measures and the follow-up actions if exceeding the timeframe (e.g. to suspend or terminate the business relationship); (b) placing appropriate limits on the number, types, and/or amount of transactions that can be performed; (c) monitoring of large and complex transactions being carried out outside the expected norms for that type of relationship; (d) keeping senior management periodically informed of any pending completion cases; and (e) ensuring that funds are not paid out to any third party. Exceptions may be made to allow payments to third parties subject to the following conditions: (i) there is no suspicion of ML/TF; (ii) the risk of ML/TF is assessed to be low; (iii) the transaction is approved by senior management, who should take account of the nature of the business of the customer before approving the transaction; and (iv) the names of recipients do not match with watch lists such as those for terrorist suspects and PEPs.
	4.7.4	Verification of identity should be completed by an FI within a reasonable timeframe, which generally refers to the following: (a) the FI completing such verification no later than 30 working days after the establishment of business relationship; (b) the FI suspending business relationship with the customer and refraining from carrying out further transactions (except to return funds to their sources, to the extent that this is possible) if such verification remains uncompleted 30 working days after the establishment of

		business relationship; and (c) the FI terminating business relationship with the customer if such verification remains uncompleted 120 working days after the establishment of business relationship.
s.3(4)(b), Sch. 2, s.25A, DTROP & OSCO, s.12, UNATMO	4.7.5	If verification cannot be completed within the reasonable timeframe set in the FI's risk management policies and procedures, the FI should terminate the business relationship as soon as reasonably practicable and refrain from carrying out further transactions (except to return funds or other assets in their original forms as far as possible). The FI should also assess whether this failure provides grounds for knowledge or suspicion of ML/TF and consider making a suspicious transaction report (STR) to the JFIU, particularly if the customer requests that funds or other assets be transferred to a third party or be "transformed" (e.g. from cash into a cashier order) without a justifiable reason.
4.8 Simplified customer due diligence (SDD)		
General		
s.4, Sch. 2	4.8.1	Section 4 of Schedule 2 permits FIs not to identify and take reasonable measures to verify the identities of the beneficial owners[44] of specific types of customers, or in relation to specific types of products related to the transactions of the customers (referred to as "simplified customer due diligence" under section 4 of Schedule 2; and as "SDD" hereafter). However, other aspects of CDD must be undertaken and it is still necessary to conduct ongoing monitoring of the business relationship. The use of SDD must be supported by robust assessment to ensure the conditions or circumstances of specific types of customers or products specified in section 4 of Schedule 2 are

[44] It includes the individuals who ultimately own or control the customer and the person(s) on whose behalf the customer is acting (e.g. underlying customer(s) of a customer that is an FI).

		met.
s.3(1)(d) & (e), s.4(1), (3), (5) & (6), Sch. 2	4.8.2	Nonetheless, SDD must not be or continue to be applied when the FI suspects that the customer, the customer's account or the transaction is involved in ML/TF, or when the FI doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or verifying the customer's identity, notwithstanding when the customer, the product, and account type falls within paragraphs 4.8.3, 4.8.15 and 4.8.17 below.
s.4(3), Sch. 2	4.8.3	An FI may apply SDD 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 paragraphs 4.19); (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 similar to those imposed under Schedule 2; and (iv) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the RAs; (c) a corporation listed on any stock exchange ("listed company"); (d) an investment vehicle where the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle is- (i) an FI as defined in the AMLO; (ii) an institution incorporated or established in Hong Kong, or in an equivalent jurisdiction that- i. has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and ii. is supervised for compliance with those

		requirements; (e) the Government or any public body in Hong Kong; or (f) the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.
s.4(2), Sch. 2	4.8.4	If a customer not falling within section 4(3) of Schedule 2 has in its ownership chain an entity that falls within that section, the FI is not required to identify or verify the beneficial owners of that entity in that chain when establishing a business relationship with or carrying out an occasional transaction for the customer. However, FIs should still identify and take reasonable measures to verify the identities of beneficial owners in the ownership chain that are not connected with that entity.
s.2(1)(a), (c) & (d), Sch. 2	4.8.5	For avoidance of doubt, the FI must still: (a) identify the customer and verify[45] the customer's identity; (b) if a business relationship is to be established and its purpose and intended nature are not obvious, obtain information on the purpose and intended nature of the business relationship with the FI; and (c) if a person purports to act on behalf of the customer, (i) identify the person and take reasonable measures to verify the person's identity; and (ii) verify the person's authority to act on behalf of the customer, in accordance with the relevant requirements stipulated in this Guideline.
<u>Local and foreign financial institution</u>		
s.4(3)(a) & (b), Sch. 2	4.8.6	FIs may apply SDD to a customer that is an FI as defined in the AMLO, or an institution that carries on

[45] For FIs and listed companies, please refer to paragraphs 4.8.7 and 4.8.8 respectively.

		a business similar to that carried on by an FI and meets the criteria set out in section 4(3)(b) of Schedule 2. If the customer does not meet the criteria, the FI must carry out all the CDD measures set out in section 2 of Schedule 2. FI may apply SDD to a customer that is an FI as defined in the AMLO that opens an account: (a) in the name of a nominee company for holding fund units on behalf of the second-mentioned FI or its underlying customers; or (b) in the name of an investment vehicle in the capacity of a service provider (such as manager or custodian) to the investment vehicle and the underlying investors have no control over the management of the investment vehicle's assets; provided that the second-mentioned FI: (i) has conducted CDD: (A) in the case where the nominee company holds fund units on behalf of the second-mentioned FI or the second-mentioned FI's underlying customers, on its underlying customers; or (B) in the case where the second-mentioned FI acts in the capacity of a service provider (such as manager or custodian) to the investment vehicle, on the investment vehicle pursuant to the provisions of the AMLO; and (ii) is authorised to operate the account as evidenced by contractual document or agreement.
	4.8.7	For ascertaining whether the institution meets the criteria set out in section 4(3)(a) & (b) of Schedule 2, it will generally be sufficient for an FI to verify that the institution is on the list of licensed (and supervised) FIs in the jurisdiction concerned.

Listed company		
s.4(3)(c), Sch. 2	4.8.8	An FI may apply SDD to a customer that is a company listed on a stock exchange. For this purpose, the FI should assess whether there are any disclosure requirements (either by stock exchange rules, or through law or enforceable means) which ensure the adequate transparency of the beneficial ownership of companies listed on that stock exchange. In such a case, it will be generally sufficient for an FI to obtain proof of the customer's listed status on that stock exchange.
Investment vehicle		
s.4(3)(d), Sch. 2	4.8.9	FIs may apply SDD to a customer that is an investment vehicle if the FI is able to ascertain that the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle falls within any of the categories of institutions set out in section 4(3)(d) of Schedule 2.
	4.8.10	An investment vehicle may be in the form of a legal person or trust, and may be a collective investment scheme or other investment entity.
	4.8.11	An investment vehicle whether or not responsible for carrying out CDD measures on the underlying investors under governing law of the jurisdiction in which the investment vehicle is established may, where permitted by law, appoint another institution ("appointed institution"), such as a manager, a trustee, an administrator, a transfer agent, a registrar or a custodian, to perform the CDD. Where the person responsible for carrying out the CDD measures (the investment vehicle[46] or the appointed institution) falls within any of the categories of

[46] If the governing law or enforceable regulatory requirements require the investment vehicle to implement CDD measures, the investment vehicle could be regarded as the responsible party for carrying out the CDD measures for the purposes of section 4(3)(d) of Schedule 2 where the investment vehicle meets the requirements, as permitted by law, by delegating or outsourcing to an appointed institution.

		institution set out in section 4(3)(d) of Schedule 2, an FI may apply SDD to that investment vehicle provided that it is satisfied that the investment vehicle has ensured that there are reliable systems and controls in place to conduct the CDD (including identification and verification of the identity) on the underlying investors in accordance with the requirements similar to those set out in the Schedule 2.
	4.8.12	If neither the investment vehicle nor appointed institution fall within any of the categories of institution set out in section 4(3)(d) of Schedule 2, the FI must identify and take reasonable measures to verify the identity of any investor ~~owning or controlling more than 25% interest~~ of the investment vehicle in accordance with the requirements for identification and verification of a beneficial owner of a specific type of customer (see paragraphs 4.3). The FI may consider whether it is appropriate to rely on a written representation from the investment vehicle or appointed institution (as the case may be) responsible for carrying out the CDD stating, to its actual knowledge, the identities of such investors or (where applicable) there is no such investor in the investment vehicle. This will depend on risk factors such as whether the investment vehicle is being operated for a small, specific group of persons. Where the FI accepts such a representation, this should be documented, retained, and subject to periodic review. ~~For the avoidance of doubt, the FI is still required to take reasonable measures to verify those investors owning or controlling more than 25% interest of the investment vehicle and (where applicable) other beneficial owners in accordance with paragraphs 4.3.~~
Government and public body		
s.4(3)(e) & (f), Sch. 2	4.8.13	FIs may apply SDD to a customer that is the Hong Kong ~~g~~Government, any public bodies in Hong Kong, the government of an equivalent jurisdiction

		or a body in an equivalent jurisdiction that performs functions similar to those of a public body.
s.1, Sch. 2	4.8.14	Public body includes: (a) any executive, legislative, municipal or urban council; (b) any Government department or undertaking; (c) any local or public authority or undertaking; (d) any board, commission, committee or other body, whether paid or unpaid, appointed by the Chief Executive or the Government; and (e) any board, commission, committee or other body that has power to act in a public capacity under or for the purposes of any enactment.
<u>SDD in relation to specific products</u>		
s.4(4) & (5), Sch. 2	4.8.15	FIs may apply SDD in relation to a customer if the FI has reasonable grounds to believe that the transaction conducted by the customer relates to any one of the following products: (a) a provident, pension, retirement or superannuation scheme (however described) that provides retirement benefits to employees, where contributions to the scheme are made by way of deduction from income from employment and the scheme rules do not permit the assignment of a member's interest under the scheme; (b) an insurance policy for the purposes of a provident, pension, retirement or superannuation scheme (however described) that does not contain a surrender clause and cannot be used as a collateral; or (c) a life insurance policy in respect of which: (i) an annual premium of no more than $8,000 or an equivalent amount in any other currency is payable; or (ii) a single premium of no more than $20,000 or an equivalent amount in any other currency is payable.

	4.8.16	For the purposes of item (a) of paragraph 4.8.15, FIs may generally treat the employer as the customer and apply SDD on the employer (i.e. choosing not to identify and take reasonable measures to verify the employees of the scheme). Where FIs have separate business relationships with the employees, it should apply CDD measures in accordance with relevant requirements set out in this Chapter.
<u>Solicitor's client accounts</u>		
s.4(6), Sch. 2	4.8.17	If a customer of an FI is a solicitor or a firm of solicitors, the FI may apply SDD to the client account opened by the customer, provided that the following criteria are satisfied: (a) the client account is kept in the name of the customer; (b) moneys or securities of the customer's clients in the client account are mingled; and (c) the client account is managed by the customer as those clients' agent.
	4.8.18	When opening a client account for a solicitor or a firm of solicitors, FIs should establish the proposed use of the account, i.e. whether to hold co-mingled client funds or the funds of a specific client.
	4.8.19	If a client account is opened on behalf of a single client or there are sub-accounts for each individual client where funds are not co-mingled at the FI, the FI should establish the identity of the underlying client(s) in addition to that of the solicitor opening the account.

4.9 Special requirements in high risk situations[47]		
s.15, Sch.2	4.9.1	An FI must comply with the special requirements set out in section 15 of Schedule 2 in: (a) a situation that by its nature may present a high risk of ML/TF taking into account the list of non-exhaustive illustrative risk indicators which may indicate higher ML/TF risks set out in Appendix A; or (b) a situation specified by the RA in a notice in writing given to the FI.
s.15, Sch. 2	4.9.2	Section 15 of Schedule 2 specifies that an FI must, in any situation that by its nature presents a high risk of ML/TF, comply with the special requirements set out therein which include: (a) obtaining the approval of senior management to ~~commence or continue the~~establish a business relationship, or continue an existing business relationship where the relationship subsequently presents a high risk of ML/TF; and (b) either: (i) taking reasonable measures to establish the relevant customer's or beneficial owner's source of wealth and the source of the funds that will be involved in the business relationship[48]; or (ii) taking additional measures to mitigate the risk of ML/TF.
	4.9.3	For illustration purposes, additional measures to mitigate the risk of ML/TF may include the examples of possible enhanced measures set out in

[47] Guidance on the special requirements in a situation specified by the RA in a notice in writing given to the FI in relation to jurisdictions subject to a call by the FATF is provided in paragraphs 4.14. Guidance on the special requirements when a customer is not physically present for identification purposes as set out in section 9 of Schedule 2, and the special requirements when a customer is a PEP as set out in section 10 of Schedule 2, are provided in paragraphs 4.10 and 4.11 respectively.

[48] Guidance on source of wealth and source of funds are provided in paragraphs 4.11.13 and 4.11.14.

		paragraph 2 of Appendix C.
4.10 Customer not physically present for identification purposes		
	4.10.1	FIs must apply equally effective customer identification procedures and ongoing monitoring standards for customers not physically present for identification purposes as for those where the customer is available for interview[49]. Where a customer has not been physically present for identification purposes, FIs will generally not be able to determine that the documentary evidence of identity actually relates to the customer they are dealing with. Consequently, there are increased risks.
Special requirements		
s.5(3)(a), s.5(4) & s.9(1), Sch. 2	4.10.2	The AMLO permits FIs to establish business relationship through various channels, both face-to-face (e.g. branch) and non-face-to-face (e.g. internet). However, an FI should take additional measures to mitigate any risk (e.g. impersonation risk) associated with customers not physically present for identification purposes. Except for the situation specified in paragraph 4.10.3, ~~I~~if a customer has not been physically present for identification purposes, the FI must carry out at least one of the following additional measures to mitigate the risks posed: (a) further verifying the customer's identity on the basis of documents, data or information referred to in section 2(1)(a) of Schedule 2 but not previously used for the purposes of verification of the customer's identity under that section; (b) taking supplementary measures to verify information relating to the customer that has been obtained by the FI; or

[49] For avoidance of doubt, this is not restricted to being physically present in Hong Kong; the face-to-face meeting could take place outside Hong Kong.

		(c) ensuring that the payment or, if there is more than one payment, the first payment made in relation to the customer's account is ~~received from~~carried out through an account opened in the customer's name with an authorized institution, or an institution that: (i) is incorporated or established ~~a bank operating~~ in an equivalent jurisdiction; ~~that~~ (ii) carries on a business similar to that carried on by an authorized institution; (iii) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and (iv) is supervised for compliance with those requirements by ~~a banking regulator~~authorities in that jurisdiction that perform functions similar to those of the HKMA.
s.9(2), Sch. 2	4.10.3	If an FI has verified the identity of the customer on the basis of data or information provided by a digital identification system that is a reliable and independent source that is recognised by the RA (see paragraph 4.2.1(d)), the FI is not required to carry out any of the additional measures set out in paragraph 4.10.2.
	4.10.4 ~~4.10.3~~	The extent of additional measures set out in paragraph 4.10.2 will depend on the nature and characteristics of the product or service requested and the assessed ML/TF risk presented by the customer.
	4.10.5 ~~4.10.4~~	Paragraph 4.10.2(b) allows an FI 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[50]; (ii) checking relevant data against reliable databases or registries; or (iii) using

[50] Further guidance on the use of an independent and appropriate person to certify identification documents is set out in paragraph 7 of Appendix C.

		appropriate technology, etc. Whether a particular measure or a combination of measures is acceptable should be assessed on a case-by-case basis. The FI should ensure and be able to demonstrate to the RA that the supplementary measure(s) taken can adequately guard against impersonation risk.
	4.10.6 ~~4.10.5~~	~~In taking additional measures to mitigate the risks posed by customers not physically present for identification purposes~~For the avoidance of doubt, LCs should also comply with the relevant provisions (presently paragraph 5.1) in the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission, having regard to the acceptable non-face-to-face account opening approaches as well as relevant circulars and frequently asked questions published by the SFC from time to time.
Other considerations		
	4.10.7 ~~4.10.6~~	While the requirements to undertake additional measures generally apply to a customer that is a natural person, ~~an FI should also mitigate any~~ increased risk ~~(e.g. applying additional due diligence measures set out in paragraph 4.10.2)~~ may arise if a customer that is not a natural person establishes a business relationship with an FI through a non-face-to-face channel~~.~~, for example when ~~The increased 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 such a case, the FI should mitigate the increased risk (e.g. applying additional due diligence measures set out in paragraph 4.10.2 to such natural person, except where the FI has verified the identity of the natural person on the basis of data or information provided by a digital identification system (see paragraph 4.2.1(d))). In addition, where an FI is provided with copies of documents for identifying and verifying a legal person customer's identity, an FI should also mitigate any increased risk (e.g. applying additional

		due diligence measures set out in paragraph 4.10.2).
4.11 Politically exposed persons (PEPs)		
General		
s.1 & s.10, Sch. 2	4.11.1	Much international attention has been paid in recent years to the risk associated with providing financial and business services to those with a prominent political profile or holding senior public office. However, PEP status itself does not automatically mean that the individuals are corrupt or that they have been incriminated in any corruption.
	4.11.2	However, their office and position may render PEPs vulnerable to corruption. The risks increase when the person concerned is from a foreign country with widely-known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have adequate AML/CFT standards.
	4.11.3	An FI should implement appropriate risk management systems to identify PEPs. Under-classification of PEPs poses a higher ML/TF risk to the FI whilst over-classification of PEPs leads to an unnecessary compliance burden to the FI and its customers.
s.15, Sch. 2	4.11.4	While the statutory definition of PEPs in the AMLO (see paragraph 4.11.7 below) only includes individuals entrusted with prominent public function in a place outside ~~the People's Republic of China~~[51] Hong Kong, ~~domestic~~ Hong Kong PEPs and international organisation PEPs may also present, by virtue of the positions they hold, a higher ML/TF risk. FIs should therefore adopt an RBA to determine whether to apply the measures in paragraph 4.11.12 below in respect of ~~domestic~~

~~[51] Reference should be made to the definition of the People's Republic of China in the Interpretation and General Clauses Ordinance (Cap. 1).~~

		Hong Kong PEPs and international organisation PEPs.
s.1, ~~s.15 &~~ s.5(3)(b) & (c), s.10 & s.15, Sch. 2	4.11.5	The statutory definition does not automatically exclude sub-national political figures. Corruption by heads of regional governments, regional government ministers and large city mayors is no less serious as sub-national figures in some jurisdictions may have access to substantial funds. Where FIs identify a customer as a sub-national figure holding a prominent public function, they should apply appropriate measures set out in paragraph 4.11.12. ~~This also applies to domestic sub-national figures assessed by the FI to pose a higher risk.~~
	4.11.6	The definitions of PEPs set out in paragraphs 4.11.7, 4.11.20~~18~~ and 4.11.21~~19~~ 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 respectively. An FI 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, an FI 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.
~~(Foreign)~~Non-Hong Kong PEPs		
Definition		
s.1, Sch. 2	4.11.7	A ~~(foreign)~~ PEP (hereafter referred to as "non-Hong Kong PEP") is defined ~~in the AMLO~~ as: (a) an individual who is or has been entrusted with a prominent public function in a place outside ~~the People's Republic of China~~Hong Kong 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 4.11.8).
s.1, Sch. 2	4.11.8	~~The AMLO defines a~~A close associate is defined as: (a) an individual who has close business relations with a person falling under paragraph 4.11.7(a) above, including an individual who is a beneficial owner of a legal person or trust of which the person falling under paragraph 4.11.7(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 4.11.7(a) above.
Identification of ~~foreign~~ non-Hong Kong PEPs		
s.19(1), Sch. 2	4.11.9	An FI must 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~~ non-Hong Kong PEP.
	4.11.10	While an FI may refer to commercially available databases to identify ~~foreign~~ non-Hong Kong 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 FI

		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 ~~foreign~~ non-Hong Kong PEPs used by the database providers may or may not align with the definition of ~~foreign~~ non-Hong Kong PEPs applied by the FI; and any technical incapability of such databases that may hinder the FI's effectiveness of ~~foreign~~ non-Hong Kong PEP identification. An FI using such databases as a support tool should ensure that they are fit for the purpose.
	4.11.11	FIs may use publicly available information or refer to relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations to assess which countries are most vulnerable to corruption (an example of which is Transparency International's "Corruption Perceptions Index", which ranks countries according to their perceived level of corruption). FIs should be vigilant where either the country to which the customer has business connections or the business/industrial sector is more vulnerable to corruption.
Special requirements and additional measures for ~~foreign~~ non-Hong Kong PEPs		
s.5(3)(b) & s.10(1) & (2), Sch. 2	4.11.12	When an FI knows that a customer or beneficial owner of a customer is a ~~foreign~~ non-Hong Kong 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~~ non-Hong Kong PEP, apply all the following measures: (a) obtaining approval from its senior management

		for establishing or continuing such business relationship[52]; (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 on that business relationship (see Chapter 5).
	4.11.13	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 FI may not have specific information about assets not deposited with or processed by it, it may be possible to gather general information from the individual, commercial databases or other open sources. Examples of information and documents which may be used to establish source of wealth include evidence of title, copies of trust deeds, audited financial statements, salary details, tax returns and bank statements.
	4.11.14	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 FI (e.g. the amounts being invested, deposited, or wired as part of the business relationship). Source of funds information should not simply be limited to knowing from where 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; e.g. salary payments and investment sale proceeds.
	4.11.15	It is for an FI to decide which measures it deems reasonable, in accordance with its assessment of the risks, to establish the source of funds and

[52] As a general rule, the approval seniority should be proportionate to the risks associated with the PEP and the related business relationship.

		source of wealth. In practical terms, this will often amount to obtaining information from the ~~foreign~~ non-Hong Kong 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. FIs should however note that not all declarations are publicly available and that a ~~foreign~~ non-Hong Kong PEP customer may have legitimate reasons for not providing a copy. FIs 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.
	4.11.16	Although the measures set out in paragraph 4.11.12 also apply to family members and close associates of the ~~foreign~~ non-Hong Kong PEP, the risks associated with them may vary depending to some extent on the social-economic and cultural structure of the jurisdiction of the ~~foreign~~ non-Hong Kong PEP.
	4.11.17	Since not all ~~foreign~~ non-Hong Kong PEPs pose the same level of ML/TF risks, an FI should adopt an RBA in determining the extent of measures in paragraph~~s~~ 4.11.12 taking into account relevant factors, such as: (a) the prominent public functions that a ~~foreign~~ non-Hong Kong PEP holds; (b) the geographical risk associated with the jurisdiction where a ~~foreign~~ non-Hong Kong 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~~and (d) ~~the level of influence that a foreign PEP may continue to exercise after stepping down from the prominent public function~~in relation to a former non-Hong Kong PEP, the risk factors

		specified in paragraph 4.11.19.
Treatment of former non-Hong Kong PEPs		
s.1, Sch. 2	4.11.18	A former non-Hong Kong PEP is defined as: (a) an individual who, being a non-Hong Kong PEP, has been but is not currently entrusted with a prominent public function in a place outside Hong Kong; (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 4.11.8).
s.5(5) & s.10(3), Sch. 2	4.11.19	An FI should adopt an RBA[53] and may decide not to apply, or not to continue to apply, the measures set out in paragraph 4.11.12 to a former non-Hong Kong PEP who no longer presents a high risk of ML/TF after stepping down. To determine whether a former non-Hong Kong PEP no longer presents a high risk of ML/TF, the FI should conduct an appropriate assessment of the ML/TF risk associated with the previous PEP status taking into account various risk factors, including but not limited to: (a) the level of (informal) influence that the individual could still exercise; (b) the seniority of the position that the individual held as a non-Hong Kong PEP; and (c) whether the individual's previous and current functions are linked in any way (e.g. formally by appointment of the former non-Hong Kong PEP's successor, or informally by the fact that the former non-Hong Kong PEP continues to

[53] The handling of a former non-Hong Kong PEP should be based on an assessment of risk and not merely on prescribed time limits.

		deal with the same substantive matters).
~~Domestic~~ Hong Kong PEPs and international organisation PEPs		
Definition		
	4.11.20 ~~4.11.18~~	For the purposes of this Guideline, a "~~domestic~~ Hong Kong PEP" refers to: (a) an individual who is or has been entrusted with a prominent public function in ~~a place within the People's Republic of China~~Hong Kong and (i) includes ~~a head of state,~~ head of government, senior politician, senior government~~,~~ or judicial ~~or military~~ official, senior executive of a ~~state~~government-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 4.11.8).
	4.11.21 ~~4.11.19~~	For the purposes of this Guideline, an "international organisation PEP" refers to: (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 4.11.8).
	4.11.22 ~~4.11.20~~	International organisations referred to in paragraph 4.11.21~~19~~ 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 UN 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 and the Association of Southeast Asian Nations; etc.
Identification of and additional measures for ~~domestic~~ Hong Kong PEPs and international organisation PEPs		
	4.11.23 ~~4.11.21~~	An FI should take reasonable measures to determine whether a customer or a beneficial owner of a customer is a ~~domestic~~ Hong Kong PEP or an international organisation PEP[54].
	4.11.24 ~~4.11.22~~	FIs should apply the measures specified in paragraph 4.11.12 with reference to the guidance provided in paragraphs 4.11.13 to 4.11.17 in any of the following situations[55]:

[54] Reference should be made to paragraphs 4.11.9 and 4.11.10.

[55] For the avoidance of doubt, an FI should consider whether the application of special requirements in paragraph 4.11.12 could mitigate the ML/TF risk arising from the high risk business relationship with a ~~domestic~~ Hong Kong PEP or an international organisation PEP. Where applicable, an FI should also take additional measures to mitigate such risk in accordance with the guidance provided in paragraphs 4.9.2 and 4.9.3.

		(a) before establishing a high risk business relationship[56] with a customer who is or whose beneficial owner is a ~~domestic~~ Hong Kong 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~~ Hong Kong 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 FI subsequently knows that the customer or the beneficial owner of the customer is a ~~domestic~~ Hong Kong PEP or an international organisation PEP.
Treatment of former Hong Kong PEPs or former international organisation PEPs		
	4.11.25 ~~4.11.23~~	In the situations described in paragraph 4.11.24,~~If a domestic PEP or an international organisation PEP is no longer entrusted with a prominent (public) function,~~ an FI ~~may~~ should adopt an RBA[57] ~~to determine whether~~ and may decide not to apply, or not to continue to apply, the measures set out in paragraph 4.11.12 ~~in a high risk business relationship with a customer who is or whose beneficial owner is that domestic~~ to a Hong Kong PEP or an international organisation PEP, who has been but not currently entrusted with a prominent (public) function (hereafter referred to as "former Hong Kong PEP" or "former international organisation PEP")[58] and no longer presents a high risk of ML/TF after stepping down.

[56] In determining whether a business relationship presents a high ML/TF risk, an FI should take into account all risk factors (including the list of illustrative risk indicators set out in Appendix A) that are relevant to the business relationship.

[57] The handling of a ~~domestic~~ former Hong Kong PEP or a~~n~~ former 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.

[58] For the avoidance of doubt, such decision may also apply to a spouse, a partner, a child or a parent, or a spouse or a partner of a child, or a close associate of the former Hong Kong PEP or the former international organisation PEP.

		To determine whether a former Hong Kong PEP or a former international organisation PEP no longer presents a high risk of ML/TF, the FI should conduct an appropriate assessment of the ML/TF risk associated with the previous PEP status taking into account various risk factors, ~~such as~~including but not limited to: (a) the level of (informal) influence that the individual could still exercise; (b) the seniority of the position that the individual held as a Hong Kong PEP or an international organisation PEP; ~~or~~and (c) whether the individual's previous and current functions are linked in any way (e.g. formally by appointment of the ~~PEPs~~ successor of the former Hong Kong PEP or the former international organisation PEP, or informally by the fact that the former Hong Kong PEP or the former international organisation PEP continues to deal with the same substantive matters). ~~The FI should obtain approval from its senior management for such a decision.~~
4.12 Bearer shares and nominee shareholders		
Bearer shares[59]		
s.15, Sch. 2	4.12.1	Bearer shares refer to negotiable instruments that accord ownership in a legal person to the person who possesses the physical bearer share certificate, and any other similar instruments without traceability. Therefore it is more difficult to establish the beneficial ownership of a company with bearer shares. An FI should adopt procedures to establish the identities of the beneficial owners of such shares and ensure that the FI is notified whenever there is

[59] For the avoidance of doubt, paragraphs 4.12.1 to 4.12.3 also apply to bearer share warrants, which refer to negotiable instruments that accord entitlement to ownership in a legal person to the person who possesses the physical bearer share warrant certificate, and any other similar warrants or instruments without traceability. In this regard, the reference to "bearer shares" or "shares" should also be read as "bearer share warrants" or "share warrants" respectively.

		a change of beneficial owner of such shares.
	4.12.2	Where bearer shares have been deposited with an authorised/registered custodian, FIs 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 FI's ongoing periodic review, it should obtain evidence to confirm the authorised/registered custodian of the bearer shares.
	4.12.3	Where the shares are not deposited with an authorised/registered custodian, the FI should obtain declarations prior to account opening and annually thereafter from each beneficial owner of such shares. FIs should also require the customer to notify it immediately of any changes in the ownership of the shares.
<u>Nominee shareholders</u>		
	4.12.4	For a customer identified to have nominee shareholders in its ownership structure, an FI 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.
4.13 Jurisdictions posing a higher risk		
	4.13.1	FIs should give particular attention to, and exercise extra care in respect of: (a) business relationships and transactions with persons (including legal persons and other FIs) from or in jurisdictions identified by the FATF as having strategic AML/CFT deficiencies; and (b) transactions and business connected with

		jurisdictions assessed as higher risk. In such case, the special requirements of section 15 of Schedule 2 may apply (see paragraphs 4.9).
	4.13.2	In determining which jurisdictions are identified by the FATF as having strategic AML/CFT deficiencies, or may otherwise pose a higher risk, FIs should consider, among other things: (a) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as not having effective AML/CFT Systems; (b) countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity; (c) countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the UN; or (d) countries, jurisdictions or geographical areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operation. "Credible sources" refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-government organisations.
4.14 Jurisdictions subject to a call by the FATF		
s.15, Sch. 2	4.14.1	An FI should apply additional measures, proportionate to the risks and in accordance with the

		guidance provided in paragraphs 4.9, to business relationships and transactions with natural and legal persons, and FIs, from jurisdictions for which this is called for by the FATF.
s.15, Sch. 2	4.14.2	Where mandatory enhanced measures or countermeasures[60] are called for by the FATF, or in other circumstances independent of any call by the FATF but also considered to be higher risk, RA may also, through a notice in writing: (a) impose a general obligation on FIs to comply with the special requirements set out in section 15 of Schedule 2; or (b) require FIs to undertake specific countermeasures identified or described in the notice. The type of measures in paragraphs (a) and (b) above would be proportionate to the nature of the risks and/or deficiencies.
4.15 Reliance on CDD performed by intermediaries		
<u>General</u>		
s.18, Sch. 2	4.15.1	An FI may rely upon an intermediary to perform any part of the CDD measures[61] specified in section 2 of Schedule 2, subject to the criteria set out in section 18 of Schedule 2. However, the ultimate responsibility for ensuring that CDD requirements are met remains with the FI. 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

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

[61] For the avoidance of doubt, an FI cannot rely on an intermediary to continuously monitor its business relationship with a customer for the purpose of complying with the requirements in section 5 of Schedule 2.

		relying FI, and would apply its own procedures to perform the CDD measures.
	4.15.2	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 FI, in accordance with the FI's procedures, and subject to the FI's control of effective implementation of these procedures by the outsourced entity or agent.
s.18(1), Sch. 2	4.15.3	When relying on an intermediary, the FI must: (a) obtain written confirmation from the intermediary that the intermediary agrees to act as the FI's intermediary and perform which part of the CDD measures specified in section 2 of Schedule 2; 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.
s.18(4)(a), Sch. 2	4.15.4	An FI that carries out a CDD measure by means of an intermediary must immediately after the intermediary has carried out that measure, obtain from the intermediary the data or information that the intermediary has obtained in the course of carrying out that measure, but nothing in this paragraph requires the FI 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.
s.18(4)(b), Sch. 2	4.15.5	Where these documents and records are kept by the intermediary, the FI should obtain an undertaking from the intermediary to keep all underlying CDD information throughout the continuance of the FI'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 FI ends or until such time as may be specified by the RA. The FI must ensure that the intermediary will, if requested by the FI within the period specified in the record-keeping requirements of AMLO, provide to the FI 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 FI 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 FI anymore.
	4.15.6	An FI should conduct sample tests from time to time to ensure CDD information and documentation is produced by the intermediary upon demand and without undue delay.
	4.15.7	Whenever an FI 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 FI intends to terminate its relationship with the intermediary, it should immediately obtain all CDD information from the intermediary. If the FI has any doubts regarding the CDD measures carried out by the intermediary previously, the FI should perform the required CDD as soon as reasonably practicable.
<u>Domestic intermediaries</u>		
s.18(3)(a), (3)(b) & (7), Sch. 2	4.15.8	An FI may rely upon any one of the following domestic intermediaries, to perform any part of the CDD measures set out in section 2 of Schedule 2: (a) an FI that is an authorized institution, a licensed corporation, an authorized insurer, a licensed individual insurance agent, a licensed insurance agency or a licensed insurance broker company (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 (Cap. 50), or a certified public accountant (practising) as defined by section 2(1) of the Accounting and Financial Reporting Council Ordinance (Cap. 588); (ii) a corporate practice as defined by section 2(1) of the ~~Professional Accountants Ordinance (Cap. 50)~~Accounting and Financial Reporting Council Ordinance (Cap. 588); or (iii) a CPA firm ~~of certified public accountants (practising) registered under Part IV~~ as defined by section 2(1) of the ~~Professional Accountants Ordinance (Cap. 50)~~ Accounting and Financial Reporting Council Ordinance (Cap. 588); (c) an estate agent meaning: (i) a licensed estate agent as defined by section 2(1) of the Estate Agents Ordinance (Cap. 511); or (ii) a licensed salesperson as defined by section 2(1) of the Estate Agents Ordinance (Cap. 511); (d) a legal professional meaning: (i) a solicitor as defined by section 2(1) of the Legal Practitioners Ordinance (Cap. 159); or (ii) a foreign lawyer as defined by section 2(1) of the Legal Practitioners Ordinance (Cap. 159); 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 FI 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 with respect to the customer[62].
s.18(3)(a) & (3)(b), Sch. 2	4.15.9	An FI should take appropriate measures to ascertain if the domestic intermediary satisfies the criteria set out in paragraph 4.15.8, 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 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.
<u>Overseas intermediaries</u>		
s.18(3)(c), Sch. 2	4.15.10	An FI may rely upon an overseas intermediary[63] carrying on business or practising in an equivalent jurisdiction [64] to perform any part of the CDD measures set out in section 2 of Schedule 2, 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;

[62] CDD requirements set out in Schedule 2 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.

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

[64] Guidance on jurisdictional equivalence is provided in paragraphs 4.19.

		(ii) a lawyer or a notary public; (iii) an auditor, a professional accountant, or a tax advisor; (iv) a trust or company service provider; (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 imposed under Schedule 2; 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).
	4.15.11	An FI should take appropriate measures to ascertain if the overseas intermediary satisfies the criteria set out in paragraph 4.15.10. Appropriate measures that should be taken to ascertain if the criterion set out in paragraph 4.15.10(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.
<u>Related foreign financial institutions as intermediaries</u>		
s.18(3)(d), (3A) & (7), Sch. 2	4.15.12	An FI may also rely upon a related foreign financial institution (related foreign FI) to perform any part of the CDD measures set out in section 2 of Schedule 2, 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: (i) it is within the same group of companies as the FI; (ii) if the FI is incorporated in Hong Kong, it is a branch of the FI; (iii) if the FI is incorporated outside Hong Kong: (A) it is the head office of the FI; or (B) it is a branch of the head office of the FI; (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; 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[65] that performs, in relation to the holding company or the head office of the FI, functions similar to those of an RA under the AMLO.
s.18(3A) & (4)(c), Sch. 2	4.15.13	The group policy set out in paragraph 4.15.12(b) refers to a policy of the group of companies to which the FI belongs and the policy applies to the FI and the related foreign FI. The group policy should include CDD and record-keeping requirements similar to the requirements imposed under Schedule 2 and group-wide AML/CFT Systems [66] (e.g. compliance and audit functions) to ensure compliance with those requirements. 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 FI should be satisfied that the related foreign FI is

[65] Guidance on jurisdictional equivalence is provided in paragraphs 4.19.
[66] Reference should be made to Chapter 3.

		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.
s.18(3A), Sch. 2	4.15.14	The FI 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.
4.16 Pre-existing customers		
s.6, Sch. 2	4.16.1	FIs must perform the CDD measures prescribed in Schedule 2 and this Guideline in respect of pre-existing customers (with whom the business relationship was established before the AMLO came into effect on 1 April 2012), when: (a) a transaction takes place with regard to the customer, which is, by virtue of the amount or nature of the transaction, unusual or suspicious; or is not consistent with the FI's knowledge of the customer or the customer's business or risk profile, or with its knowledge of the source of the customer's funds; (b) a material change occurs in the way in which the customer's account is operated; (c) the FI suspects that the customer or the customer's account is involved in ML/TF; or (d) the FI 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.
	4.16.2	Trigger events may include the re-activation of a dormant account or a change in the beneficial ownership or control of the account but FIs will need to consider other trigger events specific to their own customers and business.

s.5, Sch. 2	4.16.3	FIs should note that requirements for ongoing monitoring under section 5 of Schedule 2 also apply to pre-existing customers (see Chapter 5).
4.17 Failure to satisfactorily complete CDD measures		
s.3(4), Sch. 2	4.17.1	Where an FI is unable to complete the CDD measures in accordance with paragraph 4.1.9 or 4.7.1, the FI: (a) must not establish a business relationship or carry out any occasional transaction with that customer; or (b) must terminate the business relationship as soon as reasonably practicable if the FI has already established a business relationship with the customer. The FI should also assess whether this failure provides grounds for knowledge or suspicion of ML/TF and where there is relevant knowledge or suspicion, should make an STR to the JFIU in relation to the customer.
4.18 Prohibition on anonymous accounts		
s.16, Sch. 2	4.18.1	FIs must not open, or maintain, any anonymous accounts or accounts in fictitious names for any ~~new or existing~~ customer. Besides, confidential numbered accounts [67] should not function as anonymous accounts, rather they should be subject to exactly the same CDD and control measures[68] as all other business relationships. While a numbered account can offer additional confidentiality for the customer, the identity of the customer should be verified by the FI and known to a sufficient number of staff to facilitate effective CDD and ongoing monitoring.~~Where numbered accounts exist, FIs must maintain them in such a way that full~~

[67] In a confidential numbered account, the name of the customer (and/or the beneficial owner) is known to the FI but is substituted by an account number or code name in subsequent documentation.

[68] For example, wire transfers from numbered accounts should reflect the real name of the account holder.

		~~compliance can be achieved with the AMLO. FIs must 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's CDD ~~identification and verification~~ records must be available to the RAs, other authorities, the CO, auditors, and other staff with appropriate authority.
4.19 Jurisdictional equivalence		
General		
s.4(3)(b)(i), s.4(3)(d)(iii), s.4(3)(f), s.9(1)(c)(ii) & s.18(3)(c), Sch. 2	4.19.1	Jurisdictional equivalence and the determination of equivalence is an important aspect in the application of CDD measures under the AMLO. Equivalent jurisdiction is defined in the AMLO as meaning: (a) a jurisdiction that is a member of the FATF, other than Hong Kong; or (b) a jurisdiction that imposes requirements similar to those imposed under Schedule 2.
Determination of jurisdictional equivalence		
	4.19.2	An FI 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 for jurisdictional equivalence purposes. The FI should document its assessment of the jurisdiction, and include consideration of the following factors: (a) whether the jurisdiction concerned is a member of FATF-style regional bodies and its recent mutual evaluation report published by the FATF-style regional bodies[69]; (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 circulars issued by RAs from time

[69] FIs should bear in mind that mutual evaluation reports are at a "point in time", and should be interpreted as such.

		to time alerting FIs to such jurisdictions with poor AML/CFT controls; or (d) any other AML/CFT related publications that are published by specialised national, international, non-governmental or commercial organisations (for example, Transparency International's "Corruption Perceptions Index", which ranks countries according to their perceived level of corruption).
	4.19.3	As the AML/CFT regime of a jurisdiction will change over time, an FI should review the jurisdictional equivalence assessment from time to time.
4.20 Cross-border correspondent relationships		
Introduction		
	4.20.1	For the purposes of this Guideline, "cross-border correspondent relationships" refers to the provision of services for dealing in securities, dealing in futures contracts, or leveraged foreign exchange trading [70], by an FI [71] (hereafter referred to as "correspondent institution") to another financial institution[72] located in a place outside Hong Kong (hereafter referred to as "respondent institution"), where transactions effected on a principal or agency basis under the business relationships are initiated by the respondent institution.
	4.20.2	An FI may establish cross-border correspondent relationships with respondent institutions around the world. An example of cross-border correspondent relationship is where a securities firm located in

[70] For the avoidance of doubt, paragraphs 4.20 may be applicable to an FI providing these services to a respondent institution even where the FI may rely on any incidental or other exemptions provided in the SFO to be exempt from the requirement of being licensed or registered for Type 1, 2 or 3 regulated activity. For example, paragraphs 4.20 are applicable to an FI dealing in fund shares or units for its customer that is a distributor located outside Hong Kong for funds under the FI's management.

[71] For the purposes of paragraphs 4.20, the term "FI" means a licensed corporation or a registered institution.

[72] Financial institution in this context refers to businesses falling within the definition of the term "financial institutions" under the FATF Recommendations and which are conducted for or on behalf of customers.

		Hong Kong, as a correspondent institution, executes securities transactions on a stock exchange for a securities firm operating outside Hong Kong, which acts as a respondent institution for its underlying local customers.
	4.20.3	Where a respondent institution conducts business for or on behalf of customers through a cross-border correspondent relationship with an FI, the FI normally has limited information regarding the underlying customers and the nature or purpose of the underlying transactions because it generally does not have direct relationships with the underlying customers of the respondent institution. This will expose the FI to risks stemming from the lack or incompleteness of information about the underlying customers and transactions.
s.19(3) & s.23(b), Sch. 2	4.20.4	An FI should establish and maintain effective procedures for mitigating the risks associated with cross-border correspondent relationships which may vary depending on a number of factors (see paragraph 4.20.6).
<u>Additional due diligence measures for cross-border correspondent relationships</u>		
	4.20.5	An FI must carry out CDD measures[73] in relation to a customer including a respondent institution. Although an FI is permitted not to identify and take reasonable measures to verify the identities of the beneficial owners[74] of a financial institution which meets the criteria set out in paragraph 4.8.3(b), the FI should apply the following additional due diligence measures when it establishes a cross-border correspondent relationship to mitigate the associated risks:

[73] Please refer to paragraph 4.1.4.

[74] It includes the individuals who ultimately own or control the customer and the person(s) on whose behalf the customer is acting (e.g. underlying customer(s) of a customer that is an FI). For the avoidance of doubt, the provisions of paragraphs 4.20 do not require an FI to conduct CDD on the underlying customers of a respondent institution.

		(a) collect sufficient information about the respondent institution to enable it to understand fully the nature of the respondent institution's business (see paragraph 4.20.7); (b) determine from publicly available information the reputation of the respondent institution and the quality of regulatory supervision over the respondent institution by authorities in the jurisdictions in which it operates and/or is incorporated which perform functions similar to those of the RAs (see paragraph 4.20.8); (c) assess the AML/CFT controls of the respondent institution and be satisfied that the AML/CFT controls of the respondent institution are adequate and effective (see paragraph 4.20.9); (d) obtain approval from its senior management (see paragraph 4.20.10); and (e) understand clearly the respective AML/CFT responsibilities of the FI and the respondent institution within the cross-border correspondent relationship (see paragraph 4.20.11).
	4.20.6	Given that not all cross-border correspondent relationships pose the same level of ML/TF risks, the FI should adopt an RBA in applying the additional due diligence measures stated above, taking into account relevant factors such as: (a) the purpose of the cross-border correspondent relationship, the nature and expected volume and value of transactions; (b) how the respondent institution will provide services to its underlying customers through the account maintained by the FI for the respondent institution (hereafter referred to as "correspondent account"), including the potential use of the account by other respondent

		institutions through a "nested" correspondent relationship[75] and the purpose, and the direct respondent institution's control framework with respect to the "nested" correspondent relationship; (c) the types of underlying customers to whom the respondent institution intends to serve through the correspondent account, and the extent to which any of these underlying customers and their transactions are assessed as high risk by the respondent institution; and (d) the quality and effectiveness of the AML/CFT regulation as well as supervision by authorities in the jurisdictions in which the respondent institution operates and/or is incorporated[76].
	4.20.7	An FI should determine on a risk-sensitive basis the amount of information to collect about the respondent institution to enable it to understand the nature of the respondent institution's business including the respondent institution's management and ownership, the financial group to which the respondent institution belongs, major business activities, target markets, customer base and locations of customers. The FI may make reference to publicly available information to understand the respondent institution's business (e.g. where applicable, its corporate website, annual reports filed with stock exchanges, reputable newspapers and journals).
	4.20.8	When determining from publicly available information (e.g. public databases of regulatory and

[75] Nested correspondent relationship refers to the use of a correspondent account by a number of respondent institutions through their relationships with the FI's direct respondent institution, to conduct transactions and obtain access to other financial services.

[76] Consideration may be given to country assessment reports and other relevant information published by international bodies (including the FATF, FATF-style regional bodies, the International Monetary Fund and the World Bank) which measure AML/CFT compliance and address ML/TF risks, lists issued by the FATF in the context of its International Cooperation Review Group process, ML/TF risk assessments and other relevant public information from national authorities.

		enforcement actions, news media sources or other types of open source information) the reputation of the respondent institution and the quality of regulatory supervision over the respondent institution, consideration should be given to whether and when the respondent institution has been subject to any targeted financial sanction, ML/TF investigation or regulatory action.
	4.20.9	When assessing the AML/CFT controls of the respondent institution and ascertaining whether these controls are adequate and effective, the FI should have regard to the AML/CFT measures of the jurisdictions in which the respondent institution operates and/or is incorporated, and whether the AML/CFT controls of the respondent institution are subject to an independent audit. Information for assessing the AML/CFT controls may first be obtained from the respondent institution, for example, by way of a due diligence questionnaire, to facilitate the information collection and risk assessment processes. A more in-depth review of the respondent institution's AML/CFT controls should be conducted for any cross-border correspondent relationship that presents higher risks, possibly by interviewing compliance officers, conducting an on-site visit or reviewing the findings reported by internal or external auditors.
	4.20.10	An FI should obtain approval from its senior management before establishing a cross-border correspondent relationship. In this regard, the level of seniority of the member of an FI's senior management in making such approval should be commensurate with the assessed ML/TF risk.
	4.20.11	An FI should clearly understand the respective AML/CFT responsibilities of the FI and the

		respondent institution within the cross-border correspondent relationship, including the type and nature of services to be provided under the cross-border correspondent relationship, the respondent institution's responsibilities concerning compliance with AML/CFT requirements, and the conditions regarding the provision of documents, data or information on particular transactions and (where applicable) the underlying customers which should be provided by the respondent institution upon the FI's request. The level of detail may vary having regard to the nature of the cross-border correspondent relationship and the associated ML/TF risks. For example, an FI may also consider to impose potential restrictions on the use of the correspondent account by the respondent institution (e.g. limiting transaction types, volumes, etc.) in accordance with its terms of business when the ML/TF risks become higher.
<u>Direct access to the correspondent account by the underlying customers of a respondent institution</u>		
	4.20.12	Where a respondent institution meets the criteria set out in paragraph 4.8.3(b) and its underlying customers not being the customers of the FI (having regard to the definition of "customer" in paragraph 4.1.6) are allowed to directly access and operate the correspondent account[77], the FI should take further steps [78] and be satisfied that the respondent institution: (a) has conducted CDD on the underlying customers having direct access to the

[77] For example, where an FI provides its electronic trading system for a respondent institution under a white label arrangement which permits the underlying customers of the respondent institution to submit orders directly to the FI for execution, and the identities of those underlying customers are not known to the FI. For the avoidance of doubt, where a respondent institution does not meet the criteria set out in paragraph 4.8.3(b), the FI should identify and take reasonable measures to verify the identities of the underlying customers of the respondent institution, whether or not the underlying customers have direct access to the correspondent account.

[78] In this regard, the FI may also consider conducting sample tests from time to time.

		correspondent account, including verifying their identities and continuously monitoring its business relationships with them, in accordance with requirements similar to those imposed under the AMLO; and (b) will, upon the FI's request, provide documents, data or information obtained by the respondent institution in relation to those customers in accordance with requirements similar to those imposed under the AMLO.
<u>Ongoing monitoring</u>		
s.5(1)(a), Sch. 2	4.20.13	An FI should monitor the cross-border correspondent relationship in accordance with the guidance set out in Chapter 5, including: (a) on a regular basis and/or upon trigger events, reviewing the information obtained by the FI from applying the additional due diligence measures under paragraph 4.20.5 in the course of establishing the cross-border correspondent relationship with the respondent institution [79], together with other existing CDD records of the respondent institution, to ensure that the documents, data and information of the respondent institution obtained are up-to-date and relevant; and (b) monitoring transactions of the respondent institution with a view to detecting any unexpected or unusual activities or transactions, and any changes in the risk profile of the respondent institution for compliance with AML/CFT measures and applicable targeted financial sanctions. Where unusual activities or transactions are detected, the FI should follow up with the respondent institution by making a request for information on any particular transactions, and where applicable, more information on the

[79] If these additional due diligence measures have not previously been performed by the FI, the FI should do so during the review.

		underlying customers of the respondent institution on a risk-sensitive basis[80].
<u>Cross-border correspondent relationships with related foreign financial institutions</u>		
	4.20.14	Where a cross-border correspondent relationship is established with a related foreign financial institution, an FI may adopt a streamlined approach to applying additional due diligence measures and other risk mitigating measures for the cross-border correspondent relationship. The FI may rely on its group AML/CFT programme for this purpose. It may be sufficient for the FI to demonstrate its compliance with the requirements set out in paragraphs 4.20.5 to 4.20.13 by performing a documented assessment and satisfying itself that: (a) the group policy which applies to the respondent institution includes: (i) CDD, continuous monitoring of business relationships and record-keeping requirements similar to the requirements imposed under Schedule 2; (ii) the AML/CFT responsibilities of the respondent institution within the cross-border correspondent relationship; and (iii) group-wide AML/CFT Systems (including the compliance and audit functions, the provision of customer, account and transaction information to the FI's group-level compliance, audit or AML/CFT functions and the sharing of such

[80] Where the FI cannot obtain the requested information of the transactions and underlying customers in question, it may conclude that there are grounds for suspicion, leading to STR filing by the FI to the JFIU in accordance with paragraph 5.15, and triggering the need to conduct an appropriate review (including reassessing the risk of the respondent institution) of the cross-border correspondent relationship and apply appropriate measures to mitigate the risks identified. For the avoidance of doubt, where the level of ML/TF risks associated with the cross-border correspondent relationship becomes higher in the course of any review, the FI should take reasonable measures (e.g. performing enhanced measures by limiting the services provided or restricting individual transactions) to mitigate the risks.

		information for the purposes of CDD and ML/TF risk management[81]) which monitor and regularly review the effective implementation of CDD, continuous monitoring of business relationships and record-keeping requirements by the respondent institution and support effective group-wide ML/TF risk management; (b) the group policy is able to adequately mitigate any higher risk factors including country risk, customer risk, product/service/transaction risk, and delivery/distribution channel risk to which the respondent institution is exposed throughout the business relationship; and (c) the effective implementation of the group policy and group-wide AML/CFT Systems is supervised at the group level by a competent authority. The aforesaid assessment should be approved by an MIC of AML/CFT, MIC of Compliance or other appropriate senior management personnel.
<u>Cross-border correspondent relationships involving shell financial institutions</u>		
	4.20.15	An FI must not establish or continue a cross-border correspondent relationship with a shell financial institution. The FI should also take appropriate measures to satisfy itself that its respondent institutions do not permit their correspondent accounts to be used by shell financial institutions[82].

[81] This should include information and analysis of transactions or activities which appear unusual and could include an STR, its underlying information or the fact that an STR has been submitted. If the laws and regulations of the place where the respondent institution operates or is incorporated do not permit such sharing of information for group-wide ML/TF risk management, the FI should take appropriate measures to comply with the requirements in paragraphs 4.20.12 and 4.20.13.

[82] This includes a nested correspondent relationship under which the respondent institution uses the correspondent account to provide services to a shell financial institution with which it has a business relationship.

	4.20.16	For the purposes of this Guideline, a shell financial institution is a corporation that: (a) is incorporated in a place outside Hong Kong; (b) is authorised to carry on financial services businesses[83] in that place; (c) does not have a physical presence in that place (see paragraph 4.20.17); and (d) is not an affiliate[84] of a regulated financial group that is subject to effective group-wide supervision.
	4.20.17	A corporation is considered to have a physical presence[85] in a place or jurisdiction if: (a) the corporation carries on financial services businesses at any premises in that place or jurisdiction; and (b) at least one full-time employee of the corporation performs duties related to financial services businesses at those premises.
<u>Other group-wide considerations</u>		
	4.20.18	If an FI relies on a financial institution within the same group of companies (related FI) to establish a cross-border correspondent relationship and perform the additional due diligence and other risk mitigating measures set out in paragraphs 4.20.5 to 4.20.12 and 4.20.15, the FI should ensure that its related FI has taken into account the FI's own specific circumstances and business arrangements, and its particular cross-border correspondent relationship with the respondent institution. The

[83] In this context, this refers to businesses falling within the definition of the term "financial institutions" under the FATF Recommendations and which are conducted for or on behalf of customers.

[84] In this context, a corporation is an affiliate of another corporation if (a) the corporation is a subsidiary of the other corporation; or (b) at least one individual who is a controller of the corporation is at the same time a controller of the other corporation.

[85] In general, physical presence means meaningful mind and management located within a jurisdiction. The mere existence of a local agent or junior staff does not constitute physical presence.

		ultimate responsibility for ensuring that the additional due diligence and other relevant requirements are met remains with the FI.
	4.20.19	If an FI has cross-border correspondent relationships with several respondent institutions in different jurisdictions that belong to the same financial group, the FI whilst assessing each of the cross-border correspondent relationships independently should also take into account that these respondent institutions belong to the same group.

Chapter 5 - ONGOING MONITORING

General		
s.5(1), Sch. 2	5.1	Ongoing monitoring is an essential component of effective AML/CFT Systems. An FI must continuously monitor its business relationship with a customer by: (a) reviewing from time to time documents, data and information relating to the customer that have been obtained by the FI for the purpose of complying with the requirements imposed under Part 2 of Schedule 2 to ensure that they are up-to-date and relevant; (b) conducting appropriate scrutiny of transactions carried out for the customer to ensure that they are consistent with the FI's knowledge of the customer, the customer's business, risk profile and source of funds; and (c) 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 the findings in writing.
Keeping customer information up-to-date		
s.5(1)(a), Sch. 2	5.2	To ensure documents, data and information of a customer obtained are up-to-date and relevant[86], an FI should undertake reviews of existing CDD records of customers on a regular basis and/or upon trigger events[87]. Clear policies and procedures should be

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

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

		developed, especially on the frequency of periodic review or what constitutes a trigger event[88].
	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 FI, to ensure the CDD information retained remains up-to-date and relevant.
Transaction monitoring systems and processes		
s.19(3), Sch.2	5.4	An FI should establish and maintain adequate systems and processes (e.g. the use of large transactions exception reports which help an FI to stay apprised of operational activities) 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: (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 FI 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 FI 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

[88] Examples of trigger events are set out in paragraph 8 of Appendix C.

		a customer's multiple accounts within or across lines of business, and related customers' accounts within or across lines of business. This means preferably the FI adopts a relationship-based approach rather than on a transaction-by-transaction basis.
	5.7	In designing transaction monitoring systems and processes, including (where applicable) setting of parameters and thresholds, an FI 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 deposits); (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 FI should regularly review the adequacy and effectiveness of its transaction monitoring systems and processes, including (where applicable) 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 monitoring		
s.5(4) & (5), Sch. 2	5.9	FIs should conduct ongoing 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 the customer. Where the ML/TF risks are higher, the FI should conduct enhanced monitoring. In lower risk situations, the FI may reduce the extent of monitoring.

s.5(3), Sch. 2	5.10	FIs must take additional measures to compensate for any risk of ML/TF in monitoring business relationships involving (a) a customer not having been physically present for identification purposes; (b) a customer or a beneficial owner of a customer being a ~~foreign~~ non-Hong Kong PEP; and (c) a customer or a beneficial owner of a customer being involved in a situation referred to in section 15 of Schedule 2.
	5.11	FIs should be vigilant for changes of the basis of the business relationship with the customer over time. These may include where: (a) new products or services that pose higher risk are entered into; (b) new corporate or trust structures are created; (c) the stated activity or turnover of a customer changes or increases; or (d) the nature of transactions changes or their volume or size increases, etc.
	5.12	Where the basis of the business relationship changes significantly, FIs should carry out further CDD procedures to ensure that the ML/TF risk involved and basis of the relationship are fully understood. Ongoing monitoring procedures must take account of the above changes.
Review of transactions		
s.5(1)(b) & (c), Sch. 2	5.13	An FI 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 FI's knowledge of the customer, the customer's business, risk profile or source of funds; (b) the FI identifies transactions that (i) are complex,

		unusually large in amount or of an unusual pattern, and (ii) have no apparent economic or lawful purpose[89].
	5.14	Where the FI conducts enquiries and obtains what it considers to be a satisfactory explanation of the activity or transaction, it may conclude that there are no grounds for suspicion, and therefore take no further action. Even if no suspicion is identified, the FI should consider updating the customer risk profile based on any relevant information obtained.
	5.15	However, where the FI 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.
	5.16	An FI should be aware that making enquiries to customers, when conducted properly and in good faith, will not constitute tipping-off. However, if the FI reasonably believes that performing the CDD process will tip off the customer, it may stop pursuing the process. The FI should document the basis for its assessment and file an STR to the JFIU.
	5.17	The findings and outcomes of steps taken by the FI in paragraph 5.13, as well as the rationale of any decision made after taking these steps, should be properly documented in writing and be available to RAs, other competent authorities and auditors.
	5.18	Where cash transactions (including deposits and withdrawals) and third-party deposits and payments are being proposed by customers, and such requests are not in accordance with the customer's profile and normal commercial practices, FIs must approach

[89] An FI should examine the background and purposes of the transactions and set out its findings in writing.

		such situations with caution and make relevant further enquiries[90].
	5.19	Ongoing monitoring of a customer's account involving cash, third-party deposits and payments should be enhanced. An FI should be alert to the red flags relating to cash and third-party transactions, having regard to the list of illustrative indicators of suspicious transactions and activities set out in Appendix B.
	5.20	Where the FI has been unable to satisfy itself that any cash transaction or third-party deposit or payment is reasonable, and therefore considers it suspicious, it should make an STR to the JFIU.

[90] Guidance on third-party deposits and payments is provided in Chapter 11.

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 United Nations Security Council (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 & s.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 [91] 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, s.7, s.8, s.8A & s.11L, UNATMO	6.5	A number of provisions in the UNATMO are of particular relevance to FIs, and are listed below. (a) section 6 empowers the Secretary for Security (S for S) to 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 and 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

[91] 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.

		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), s.8 & s.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 FI seeking such a licence should write to the Security Bureau.
Financial sanctions & proliferation financing		
s.3(1), UNSO	6.7	UNSO empowers the Chief Executive to make regulations to implement sanctions decided by the UNSC, including targeted financial sanctions [92] against ~~individuals~~ certain persons 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 Department Bureau. Except under the authority of a licence granted by the Chief Executive, ~~I~~it is an offence: (a) to make available, directly or indirectly, any funds, or other financial assets, or economic resources, to, or for the benefit of, (i) ~~a~~ designated persons or ~~entity, as well as~~entities, (ii) persons or entities ~~those~~ acting on ~~their~~ behalf~~,~~ or at the~~ir~~ direction of the designated persons or entities mentioned in (i), or (iii) entities owned or controlled by ~~them~~any persons or entities mentioned in (i) or (ii); or ~~(a)~~(b) to deal with, directly or indirectly, any funds~~,~~ or other financial assets or economic resources

[92] 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~~ persons and entities falling within paragraph 6.7(a).

		belonging to, or owned or controlled by, ~~such~~ persons and entities~~, except under the authority of a licence granted by the Chief Executive~~ falling within paragraph (a) above.
Applicable UNSO Regulation	6.8	The Chief Executive may grant a licence for making available ~~or dealing with~~ any funds~~,~~ or other financial assets~~, and~~ or economic resources to; or dealing with any funds or other financial assets or economic resources belonging to, ~~a designated person or entity or owned or controlled by, persons or entities falling within paragraph 6.7(a)~~ under specified circumstances in accordance with the provisions of the relevant regulation made under the UNSO. An FI 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 the Democratic People's Republic of Korea (DPRK) and UNSCR 2231 (2015) against the Islamic Republic of Iran (Iran) and their successor resolutions.
s.4, WMD(CPS)O	6.10	The counter ~~proliferation financing~~ PF 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 FIs 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 FI 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 their operations, FIs should consider what implications exist 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 FI 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 FIs 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 FI should be able to identify terrorist suspects and possible designated parties, and detect prohibited transactions. To this end, an FI 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 FI. Alternatively, an FI may make arrangements to access to such a database maintained by third party service providers 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. RAs draw to the attention to FIs from time to time whenever there are any updates to the UNSCRs or sanctions lists relating to terrorism, TF and PF promulgated by the UNSC. The FI 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 FI should include in its database (i) the lists published in the Gazette or on the website of the Commerce and Economic Development Bureau; and (ii) the lists that RAs draw to the attention of FIs from time to time~~; and (iii) any relevant designations by overseas authorities which may affect its operations~~. The database should 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~~ persons or entities falling within paragraph 6.7(a), an FI should implement an effective screening mechanism [93], which should include: (a) screening its customers and any beneficial owners of the 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

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

		executing the transfer.
	6.17	The screening requirements set out in paragraph 6.16 (a) and (b) should extend to other connected parties as defined in paragraph 4.2.13 and PPTAs of a customer using an RBA.
	6.18	When possible name matches are identified during screening, an FI should conduct enhanced checks to determine whether the possible matches are genuine hits. In case of any suspicions of TF, PF or sanction violations, the FI 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 FI may rely on its overseas office to maintain the database or to undertake the screening process. However, the FI is reminded that the ultimate responsibility for ensuring compliance with the relevant regulations and legislation on TF, financial sanctions and PF remains with the FI.

Chapter 7 – SUSPICIOUS TRANSACTION REPORTS AND LAW ENFORCEMENT REQUESTS

General issues		
s.25A(1) & (7), DTROP & OSCO, s.12(1) & s.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 $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 FI is concerned, when a transaction or a series of transactions of a customer is not consistent with the FI's knowledge of the customer, or is unusual (e.g. in a pattern that has no apparent economic or lawful purpose), the FI should take appropriate steps to further examine the transactions and identify if there is any suspicion (see paragraphs 5.13 to 5.20).

	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 FI should file an STR even where no transaction has been conducted by or through the FI[94]; and (b) the STR must 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 FI, but has not yet been reported to the JFIU.
AML/CFT Systems in relation to suspicious transaction reporting		
	7.7	An FI should implement appropriate AML/CFT Systems in order to fulfil its statutory reporting obligation, 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

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

		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	The FI 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 size of the business.
<u>Money laundering reporting officer</u>		
	7.9	An FI 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, 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. To fulfil these functions, all FIs must ensure that the MLRO receives full co-operation from all staff and full access to all relevant documentation so that he is in a position to decide whether attempted or actual ML/TF is suspected or known.
<u>Identifying suspicious transactions</u>		
	7.10	An FI 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	An FI 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).
	7.12	An FI should have reasonable policies and procedures to identify and analyse relevant red flags of suspicious activities for its customer accounts. A list of non-exhaustive illustrative indicators of suspicious transactions and activities is provided in Appendix B to assist an FI in determining what types of red flags are relevant to its businesses, taking into account the nature of customer transactions, risk profile of the customers and business relationships. The list is intended solely to provide an aid to FIs, and must not be applied by FIs as a routine instrument without analysis or context. The detection of any relevant red flag by an FI however should prompt further investigations and be a catalyst towards making at least initial enquiries about the source of funds. FIs should also be aware of elements of individual transactions and situations that might give rise to suspicion of TF in certain circumstances. The FATF publishes studies of methods and trends of TF from time to time, and FIs may refer to the FATF website for additional information and guidance.
<u>Internal reporting</u>		
	7.13	An FI 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 must reach the MLRO without undue delay.
	7.14	While FIs 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 member of an FI has reported suspicion to the MLRO in accordance with the policies and procedures established by the FI for the making of such reports, the statutory obligation of the staff member has been fully satisfied.
	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 member upon internal reporting.
	7.18	When evaluating an internal report, the MLRO must take reasonable steps to consider all relevant information, including CDD and ongoing monitoring information available within or to the FI concerning the customers 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[95].
	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, the MLRO decides that there are grounds for knowledge or suspicion, he should disclose the information to the JFIU as soon as it is reasonable to do so after his evaluation is complete together with the information on which that knowledge or suspicion is based. 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

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

		taking into account all available information. It is however vital for the MLRO to keep proper records of the 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 FI 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 law enforcement investigation, an FI should indicate this in the STR. Where exceptional circumstances exist in relation to an urgent reporting, an initial notification by telephone should be considered.
	7.23	An FI is recommended to indicate any intention to terminate a business relationship in its initial disclosure to the JFIU~~, thereby allowing the JFIU to comment, at an early stage, on such a course of action~~.
	7.24	An FI should ensure STRs filed with the JFIU are of high quality taking into account feedback and guidance provided by the JFIU and RAs from time to time.
	7.25	The JFIU recognises the importance of having effective feedback procedures in place and therefore, provides feedback both in its quarterly report [96] and other appropriate platform when needed.
<u>Post reporting matters</u>		
s.25A(2)(a), DTROP & OSCO, s.12(2B)(a),	7.26	The JFIU will acknowledge receipt of an STR made by an FI under section 25A of both the DTROP and the OSCO, and section 12 of the UNATMO. If there

[96] 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. ~~LCs~~ <u>FIs</u> 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.

UNATMO		is no need for imminent action, e.g. the issue of a restraint order on an account, consent will usually be given for the institution to operate the account under the provisions of section 25A(2) of both the DTROP and the OSCO, and section 12(2B)(a) of the UNATMO. The JFIU may, on occasion, seek additional information or clarification with an FI of any matter on which the knowledge or suspicion is based. ~~If a no-consent letter is issued by the JFIU~~Otherwise, the FI should ~~act according to the content of the letter~~take appropriate action and seek legal advice where necessary.
s.25A(2), DTROP & OSCO, s.12(2), UNATMO	7.27	Filing a report to the JFIU provides FIs 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 FI 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 FI has performed the disclosed acts (transaction(s)) and the report is made on the FI's own initiative and as soon as it is reasonable for the FI to do so.
	7.28	However, the statutory defence stated in paragraph 7.27 does not absolve an FI from the legal, reputational or regulatory risks associated with the account's continued operation. An FI 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 FI.
	7.29	An FI 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 FI'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 FI's business objectives, and its capacity to mitigate the risks identified.
	7.30	An FI 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, must continue to be reported to the MLRO who should make further reports to the JFIU if appropriate.
Record-keeping		
	7.31	An FI must 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.
	7.32	An FI must 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		
	7.33	An FI may receive various requests from law enforcement agencies, e.g. search warrants, production orders, restraint orders or confiscation orders, pursuant to relevant legislation 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 FI should establish clear policies and procedures to handle these requests in an effective and timely manner, including allocation of sufficient resources. An FI should appoint a staff member as the main point of contact with law enforcement agencies.
	7.34	An FI 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 FI encounters difficulty in complying with the timeframes stipulated, the FI should at the earliest opportunity contact the officer-in-charge of the investigation for further guidance.
s.10 & s.11, DTROP, s.15 & s.16, OSCO, s.6, UNATMO	7.35	During a law enforcement investigation, an FI may be served with a restraint order which prohibits the dealing with particular funds or property pending the outcome of an investigation. An FI must ensure that it is able to ~~freeze~~ withhold 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 FIs 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	7.36	Upon the conviction of a defendant, a court may order the confiscation of his criminal proceeds and an FI may be served with a confiscation order in the event that it holds funds or other property belonging to that defendant that are deemed by the Courts 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.
	7.37	When an FI 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 FI should timely assess the risk 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 also 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. Record-keeping also enables an FI to demonstrate compliance with the requirements set out in the AMLO, this Guideline and other relevant guidance promulgated by the RAs from time to time.
	8.2	An FI should maintain CDD information, transaction records and other records that are necessary and sufficient to meet the statutory ~~record-keeping requirements under the AMLO, this Guideline~~ and ~~other~~ regulatory requirements, that are appropriate to the nature, size and complexity of its businesses. The FI should ensure that: (a) the audit trail for funds moving through the FI 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 RAs, 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 RAs.

Retention of records relating to CDD and transactions		
	8.3	An FI should keep:
s.20(1)(b)(i), Sch. 2		(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 SDD, situations where special requirements are required, additional due diligence measures and other requirements for cross-border correspondent relationships, and when taking simplified and enhanced measures[97];
s.2(1)(c), Sch. 2		(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;
s.20(1)(b)(ii), Sch. 2		(d) the original or a copy of the records and documents relating to the customer's account (e.g. account opening form; risk assessment form[98]) and business correspondence[99] 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

[97] For SDD, please refer to paragraphs 4.8; for situations where special requirements are required, please refer to paragraphs 4.9 to 4.14; for additional due diligence measures and other requirements for cross-border correspondent relationships, please refer to paragraphs 4.20; for simplified and enhanced measures, please refer to paragraph 4.1.2.

[98] This refers to a document which FIs may use to document the assessment of ML/TF risk levels associated with customers or business relationships. For example, the ML/TF risk rating of a customer (~~refer to~~ see paragraph 2.16), the assessment of ML/TF risk associated with the previous PEP status of the former non-Hong Kong PEPs, ~~the risk assessment of business relationships with domestic~~ the former Hong Kong PEPs or the former international organisation PEPs ~~who are no longer entrusted with a prominent (public) function~~ (~~refer to~~ see paragraphs 4.11.19 and 4.11.25~~23~~), etc.

[99] An FI 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 the AMLO.

		(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).
s.20(2), ~~&~~ (3) ~~&~~ (3A), Sch. 2	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 occasional transaction equal to or exceeding the CDD thresholds (i.e. $8,000 for wire transfers and $120,000 for other types of transactions[100]), an FI should keep all documents and records mentioned in paragraph 8.3 for a period of at least five years after the date of the occasional transaction.
s.20(1)(a), Sch. 2	8.5	FIs 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 FI 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.
s.20(2), Sch. 2	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.
s.21, Sch. 2	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

[100] For the avoidance of doubt, FIs that are LCs or SFC-licensed VAS Providers should not carry out occasional transactions. ~~the CDD threshold of $120,000 for other types of transactions does not apply to FIs that are SFC-licensed VAS Providers.~~ FIs ~~that are SFC-licensed VAS Providers~~ should also refer to the guidance provided in paragraph~~s~~ 12.9.1 for occasional transaction that is a virtual asset transfer~~ and 12.9.2~~.

		consists of data or information, such record should be kept either on microfilm or in the database of a computer.
s.20(4), Sch. 2	8.8	An RA may, by notice in writing to an FI, require it to keep the records relating to a specified transaction or customer for a period specified by the RA 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 carried out by the RA, or to any other purposes as specified in the notice.
Part 3, Sch. 2	8.9	Irrespective of where CDD and transaction records are held, an FI is required to comply with all legal and regulatory requirements in Hong Kong, especially Part 3 of Schedule 2.
Records kept by intermediaries		
s.18(4)(b), Sch. 2	8.10	Where customer identification and verification documents are held by an intermediary on which the FI is relying to carry out CDD measures, an FI concerned remains responsible for compliance with all record-keeping requirements. The FI should ensure that the intermediary being relied on has systems in place to comply with all the record-keeping requirements under the AMLO and 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 FI.
s.18(4)(a), Sch. 2	8.11	For the avoidance of doubt, an FI that relies on an intermediary for carrying out a CDD measure should immediately obtain the data or information that the intermediary has obtained in the course of carrying out that measure.
	8.12	An FI should ensure that an intermediary will pass the documents and records to the FI, 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 FI'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 FI 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 FI 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 FI 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 FI's and their own personal statutory obligations and the possible consequences for failure to comply with CDD and record-keeping requirements under the AMLO; (b) their FI'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 FIs and themselves under the

		DTROP, the OSCO, the UNATMO, the UNSO, the WMD(CPS)O and the AMLO, and the possible consequences of breaches of these obligations; (d) the FI'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 FI 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 FI; and (ii) the need for identifying and reporting of any suspicious transactions to the MLRO, and the offence of tipping-off; (b) front-line personnel who are dealing directly with the public: (i) the importance of their roles in the FI's ML/TF strategy, as the first point of contact with potential money launderers; (ii) the FI'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 FI'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 FI 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 FI may consider including available FATF papers and typologies as part of the training materials. The FI should be able to demonstrate to the RA that all materials should be up-to-date and in line with current requirements and standards.
	9.7	No matter which training approach is adopted, an FI 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 FI should monitor the effectiveness of the training. This may be achieved by: (a) testing staff's understanding of the FI'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 FI'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	This Chapter primarily applies to authorized institutions and money service operators. Other FIs should also comply with section 12 of Schedule 2 and the guidance provided in this Chapter if they act as an ordering institution, an intermediary institution or a beneficiary institution as defined under the AMLO. Where an FI 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 under section 12 of Schedule 2 or this Chapter in respect of that transaction.
s.1(4) & s.12(11), Sch. 2	10.2	A wire transfer is a transaction carried out by an institution (the ordering institution) on behalf of a person (the originator) by electronic means with a view to making an amount of money available to that person or another person (the recipient) at an institution (the beneficiary institution), which may be the ordering institution [101] or another institution, whether or not one or more other institutions (intermediary institutions) participate in completion of the transfer of the money. An FI should follow the relevant requirements set out in this Chapter with regard to its role in a wire transfer.
	10.3	The requirements set out in section 12 of Schedule 2 and this Chapter are also applicable to wire transfers using cover payment mechanism (e.g. MT202COV payments)[102].
s.12(2), Sch. 2	10.4	Section 12 of Schedule 2 and this Chapter do not apply to the following wire transfers:

[101] For example, a wire transfer conducted between branches of the same FI.

[102] 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.

		(a) a wire transfer between two FIs as defined in the AMLO if each of them acts on its own behalf; (b) a wire transfer between an FI as defined in the AMLO and a foreign institution[103] 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 or prepaid 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 card, ~~or~~ debit card or prepaid card)~~,~~; ~~(i)~~(ii) ~~except when~~ the card is not used as a payment system to effect a person-to-person transfer ~~of money~~; and ~~(ii)~~(iii)the number (or equivalent unique identifier) of the credit card ~~or,~~ debit card or prepaid card ~~number~~ is included in the message or payment form accompanying the transfer.
Ordering institutions		
s.12(3) & (5), Sch. 2	10.5	An ordering institution must ensure that a wire transfer of amount equal to or above $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 by the ordering institution;

[103] For the purposes of section 12 of Schedule 2 and 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.

		(c) the originator's address or, the originator's customer identification number [104] 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.
s.12(3), (3A) & (5), Sch. 2	10.6	An ordering institution must ensure that a wire transfer of amount below $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 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.

[104] 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 must 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 $8,000 (or an equivalent amount in any other currency), an ordering institution must ensure that the required originator information accompanying the wire transfer is accurate.
s.3(1)~~(c) &~~(d) & (1A), Sch. 2	10.9	For an occasional wire transfer involving an amount equal to or above $8,000 (or an equivalent amount in any other currency), an ordering institution must verify the identity of the originator. For an occasional wire transfer below $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 $8,000 (or an equivalent amount in any other currency), or when there is a suspicion of ML/TF.
s.12(7), Sch. 2	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.
s.12(6), Sch. 2	10.11	For a domestic wire transfer [105], 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

[105] 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.

		traceability of the wire transfer.
s.12(6), Sch. 2	10.12	If an ordering institution chooses not to include complete required originator information as stated in paragraph 10.11, it must, on the request of the institution to which it passes on the transfer instruction or the RA, 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.
s.19(2), Sch. 2	10.13	An ordering institution should establish and maintain effective procedures to ensure that proper safeguards exist to prevent carrying out outgoing wire transfers that do not comply with the relevant originator or recipient information requirements, which include: (a) taking reasonable measures (e.g. regular review or testing by internal control or audit function to assess system capabilities) to identify whether domestic or cross-border wire transfers lack required originator information or required recipient information; and (b) having risk-based policies and procedures for handling wire transfers lacking required originator information or required recipient information, and timely rectifying any control deficiencies identified.
Intermediary institutions		
s.12(8), Sch. 2	10.14 ~~10.13~~	An intermediary institution must 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.
	10.15 ~~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.
s.19(2), Sch. 2	10.16 ~~10.15~~	An intermediary institution must 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.
s.12(10)(a), Sch. 2	10.17 ~~10.16~~	In respect of the risk-based policies and procedures referred to in paragraph 10.16~~5~~, if a cross-border wire transfer is not accompanied by the required originator information or required recipient information, the intermediary institution must 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.

s.12(10)(b), Sch. 2	10.18 ~~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 must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved.
Beneficiary institutions		
s.19(2), Sch. 2	10.19 ~~10.18~~	A beneficiary institution must 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.
s.12(9)(a) & s.12(10)(a), Sch.2	10.20 ~~10.19~~	In respect of the risk-based policies and procedures referred to in paragraph 10.1~~98~~, if a domestic or cross-border wire transfer is not accompanied by the required originator information or required recipient information, the beneficiary institution must 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.
s.12(9)(b) & s.12(10)(b), Sch.2	10.21 ~~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 must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved.
s.3(1) & ~~(c)~~(1A), Sch. 2	10.22 ~~10.21~~	For a wire transfer of amount equal to or above $8,000 (or an equivalent amount in any other currency), a beneficiary institution should verify the identity of the recipient, if the identity has not been previously verified.

Chapter 11 – THIRD-PARTY DEPOSITS AND PAYMENTS

General		
	11.1	When a customer uses a third party[106] to pay for or receive the proceeds of investment, there is a risk that the arrangement may be used to disguise the true beneficial owner or the source of funds. There are increased risks that these investment transactions are linked to predicate offences in securities markets (such as insider dealing and market manipulation) or used to launder illicit proceeds obtained elsewhere.
s.23(b), Sch. 2	11.2	An FI must take all reasonable measures to mitigate the ML/TF risks associated with transactions involving third-party deposits and payments, having regard to the provisions in this ~~Chapter~~ Guideline as well as relevant circulars and frequently asked questions published by the SFC from time to time.
Policies and procedures		
	11.3	Third-party deposits or payments should be accepted only under exceptional and legitimate circumstances and when they are reasonably in line with the customer's profile and normal commercial practices. Before an FI accepts any third-party deposit or payment arrangement, it should ensure that adequate policies and procedures are put in place to mitigate the inherently high risk and meet all applicable legal and regulatory requirements. These policies and procedures should be approved by senior management and address, among others:

[106] For the purposes of Chapter 11, "third party" means any person other than the customer.

		(a) the exceptional and legitimate circumstances under which third-party deposits or payments[107] may be accepted and their evaluation criteria; (b) the monitoring systems and controls for identifying transactions involving third-party deposits in the form of funds (i.e. fiat currency)[108]; (c) if applicable, the due diligence process for assessing whether third-party deposits or payments meet the evaluation criteria for acceptance; (d) if an FI allows the due diligence on the source of a deposit or the evaluation of a third-party deposit to be completed after settling transactions with the deposited funds (please refer to paragraphs 11.9 to 11.11) in exceptional situations, the identification of those exceptional situations and the risk management policies and procedures concerning the conditions under which such delayed due diligence or evaluation may be allowed[109]; (e) the enhanced monitoring of client accounts involving third-party deposits or payments[110], and the reporting of any ML/TF suspicions identified to the JFIU; and (f) the respective designated managers or staff members responsible for carrying out these policies and procedures. An MIC of AML/CFT, MIC of Compliance or other appropriate senior management personnel should

[107] Given that the need for third-party payments should be rare and normal commercial practices may differ, circumstances which may be considered to be exceptional and legitimate for third-party payments may not be the same as or similar to those for third-party deposits.

[108] For example, an FI may require the client to confirm whether a cheque deposit made for the account of the client has originated from the bank account of client or a third party, and provide an image of the cheque showing the name of its drawer.

[109] For the avoidance of doubt, delayed due diligence on the source of a deposit or evaluation of a third-party deposit should be allowed only when there is no suspicion of ML/TF.

[110] The extent of enhanced monitoring should be commensurate with the ML/TF risks posed by the third parties. For example, closer monitoring should be applied to deposits from third parties who are not immediate family members (e.g. a spouse, parent or child), beneficial owners or affiliated companies of the clients, regulated custodians or lending institutions.

		be designated to oversee the proper design and implementation of these policies and procedures.
	11.4	To facilitate the prompt identification of the sources of deposits in the form of funds, FIs are strongly encouraged to require their clients to designate bank accounts held in their own names or the names of any acceptable third parties for the making of all deposits. This will make it easier for FIs to ascertain whether deposits have originated from their clients or any acceptable third parties[111].
Due diligence process for assessing third-party deposits and payments		
	11.5	Due diligence process for assessing third-party deposits and payments should include: (a) critically evaluating the reasons and the need for third-party deposits or payments; (b) taking reasonable measures on a risk-sensitive basis to: (i) verify the identities of the third parties; and (ii) ascertain the relationship between the third parties and the customers; (c) obtaining the approval of the MIC of AML/CFT, another member of senior management with a relevant role at the FI with respect to AML/CFT, or MLRO (hereafter referred to as "third-party deposit or payment approvers") for the acceptance for a third-party deposit or payment; and (d) documenting the findings of inquiries made and corroborative evidence obtained during the due diligence process as well as the approval of a third-party deposit or payment.

[111] Likewise, if applicable, the use of designated bank accounts held in the names of any acceptable third parties for the making of fund withdrawals will make it easier for FIs to complete the necessary due diligence to determine the acceptability of a third-party payee before effecting a third-party fund payment.

	11.6	While a standing approval may be given by third-party deposit or payment approvers for accepting deposits or payments from or to a particular third party after assessing the risks and reasonableness of the third-party arrangement, the standing approval should be subject to review periodically or upon trigger events to ensure that it remains appropriate.
	11.7	Given that not all third-party payors and payees pose the same level of ML/TF risk[112], an FI should apply enhanced scrutiny to those third parties which might pose higher risks, and require the dual approval of deposits or payments from or to such third parties by the third-party deposit or payment approvers for enhanced control.
	11.8	An FI should exercise extra caution when the relationship between the customer and the third party is hard to verify, the customer is unable to provide details of the identity of the third-party payor for verification before the deposit is made, or one third party is making or receiving payments for or from several seemingly unrelated customers.
Delayed due diligence on the source of a deposit or evaluation of a third-party deposit in the form of funds		
	11.9	An FI should perform due diligence on the source of a deposit and evaluation of any third-party deposit (hereafter referred to as "third-party deposit due diligence") before settling transactions with the deposited funds. However, FIs may, in exceptional situations, complete the third-party deposit due diligence after settling transactions with the deposited funds, provided that: (a) any risk of ML/TF arising from the delay in

[112] Examples of third parties that are generally considered to pose relatively low risks include immediate family members (e.g. a spouse, parent or child), beneficial owners or affiliated companies of the customers, or regulated custodians or lending institutions. Other third parties might pose higher risks.

		completing the third-party deposit due diligence can be effectively managed; (b) it is necessary to avoid interruption of the normal conduct of business with the customer[113]; and (c) the third-party deposit due diligence is completed as soon as possible after settling transactions with the deposited funds.
	11.10	If an FI allows third-party deposit due diligence to be delayed in exceptional situations, it should adopt appropriate risk management policies and procedures setting out the conditions under which the customer may utilise the deposited funds prior to the completion of the third-party deposit due diligence. These policies and procedures should include: (a) establishing a reasonable timeframe[114] for the completion of the third-party deposit due diligence, and the follow-up actions if the stipulated timeframe is exceeded (e.g. to suspend or terminate the business relationship); (b) placing appropriate limits on the number, types, and/or amount of transactions that can be performed[115]; (c) performing enhanced monitoring of transactions carried out by or for the customer; and (d) ensuring senior management is periodically informed of all cases involving delay in completing third-party deposit due diligence.

[113] An example of a situation where it may be necessary not to interrupt the normal conduct of business is when FIs are required to meet settlement obligations on behalf of its customers (e.g. to meet a margin call deadline) using funds the customer has deposited shortly before.

[114] In determining the reasonable timeframe for completing third-party deposit due diligence, an FI should take into account the ML/TF risks associated with the business relationship with a customer, e.g. a stricter timeframe is imposed on deposits for high risk customers.

[115] For example, prior to the completion of third-party deposit due diligence on the deposited funds, an FI may restrict a customer from withdrawing the subsequent sales proceeds arising from the disposal of investments purchased with the deposited funds (except to return funds to the payment source). In this regard, the FI should ensure that a standing authority or written direction is obtained from the client to return the funds to the third party's payment source (see sections 4 to 8 of the Securities and Futures (Client Money) Rules).

	11.11	If the third-party deposit due diligence cannot be completed within the reasonable timeframe set out in the FI's risk management policies and procedures, the FI should refrain from carrying out further transactions for the customer. The FI should assess whether there are grounds for knowledge or suspicion of ML/TF and filing an STR to the JFIU, particularly where the customer refuses without reasonable explanation to provide information or document requested by the FI, or otherwise refuses to cooperate with the third-party deposit due diligence process.

Chapter 12 – VIRTUAL ASSETS

12.1 Introduction		
	12.1.1	This Chapter provides guidance on the ML/TF risks in relation to virtual assets and the AML/CFT regulatory requirements and standards for addressing such risks. These include factors that should be taken into consideration when conducting risk assessments under an RBA, virtual asset-specific requirements in conducting CDD and ongoing monitoring, and requirements in relation to virtual asset transfers and third-party deposits and payments in the form of virtual assets. It also provides elaborations and explanations of existing requirements in this Guideline with respect to their application to virtual asset transactions and activities, and sets out non-exhaustive illustrative risk indicators for assessing ML/TF risks and indicators of suspicious transactions and activities in relation to virtual assets.
	12.1.2	This Chapter is applicable to FIs that are SFC-licensed VAS Providers,~~. For~~ and LCs ~~which are not SFC-licensed VAS Providers, they should comply with and/or have regard to the relevant provisions in this Chapter~~ when carrying out businesses associated with virtual assets[116] or businesses which give rise to ML/TF risks in relation to virtual assets[117].
	12.1.3	For the purposes of this Chapter, ~~T~~the term "virtual assets" means (i) any "virtual asset" as defined in section 53ZRA of the AMLO; and (ii) any security token. The term "security token" means a cryptographically secured digital representation of

[116] ~~For example, when an LC offers products, services or transactions involving virtual assets.~~

[117] For example, when an LC offers products, services or transactions involving virtual assets, or when an LC's customer derives its funds or wealth substantially from virtual assets or carries out virtual asset businesses.

		value which constitutes “securities” as defined in section 1 of Part 1 of Schedule 1 to the SFO.
s.23(a) & (b), Sch. 2	12.1.4	An FI must take all reasonable measures to ensure that proper safeguards exist to prevent a contravention of any requirement under Part 2 or 3 of Schedule 2 and to mitigate the ML/TF risks in relation to virtual assets, having regard to the guidance and requirements set out in this Chapter as well as (where applicable) relevant circulars and frequently asked questions published by the SFC from time to time.
Potential uses of the virtual asset sector in the money laundering process		
	12.1.5 ~~12.1.4~~	Virtual asset transactions are, in general, pseudonymous or anonymity-enhanced by nature. Illicit actors or money launderers could take advantage of the borderless nature and near-instantaneous transaction speed that virtual assets provide. In addition, virtual asset transactions could be exploited by illicit actors or money launderers as they can be conducted on peer-to-peer basis without any involvement of intermediaries to carry out AML/CFT measures such as CDD and transaction monitoring.
	12.1.6 ~~12.1.5~~	There are three common stages in the laundering of money, and they frequently involve numerous transactions. An FI should be alert to any such sign for potential criminal activities. These stages are: (a) Placement - the ~~physical~~ disposal of cash proceeds or disposal of virtual assets derived from illegal activities; (b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions, or utilising technologies (e.g. anonymity-enhancing technologies or mechanisms), designed to disguise the source of the funds or virtual assets, 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.
	12.1.7 ~~12.1.6~~	Transactions facilitated by virtual asset businesses may be cash based, and hence may be used as the initial placement of criminally derived cash proceeds. Further, virtual asset businesses may be used as the placement facility for disposing or depositing virtual assets derived from illicit activities or linked to predicate offences (such as online scams, ransomware and other cybercrimes).
	12.1.8 ~~12.1.7~~	~~The v~~Virtual asset businesses are also likely to be used at the second stage of money laundering, i.e. the layering process. These businesses provide a potential avenue which enables the illicit actors or money launderers to dramatically alter the form of funds (i.e. fiat currency) or virtual assets. ~~Such alteration~~This not only allows conversion from cash in hand or other funds to virtual assets ~~or~~ as well as conversion from one type of virtual asset to another, ~~but~~ it also allows conversion from virtual assets derived from illicit activities or associated with illicit sources to cash in hand or other funds after conducting transactions for no other purposes but to further obfuscate the fund flows~~,~~ and the identity of the holder or beneficial owner of the virtual assets. To obfuscate the sources of virtual assets derived from illicit activities, illicit actors or money launderers may move assets across multiple wallet addresses, service providers, types of virtual assets or blockchains. They may exploit virtual

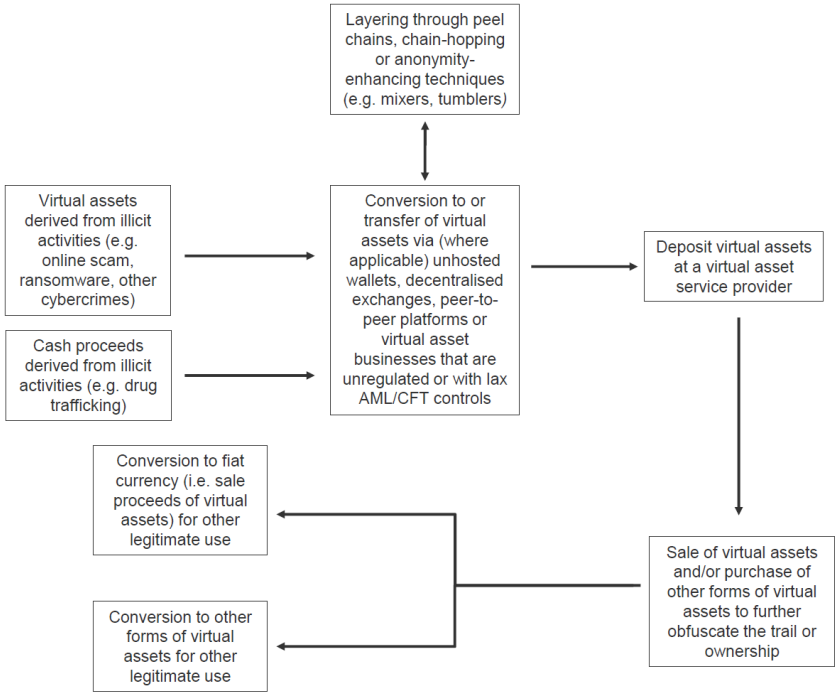
		asset-specific layering techniques such as peel chains[118] and chain-hopping[119]. Virtual assets are sometimes laundered through anonymity-enhancing services such as mixers or tumblers [120] and the use of other anonymity-enhancing technologies or mechanisms (e.g. anonymity-enhanced virtual asset or privacy coin, privacy wallet, etc.).
	12.1.9 ~~12.1.8~~	Unhosted wallets [121], decentralised virtual asset exchanges, peer-to-peer platforms, or virtual asset businesses that are unregulated or with lax AML/CFT controls are particularly attractive to illicit actors or money launderers.
	12.1.10 ~~12.1.9~~	The combination of the ability to readily convert virtual assets procured with both licit and illicit proceeds, the ability to conceal the source of the illicit proceeds, the availability of a vast array of virtual assets, and the ease and near-instantaneous transaction speed with which virtual asset transactions can be effected, offers illicit actors or money launderers attractive ways to effectively integrate criminal proceeds into the general economy.

[118] Peel chains mean moving a large amount of virtual assets through a series of transactions in which a slightly smaller amount of virtual assets is transferred to a new address each time.

[119] Chain-hopping means moving virtual assets on a blockchain to another blockchain, often in rapid succession and with the aim of evading attempts to track these movements.

[120] Mixers or tumblers are services which mix virtual assets from different users and subsequently return the assets to a new wallet address designated by the users, with an aim to break the connection between a sending and receiving address and obscure the trail to the original source while simultaneously improving the anonymity of transactions.

[121] An unhosted wallet refers to software or hardware that enables a person to store and transfer virtual assets on his own behalf, and in relation to which the private key is controlled or held by that person.

	12.1.11 ~~12.1.10~~	In addition to the examples of money laundering methods and characteristics of financial transactions that have been linked with terrorist financing provided in paragraph 1.19, the chart set out below illustrates the money laundering process relevant to the virtual asset sector in detail. 
12.2 RBA - Institutional risk assessment and customer risk assessment		
Considering relevant risk factors		
	12.2.1	In addition to the factors set out in paragraph 2.7 which an FI should holistically consider in determining the level of overall risk that the FI is exposed to, an FI should consider: (a) in relation to country risk, the regulatory and supervisory regime and controls of the jurisdictions in which the FI is operating or otherwise exposed to – for example, the regulatory treatment of virtual assets in the jurisdiction; and the AML/CFT laws and regulations of the jurisdiction, including (where applicable) those in relation to virtual asset service providers (VASPs) (referred to in

		paragraph 12.6.1); and (b) in relation to product/service/transaction risk: (i) the characteristics of the products and services that it offers and transactions it executes, and the extent to which these are vulnerable to ML/TF abuse, for example, (A) the market capitalisation, value and price volatility, trading volume or liquidity, and (where applicable) market share of a virtual asset that it offers; (B) whether a product is or a service involves an anonymity-enhanced virtual asset or other virtual asset that has characteristics that promote anonymity, obfuscate the trail of transactions or impede the FI in identifying the counterparties of the transactions; (C) whether the virtual asset transactions are effected under an open (e.g. public blockchain) or closed-loop system (e.g. private blockchain); and (D) (where applicable) the reputation and AML/CFT controls of the issuer and/or the central entity governing the arrangement in relation to the virtual asset; and (ii) the proportion of virtual asset transactions conducted for its customers that are identified as being associated with illicit or suspicious activities/sources[122].
	12.2.2	Pursuant to paragraph 2.8, in identifying and assessing the ML/TF risks that may arise in relation to the development of new products and new business practices and the use of new or developing technologies for both new and pre-existing products, an FI should also identify and assess the ML/TF risks that may arise from

[122] Examples of illicit or suspicious activities/sources are provided in paragraph 12.7.3.

		conducting virtual asset transactions involving the use of anonymity-enhancing technologies or mechanisms, including but not limited to anonymity-enhanced virtual assets, mixers, tumblers, privacy wallets and other technologies that obfuscate the identity of the originator, recipient, holder, or beneficial owner of a virtual asset. In taking appropriate measures to mitigate and manage the risks identified, the FI should refrain from conducting such virtual asset transactions if the identified risks cannot be mitigated and managed.
Conducting risk assessment		
	12.2.3	When conducting institutional risk assessment and customer risk assessment, in addition to the list of illustrative risk indicators set out in Appendix A, an FI should also refer to paragraphs 12.15 for the list of non-exhaustive illustrative risk indicators in relation to virtual assets, which may help identify a higher or lower level of risk associated with the risk factors stated in paragraphs 2.6 and 2.17 and should be taken into account holistically whenever relevant.
12.3 CDD – What CDD measures are and when they must be carried out		
When CDD measures must be carried out		
s.3(1A), Sch.2	12.3.1	In addition to the circumstances set out in paragraph 4.1.9 pursuant to which an FI must carry out CDD measures in relation to a customer, an FI must carry out CDD measures in relation to a customer before carrying out for the customer an occasional transaction that is a virtual asset transfer involving virtual assets that amount to no less than $8,000, whether the transaction is carried out in a single operation or in several operations that appear to the FI to be linked.

~~s.3(1B), Sch.2~~	~~12.3.2~~	~~In addition to the circumstances set out in paragraphs 4.1.9 and 12.3.1 pursuant to which an FI must carry out CDD measures in relation to a customer, an FI that is an SFC-licensed VAS Provider must carry out CDD measures in relation to a customer before carrying out for the customer an occasional transaction that:~~ ~~involves an amount equal to or above $8,000 or an equivalent amount in any other currency; and~~ ~~is not a wire transfer or a virtual asset transfer,~~ ~~whether the transaction is carried out in a single operation or in several operations that appear to the SFC-licensed VAS Provider to be linked.~~
	12.3.2 ~~12.3.3~~	In the context of virtual assets, "occasional transactions" [123] may also include, for example, virtual asset transfers and virtual asset conversions.
	12.3.3 ~~12.3.4~~	The criterion in paragraph 4.1.9(c) also applies irrespective of the $8,000 threshold applicable to occasional transactions set out in paragraphs 12.3.1 ~~and 12.3.2~~.
	12.3.4 ~~12.3.5~~	An FI should be vigilant to the possibility that a series of linked occasional transactions could meet or exceed the CDD thresholds of $8,000 for occasional transactions set out in paragraphs 12.3.1 ~~and 12.3.2~~. Where FIs become aware that this threshold is met or exceeded, CDD measures must be carried out.
	12.3.5 ~~12.3.6~~	The factors linking occasional transactions are inherent in the characteristics of the transactions – for example, where several payments are made to the same recipient from one or more sources over

[123] It should be noted that ~~"occasional transactions" do not apply to~~ FIs that are LCs or SFC-licensed VAS Providers should not carry out "occasional transactions".

		a short period, where a customer regularly transfers funds or virtual assets to one or more destinations. In determining whether the transactions are in fact linked, FIs should consider these factors against the timeframe within which the transactions are conducted.
12.4 CDD – Identification and verification of the customer's identity		
Other considerations		
	12.4.1	In addition to the identification information in paragraphs 4.2.2, 4.2.5 and 4.2.10, (where applicable) an FI should obtain additional customer information that enables it to identify, manage and mitigate the ML/TF risks associated with the channels [124] through which the FI establishes business relationship with its customers, and/or through which its customers conduct ~~the~~ virtual asset transactions ~~are conducted by its customers~~. Such additional customer information could include: (a) IP address(es) with an associated time stamp; (b) geo-location data; and (c) device identifier(s).
12.5 CDD – Pre-existing customers		
	12.5.1	For SFC-licensed VAS Providers that were not licensed by the SFC under the SFO before 1 June 2023, the reference to "the AMLO came into effect on 1 April 2012" in paragraph 4.16.1 should be read as "1 June 2023".
12.6 CDD – Cross-border correspondent relationships		
Introduction		
	12.6.1	In the context of virtual assets, "cross-border correspondent relationships" set out in paragraph

[124] For example, virtual asset transactions are typically conducted by customers of an FI through non-face-to-face channels (e.g. web-based platforms and mobile applications).

		4.20.1 also refers to, for the purposes of this Guideline, the provision of services by an FI in the course of providing a VA service as defined in section 53ZR of the AMLO –(hereafter referred to as "correspondent institution") to a VASP[125] or financial institution[126] located in a place outside Hong Kong (hereafter referred to as "respondent institution"), where transactions effected on a principal or agency basis under the business relationships are initiated by the respondent institution.
	12.6.2	An example of a cross-border correspondent relationship in the context of virtual assets is where an FI located in Hong Kong, as a correspondent institution, executes virtual asset trading transactions for a VASP or a financial institution operating outside Hong Kong, which acts as a respondent institution for its underlying local customers.
Additional due diligence measures for cross-border correspondent relationships		
	12.6.3	In determining on a risk-sensitive basis pursuant to paragraph 4.20.7 the amount of information to collect about a respondent institution to enable it to understand the nature of the respondent institution's business, an FI should understand whether the respondent institution engages in activities or transactions involving virtual assets that provide higher anonymity such as anonymity-enhanced virtual assets; and the extent to which any of these activities or transactions are conducted for non-resident customers of the respondent institution.

[125] For the purposes of this Guideline, VASP refers to businesses falling within the definition of the term "virtual asset service providers" under the FATF Recommendations and which are conducted for or on behalf of customers.

[126] For the purposes of this Chapter, financial institution refers to businesses falling within the definition of the term "financial institutions" under the FATF Recommendations and which are conducted for or on behalf of customers.

	12.6.4	When assessing the AML/CFT controls of a respondent institution pursuant to paragraph 4.20.9, where the respondent institution handles virtual asset transactions, an FI should assess and ascertain whether the AML/CFT controls implemented by the respondent institution in relation to, among other things, virtual asset transfers, and screening of virtual asset transactions and the associated wallet addresses are adequate and effective.
Ongoing monitoring		
	12.6.5	In monitoring transactions of the respondent institution under paragraph 4.20.13(b), an FI should also take into account the requirements for ongoing monitoring of virtual asset transactions and the associated wallet addresses in paragraphs 12.7.2 to 12.7.4 and 12.7.6.
Cross-border correspondent relationships involving shell VASPs		
	12.6.6 ~~12.6.5~~	In addition to the prohibition to establish or continue a cross-border correspondent relationship with a shell financial institution under paragraph 4.20.15, an FI must not establish or continue a cross-border correspondent relationship with a shell VASP. The FI should also take appropriate measures to satisfy itself that its respondent institutions do not permit their correspondent accounts to be used by shell VASPs[127].
	12.6.7 ~~12.6.6~~	For the purposes of this Guideline, a shell VASP is a corporation that: (a) is incorporated in a place outside Hong Kong;

[127] This includes a nested correspondent relationship under which the respondent institution uses the correspondent account to provide services to a shell VASP with which it has a business relationship.

		(b) is authorised to carry on virtual asset businesses[128] in that place; (c) does not have a physical presence in that place (see paragraph 4.20.17); and (d) is not an affiliate[129] of a regulated financial group that is subject to effective group-wide supervision.
Other considerations		
	12.6.8 ~~12.6.7~~	Where an FI establishes similar business relationships with VASPs or financial institutions operating in Hong Kong ("correspondent relationships")[130], the FI will also be exposed to risks similar to cross-border correspondent relationships (i.e. lack or incompleteness of information about the underlying customers and transactions). In particular, the FI will be exposed to higher risks for correspondent relationships with VASPs that are not licensed or regulated but operating in Hong Kong. Where applicable, the FI should adopt an RBA in applying the additional due diligence and other risk mitigating measures set out in paragraphs 4.20.5 to 4.20.13 and 12.6.3 to 12.6.4 for the correspondent relationships with VASPs or financial institutions operating in Hong Kong.
12.7 Ongoing monitoring in relation to virtual asset transactions and activities		
	12.7.1	Given the pseudonymous nature and transaction speed of virtual assets, illicit actors and designated

[128] In this context, this refers to businesses falling within the definition of the term "virtual asset service providers" under the FATF Recommendations and which are conducted for or on behalf of customers.

[129] In this context, a corporation is an affiliate of another corporation if (a) the corporation is a subsidiary of the other corporation; or (b) at least one individual who is a controller of the corporation is at the same time a controller of the other corporation.

[130] This refers to where an FI provides services in the course of providing a VA service as defined in section 53ZR of the AMLO to VASPs or financial institutions operating in Hong Kong, where transactions effected on a principal or agency basis under the business relationships are initiated by the VASPs or financial institutions.

		parties may easily obfuscate the fund flows and further complicate the trail by utilising multiple wallets to conduct numerous ~~and/~~or structured virtual asset transactions, thereby concealing the origin and destination of their virtual assets to avoid the detection of their ML/TF or other illicit activities.
	12.7.2	An FI[131] should therefore implement effective risk-based transaction monitoring procedures to detect the origin and destination of the virtual assets transferred from or to its customers or other parties in relation to virtual asset transactions conducted for its customers[132], particularly those from or to a VA transfer counterparty that presents a higher ML/TF risk (see paragraph 12.13.11) or an unhosted wallet (see paragraph 12.14.3), and to identify and report suspicious transactions as well as take~~ing~~ appropriate follow-up actions.
	12.7.3	In this connection, the FI should establish and maintain adequate and effective systems and controls to conduct screening of virtual asset transactions and the associated wallet addresses. In particular, the FI should[133]: (a) track the transaction history of virtual assets to more accurately identify the source and destination of these virtual assets; and

[131] For the avoidance of doubt, paragraphs 12.7.2 to 12.7.4 and 12.7.6, Chapter 11 and paragraphs 12.10 are applicable to an FI that is an LC when it manages or distributes virtual asset funds that accept subscriptions or redemptions made by the fund investors in the form of virtual assets. Where such subscriptions or redemptions are handled by an appointed institution such as an administrator or a transfer agent, the LC should ensure that the appointed institution has appropriate measures in place to ensure compliance with the requirements similar to those imposed in paragraphs 12.7.2 to 12.7.4 and 12.7.6, Chapter 11 and paragraphs 12.10, so as to ensure that proper safeguards exist to mitigate the associated ML/TF risks.

[132] These include virtual asset transfers referred to in paragraphs 12.11.5 to 12.11.2~~43~~ and 12.14.

[133] For the avoidance of doubt, the FI should conduct screening of virtual asset transactions and/or the associated wallet addresses before conducting a virtual asset transfer or making the transferred virtual assets available to the customer, and after conducting a virtual asset transfer on a risk-sensitive basis, so as to more timely and accurately identify the source and destination of these virtual assets and involvement or subsequent involvement of wallet addresses that are directly and/or indirectly associated with illicit or suspicious activities/sources, or designated parties.

		(b) identify transactions involving wallet addresses that are directly and/or indirectly associated with illicit or suspicious activities/sources[134], or designated parties. The FI should adopt appropriate technological solutions (e.g. blockchain analytic tools[135]) that enable the tracking of virtual assets and the associated wallet addresses and identification of potentially suspicious transactions.
	12.7.4	Where an FI employs a technological solution provided by an external party to conduct screening of virtual asset transactions and the associated wallet addresses, the FI remains responsible for discharging its AML/CFT obligations. The FI should conduct due diligence on the solution before deploying ~~the solution~~it, taking into account relevant factors such as: (a) the quality and effectiveness of the tracking and detection tools; (b) the coverage, accuracy and reliability of the information maintained in the database that supports its screening capability (e.g. whether the list of wallet addresses that are directly and/or indirectly associated with illicit or suspicious activities/sources, or designated parties, is subject to timely review and update); and (c) any limitations (e.g. limited reach of the blockchain analytical tools; ~~and~~or inability to

[134] Illicit activities include, for example, ransomware, fraud, identity theft, phishing, and other cybercrimes; and suspicious activities/sources include, for example, darknet marketplaces, online gambling services, peel chains and use of anonymity-enhancing technologies or mechanisms (e.g. mixers, tumblers, privacy wallets). In addition, any wallet addresses owned or controlled by customer(s) with which the FI has decided not to establish or continue business relationships due to suspicion of ML/TF should be included as those associated with suspicious sources. Please refer to the meaning of peel chains and mixers and tumblers set out in paragraph 12.1.~~87~~.

[135] Blockchain analytic tools typically enable their users to trace the on-chain history of specific virtual assets. These tools support a number of common virtual assets and compare transaction histories against a database of wallet addresses connected to illicit or suspicious activities/sources, and flag identified transactions.

		deal with virtual assets or wallet addresses involving the use of anonymity-enhancing technologies or mechanisms such as anonymity-enhanced virtual assets, mixers or tumblers).
	12.7.5	An FI should (where applicable) monitor the additional customer information (i.e. IP addresses with associated time stamps, geo-location data, and device identifiers) referred to in paragraph 12.4.1 obtained by the FI on an ongoing basis[136] to identify suspicious transactions and activities as well as takeing appropriate follow-up actions.
	12.7.6	The FI should also put in place policies and procedures to identify and analyse any additional red flags of suspicious transactions and activities in connection with the screening of virtual asset transactions and the associated wallet addresses as well as the ongoing monitoring of additional customer information, having regard to the list of illustrative indicators of suspicious transactions and activities set out in paragraphs 12.16 and Appendix B, which should prompt further investigations (see paragraph 7.12); and take appropriate steps such as making appropriate enquiries with customers to identify if there are any grounds for suspicion (see paragraphs 5.13 to 5.17)[137]. Furthermore, where the FI becomes aware of any heightened ML/TF risks from the screening of virtual asset transactions and the associated wallet addresses or the ongoing monitoring of additional customer information, the FI should apply enhanced customer due diligence and ongoing monitoring, and take other additional preventive or

[136] For example, an FI may adopt technological solution(s) that enables it to track and monitor the additional customer information on an ongoing basis.

[137] When an FI evaluates a potentially suspicious transaction identified from the screening of virtual asset transactions and the associated wallet addresses, it may take into account the required originator and recipient information, as well as other customer information, transaction history, and any additional information that the FI obtained from the customer.

		mitigating actions as necessary to mitigate the ML/TF risks involved[138].
12.8 Terrorist financing, financial sanctions and proliferation financing – Database maintenance, screening and enhanced checking		
	12.8.1	In implementing an effective screening mechanism pursuant to paragraph 6.16, an FI's screening mechanism should also include screening all relevant parties in a virtual asset transfer (referred to in paragraphs 12.11.53 to 12.11.243 and 12.14), including: (a) the recipient if the FI acts as the ordering institution or the virtual asset is transferred to an unhosted wallet; (b) the originator if the FI acts as the beneficiary institution or the virtual asset is transferred from an unhosted wallet; or (c) both the originator and recipient if the FI acts as the intermediary institution, against current database before executing the virtual asset transfer.
	12.8.2	For the screening requirement set out in paragraph 12.8.1, an FI should screen the required originator and recipient information[139] referred to in: (a) paragraph 12.11.5 or 12.11.6 in relation to a virtual asset transfer (including information which may be held separately to the virtual

[138] For example, where a customer enters the FI's platform from and/or initiates transactions with a masked IP address, the FI may request the customer to unmask the IP address and, where necessary, the FI may decline to provide services to that customer if the IP address remains masked.

[139] An FI should include the names of relevant parties in the screening, and should take into consideration the address, identification document number or date and place of birth of the originator (where applicable) in the screening. In addition, the FI should observe the requirements ~~on~~for ongoing monitoring of virtual asset transactions and the associated wallet addresses in paragraphs 12.7.2 to 12.7.4 and 12.7.6 when carrying out virtual asset transfers on behalf of its customers.

		asset transfer itself); or (b) paragraph 12.14.2 in relation to a virtual asset transfer to or from an unhosted wallet.
	12.8.3	Where an incoming virtual asset transfer ~~can be completed prior to or~~is conducted without the said screening or when any of the required originator and recipient information in relation to an incoming virtual asset transfer is missing (which renders the FI unable to conduct screening), the FI should take appropriate risk mitigating measures, having regard to its business practices[140]. The risk mitigating measures taken by the FI should be documented.
12.9 Record-keeping – Retention of records relating to CDD and transactions		
s.20(3A), Sch. 2	12.9.1	In addition to the documents and records required to be kept and the period of time such documents and records are required to be kept pursuant to paragraphs 8.3 and 8.4, for an occasional transaction that is a virtual asset transfer involving virtual assets that amount to no less than $8,000, an FI should keep all documents and records mentioned in paragraph 8.3 for a period of at least five years beginning on the date on which the occasional transaction is completed.
~~s.20(3A), Sch. 2~~	12.9.2	~~In addition to the documents and records required to be kept pursuant to paragraphs 8.3, 8.4 and 12.9.1, for an occasional transaction that involves an amount equal to or above $8,000 or an equivalent amount in any other currency and is not a wire transfer or a virtual asset transfer, an FI that is an SFC-licensed VAS Provider should keep all documents and records mentioned in paragraph~~

[140] ~~For example,~~These may include implementing controls to prevent the relevant virtual assets from being made available to the recipient, or putting the receiving wallet on hold, until the screening is completed and confirmed that no concern is raised. Please also refer to risk mitigating measures in paragraph 12.11.22.

		~~8.3 for a period of at least five years beginning on the date on which the occasional transaction is completed.~~
s.20(1)(a), Sch. 2	12.9.2 ~~12.9.3~~	In addition to the documents and records required to be kept and the period of time such documents and records are required to be kept pursuant to paragraphs 8.5 and 8.6, ~~A~~an FI should keep the required originator and recipient information set out in paragraphs 12.11.5 and 12.11.6 obtained or received by the FI in relation to a virtual asset transfer referred to in paragraphs 12.11.5 to 12.11.2~~43~~, and/or the required originator and recipient information set out in paragraph 12.14.2 obtained by the FI in relation to a virtual asset transfer to or from an unhosted wallet referred to in paragraphs 12.14, for a period of at least five years after the completion of the transfer, regardless of whether the business relationship ends during the period.
12.10 Third-party deposits and payments		
General		
	12.10.1	For the purposes of Chapter 11, paragraphs 5.18 to 5.20 and 12.10, unless otherwise specified, when an FI handles deposits and payments in the form of virtual assets on behalf of its customer, the term “third-party deposits or payments” covers both third-party deposits or payments in the form of funds (i.e. fiat currency) and virtual assets.
	12.10.2	Where a customer uses a third party to make or receive payments in the form of virtual assets to or from an FI, there is a risk that the arrangement may be used to disguise the true beneficial owner or the source of funds. There are increased risks that these transactions are linked to predicate offences (such as online scams, ransomware and other cybercrimes, insider dealing and market manipulation), or used to launder illicit proceeds obtained elsewhere.

Policies and procedures		
	12.10.3	In relation to the policies and procedures for the acceptance of third-party deposits and payments as required under paragraph 11.3, the policies and procedures of an FI should also address the monitoring systems and controls for identifying transactions involving third-party deposits or payments in the form of virtual assets[141] (please refer to paragraph 12.10.6).
	12.10.4	In relation to the guidance in paragraph 11.3(d) requiring FIs to have policies and procedures for the exceptional situations under which delayed due diligence or evaluation may be allowed, it should be noted that delayed due diligence on the source of a deposit or evaluation of a third-party deposit does not apply to a deposit in the form of virtual assets considering the nature and ~~heightened~~ ML/TF risks associated with virtual assets.
	12.10.5	To facilitate the prompt identification of the sources of deposits in the form of virtual assets, FIs are strongly encouraged to whitelist accounts (or wallet addresses as appropriate[142]) owned or controlled by their clients or any acceptable third parties for the making of all such deposits. This will make it easier for FIs to ascertain whether the deposits have originated from their clients or any acceptable third parties[143].

[141] Unlike payments in the form of funds which are usually made to bank accounts designated in the name of a payee which can be easily identified by an FI before making payments, payments in the form of virtual assets are usually made to wallet addresses which are not designated in the name of a payee. Hence, an FI should put in place monitoring systems and controls for identifying transactions involving a third party for both deposits and payments in the form of virtual assets (e.g. by ascertaining the ownership or control of the account or wallet address).

[142] When whitelisting accounts (or wallet addresses as appropriate) owned or controlled by its clients or any acceptable third parties, an FI should only accept wallet addresses that the FI has assessed to be reliable and have regard to the relevant requirements set out in paragraphs 12.10.6, 12.10.7 and 12.14.3(b).

[143] Likewise, if applicable, the use of whitelisted accounts (or wallet addresses as appropriate) owned or controlled by any acceptable third parties for the making of withdrawals will make it easier for FIs to complete the necessary due diligence to determine the acceptability of a third-party payee before effecting a third-party payment.

	12.10.6	For deposits and payments in the form of virtual assets, the nature and extent of monitoring systems and controls set out in paragraph 12.10.3 should be commensurate with the channel of deposits or payments (i.e. whether the deposits or payments were made via a VA transfer counterparty (referred to in paragraphs 12.13) or an unhosted wallet (referred to in paragraphs 12.14)), having regard to the associated ML/TF risks[144]. For a virtual asset deposit or payment made via an ordering or beneficiary institution that presents low ML/TF risk, the required originator or recipient information verified by the ordering or beneficiary institution may be sufficient for an FI to ascertain whether the transaction involves a third party[145]. Conversely, where a virtual asset deposit or payment is made via an ordering or beneficiary institution that presents higher ML/TF risk or an unhosted wallet, the FI should ascertain the customer's ownership or control of the account (or wallet address as appropriate) maintained with the ordering or beneficiary institution, or the unhosted wallet, by taking appropriate measures, for example: (a) using appropriate confirmation methods[146]; and (b) obtaining evidence from the customer such as statement of account issued by the VA transfer counterparty.
Due diligence process for assessing third-party deposits and payments		
	12.10.7	In addition to the due diligence process set out in paragraphs 11.5 to 11.8, an FI should take

[144] Where applicable, an FI should have regard to the results of the counterparty due diligence as set out in paragraphs 12.13.

[145] In other words, this means that whether the originator and the recipient are the same person.

[146] Examples of confirmation methods may include requesting the customer to perform the micropayment test (i.e. by effecting a virtual asset transfer with an (typically small) amount specified by the FI) or message signing test (i.e. by signing a message specified by the FI which is then verified by the FI).

		reasonable measures on a risk-sensitive basis to ascertain the third party's ownership of the account (or wallet address as appropriate). For a virtual asset deposit or payment made via an ordering or beneficiary institution that presents low ML/TF risk, it may be sufficient for an FI to rely on the required originator or recipient information verified by the ordering or beneficiary institution for ascertaining the third party's ownership of the account. Conversely, where a virtual asset deposit or payment is made via an ordering or beneficiary institution that presents higher ML/TF risk or an unhosted wallet, the FI should use its best endeavours to ascertain the third party's ownership or control of the account (or wallet address as appropriate) maintained with the ordering or beneficiary institution, or the unhosted wallet, by taking appropriate measures which may include the examples mentioned in paragraph 12.10.6.
12.11 Virtual asset transfers		
General		
	12.11.1	An FI should comply with section 13A of Schedule 2, the guidance and requirements set out in paragraphs 12.11 to 12.14 as well as (where applicable) relevant circulars and frequently asked questions published by the SFC from time to time when acting as an ordering institution, an intermediary institution or a beneficiary institution as defined in paragraph 12.11.4 in a virtual asset transfer, and/or when conducting virtual asset transfers to or from an unhosted wallet[147]. For the avoidance of doubt, where an FI is the originator or recipient of a virtual asset transfer, it is not acting as an ordering institution, an intermediary institution or a beneficiary institution and is thus not required to comply with the requirements under section 13A of Schedule 2 and

[147] Refer to paragraph 12.1.98 for the meaning of "unhosted wallets".

		paragraphs 12.11.5 to 12.11.243, 12.12 and 12.13 in respect of that transaction.
~~s.13A, s.19(3), s.23(a) & (b), Sch. 2~~	12.11.2	To prevent criminals and terrorists from having unfettered ~~access~~opportunities to move their assets through virtual asset transfers ~~for moving their assets~~ and ~~for~~to detecting such misuse when it occurs, an FI must take all reasonable measures to ensure that proper safeguards exist to mitigate the ML/TF risks associated with virtual asset transfers. In particular, an FI should establish and maintain effective procedures to ensure compliance with: (a) the virtual asset transfers requirements under paragraphs 12.11.5 to 12.11.243 (a.k.a. travel rule[148]); and (b) other relevant requirements under paragraphs 12.12 to 12.14, to enable it to carry out sanctions screening and transaction monitoring procedures on all relevant parties involved in a virtual asset transfer in an effective manner.
Virtual asset transfers to or from an institution		
	12.11.3	Paragraphs 12.11.5 to 12.11.243, 12.12 and 12.13 apply to virtual asset transfers to or from an institution, including an institution that is a VASP or financial institution (referred to in paragraph 12.6.1) located in a place within or outside Hong Kong. Requirements that apply to virtual asset transfers to or from unhosted wallets are set out in paragraphs 12.14.

[148] The ~~T~~travel rule refers to the application of the wire transfer requirements set out in FATF Recommendation 16 in a modified form in the context of virtual asset transfers (in particular, the requirements to obtain, hold, and submit required and accurate originator and required recipient information immediately and securely when conducting virtual asset transfers), recognising the unique technological properties of virtual assets.

s.13A(1) & (8), Sch. 2	12.11.4	Section 13A of Schedule 2, paragraphs 12.11.5 to 12.11.243, 12.12 and 12.13 apply to a virtual asset transfer that is a transaction carried out: (a) by an institution (the ordering institution) on behalf of a person (the originator) by transferring any virtual assets; and (b) with a view to making the virtual assets available: (i) to that person or another person (the recipient); and (ii) 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 virtual assets. An FI should comply with the corresponding requirements set out in paragraphs 12.11.5 to 12.11.243 when acting as an ordering institution, an intermediary institution or a beneficiary institution (as the case may be) in a virtual asset transfer.
Ordering institutions		
s.13A(2), Sch.2	12.11.5	Before carrying out a virtual asset transfer involving virtual assets that amount to not less than $8,000, an ordering institution must obtain and record the following originator and recipient information[149]: (a) the originator's name; (b) the number of the originator's account maintained with the ordering institution and

[149] For the avoidance of doubt, in relation to virtual asset transfers carried out for a customer, an FI is not required to obtain the originator information from a customer that is the originator before carrying out every individual virtual asset transfer (unless doubts arise as to veracity or adequacy of the ~~evidence~~information previously obtained for the purposes of ~~CDD~~customer identification and verification).

		from which the virtual assets are transferred (i.e. the account used to process the transaction) or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the ordering institution; (c) the originator's address [150], the originator's customer identification number [151] 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 virtual assets are transferred (i.e. the account used to process the transaction) or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the beneficiary institution.
s.13A(2) & (3), Sch.2	12.11.6	Before carrying out a virtual asset transfer involving virtual assets that amount to less than $8,000, an ordering institution must obtain and record 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 virtual assets are transferred or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the ordering institution;

[150] The originator's address refers to the geographical address of the originator (i.e. residential address of the originator that is a natural person; or the address of registered office (or principal place of business if different from the registered office) of the originator that is a legal person, a trust or other similar legal arrangement).

[151] Customer identification number means a number which uniquely identifies the originator to the ~~originating~~ordering institution and is a different number from the unique transaction reference number referred to in paragraph 12.11.8. The customer identification number must refer to a record held by the ordering institution which contains at least one of the following: the customer's address, identification document number, or date and place of birth.

		(c) the recipient's name; and (d) the number of the recipient's account maintained with the beneficiary institution and to which the virtual assets are transferred or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the beneficiary institution.
	12.11.7	Where applicable, the number of the account maintained with the ordering institution or beneficiary institution from or to which the virtual assets are transferred referred to in paragraphs 12.11.5 and 12.11.6 could mean the wallet address of the originator or recipient maintained with the ordering institution or beneficiary institution and used to process the transaction.
	12.11.8	The unique reference number assigned to the virtual asset transfer by the ordering institution or beneficiary institution referred to in paragraphs 12.11.5 and 12.11.6 should permit traceability of the virtual asset transfer.
s.13A(4), Sch.2	12.11.9	An ordering institution must submit~~:~~ the required originator and recipient information obtained and held under paragraphs 12.11.5 and 12.11.6 (hereafter referred to as "required information") ~~the information obtained and held under paragraph 12.11.5 in relation to a virtual asset transfer involving virtual assets that amount to not less than $8,000; or~~ ~~the information obtained and held under paragraph 12.11.6 in relation to a virtual asset transfer involving virtual assets that amount to less than $8,000,~~ to the beneficiary institution ~~immediately (see paragraph 12.11.11) and~~ securely (see paragraph 12.11.12).
s.13A(4), Sch.2	12.11.10	In addition, the ordering institution must submit the required information to the beneficiary institution

		immediately (see paragraph 12.11.13).
	12.11.11 12.11.10	For the avoidance of doubt, the ~~required originator and recipient information referred to in paragraphs 12.11.5 and 12.11.6 (hereafter referred to as "~~required information~~")~~ may be submitted either directly or indirectly to the beneficiary institution provided that it is submitted ~~immediately and securely~~in accordance with the requirements set out in paragraphs 12.11.9 and 12.11.10. This means that it is not necessary for the required information to be attached directly to, or be included in, the virtual asset transfer itself.
	~~12.11.11~~	~~"Immediately" referred to in paragraph 12.11.9 means that the ordering institution should submit the required information prior to, or simultaneously or concurrently with, the virtual asset transfer (i.e. the submission must occur before or when the virtual asset transfer is conducted)[152].~~
	12.11.12	"Securely" referred to in paragraph 12.11.9 means that the ordering institution should store and submit the required information in a secure manner to protect the integrity and availability of the required information for facilitating record-keeping and the use of such information by the beneficiary institution and, where applicable, the intermediary institution, in fulfilling its AML/CFT obligations[153]; and protect the information from unauthorised access or disclosure.

~~[152] Where an intermediary institution is involved in a virtual asset transfer, an ordering institution should undertake the VA transfer counterparty due diligence measures as set out in paragraphs 12.13 to determine if the intermediary institution can submit the required information immediately to the beneficiary institution, or where applicable, another intermediary institution and should not execute the virtual asset transfer otherwise.~~

[153] AML/CFT obligations include, among others, identifying and reporting suspicious virtual asset transfers, ~~and~~ taking freezing actions and prohibiting virtual asset transfers with designated persons and entities.

		To ensure that the required information is submitted in a secure manner, an ordering institution should[154]: (a) undertake the VA transfer counterparty due diligence measures as set out in paragraphs 12.13 to determine whether the beneficiary institution and, where applicable, the intermediary institution can reasonably be expected to adequately protect the confidentiality and integrity of the information submitted to it; and (b) take other appropriate measures and controls, for example: (i) entering into a bilateral data sharing agreement with the beneficiary institution and, where applicable, the intermediary institution and/or (where applicable) a service-level agreement with the technological solution provider for travel rule compliance (see paragraphs 12.12) which specifies the responsibilities of the institutions involved and/or of the provider to ensure the protection of the confidentiality and integrity of the information submitted; (ii) using, or ensuring the technological solution adopted for travel rule compliance (where applicable) uses, a strong encryption algorithm to encrypt the information during the data submission; and (iii) implementing adequate information security controls to prevent unauthorised access, disclosure or alteration. For the avoidance of doubt, an ordering institution should not execute a virtual asset transfer when it could not ensure that the required information

[154] An ordering institution should give due regard to the laws and regulations on privacy and data protection of the jurisdictions in which the ordering institution operates and/or is incorporated.

		could be submitted to a beneficiary institution, and where applicable, an intermediary institution, in a secure manner having regard to the above guidance and the VA transfer counterparty due diligence results.
	12.11.13 ~~12.11.11~~	"Immediately" referred to in paragraph 12.11.10~~9~~ means that the ordering institution should submit the required information prior to, or simultaneously or concurrently with, the virtual asset transfer (i.e. the submission must occur before or when the virtual asset transfer is conducted)[155].
	12.11.14 ~~12.11.13~~	An ordering institution should keep records and relevant documents so that it can demonstrate to the relevant authority whether and how the required information is submitted to a beneficiary institution ~~immediately and securely~~in accordance with the requirements set out in paragraphs 12.11.9 and 12.11.10[156].
	12.11.15 ~~12.11.14~~	For a virtual asset transfer involving virtual assets that amount to not less than $8,000, an ordering institution must ensure that the required originator information submitted with the virtual asset transfer is accurate[157].

[155] Where an intermediary institution is involved in a virtual asset transfer, an ordering institution should undertake the VA transfer counterparty due diligence measures as set out in paragraphs 12.13 to determine if the intermediary institution can submit the required information immediately to the beneficiary institution, or where applicable, another intermediary institution and should not execute the virtual asset transfer ~~otherwise~~ if the intermediary institution is unable to do so.

[156] For the avoidance of doubt, where technological solution is adopted for travel rule compliance, the ordering institution should keep any records or relevant documents of its due diligence on the technological solution. Please also refer to the guidance provided in paragraphs 12.12. In addition, where an intermediary institution is involved in a virtual asset transfer, the ordering institution should keep records and relevant documents that demonstrate whether and how the required information is submitted to the beneficiary institution ~~immediately and securely~~ through the intermediary institution in accordance with the requirements set out in paragraphs 12.11.9 and 12.11.10.

[157] "Accurate" in this context means information that has been verified for accuracy as part of its CDD process. For example, if the originator's address is part of the required information to be submitted by the ordering institution as set out in paragraphs 12.11.9 and 12.11.10, the ordering institution should ensure that the originator's address is accurate having regard to the CDD information obtained pursuant to paragraph 4.2.4, 4.2.5 or 4.2.10 as appropriate.

s.3(1)(d) & (1A), Sch.2	12.11.16 ~~12.11.15~~	For an occasional virtual asset transfer[158] involving virtual assets that amount to not less than $8,000, an ordering institution must verify the identity of the originator[159]. For an occasional virtual asset transfer involving virtual assets that amount to less than $8,000, 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 amount to not less than $8,000, or when there is a suspicion of ML/TF.
	12.11.17 ~~12.11.16~~	The ordering institution should not execute a virtual asset transfer unless it has ensured compliance with the requirements in paragraphs 12.11.5 to 12.11.16~~5~~.
Intermediary institutions		
s.13A(6), Sch.2	12.11.18 ~~12.11.17~~	An intermediary institution must ensure that all originator and recipient information as set out in paragraphs 12.11.5 and 12.11.6 which the intermediary institution receives in connection with the virtual asset transfer is retained with the required information submission, and is transmitted to the institution to which it passes on the transfer instruction[160].
	12.11.19 ~~12.11.18~~	As with the submission of required information by an ordering institution, an intermediary institution should transmit the aforesaid information to another intermediary institution or the beneficiary institution ~~immediately and securely,~~ in accordance with the ~~requirements~~manner set out in paragraphs

[158] It should be noted that ~~occasional virtual asset transfers do not apply to~~ FIs that are LCs or SFC-licensed VAS Providers should not carry out occasional virtual asset transfers.

[159] For the avoidance of doubt, where the originator is a customer of an FI, the FI does not need to re-verify the identity of the customer that has been verified (unless doubts arise as to veracity or adequacy of the ~~evidence~~information previously obtained for the purposes of customer identification~~y~~ and verification).

[160] An intermediary institution should undertake the VA transfer counterparty due diligence measures on the ordering institution and, where applicable, another intermediary institution(s), as set out in paragraphs 12.13.

		12.11.121 to 12.11.13 and the requirement set out in paragraph 12.11.14[161].
Beneficiary institutions		
s.13A(5), Sch.2	12.11.20 12.11.19	A beneficiary institution must obtain and record the required information submitted to it by the institution from which it receives the transfer instruction[162].
s.3(1A), Sch. 2	12.11.21 12.11.20	For a virtual asset transfer involving virtual assets that amount to not less than $8,000, a beneficiary institution should verify the identity of the recipient if the identity has not been previously verified as part of its CDD process. The beneficiary institution should also confirm whether the recipient's name and account number obtained from the institution from which it receives the transfer instruction match with the recipient information verified by it, and take reasonable measures as set out in paragraph 12.11.243 where such information does not match.
Identification and handling of incoming virtual asset transfers lacking the required information		
s.19(2A), Sch.2	12.11.22 12.11.21	A beneficiary institution or an intermediary institution (hereafter referred to as "instructed institution") must establish and maintain effective procedures for identifying and handling incoming virtual asset transfers that do not comply with the relevant requirements on required originator or recipient information, which include: (a) taking reasonable measures (e.g. real-time or post-event monitoring) to identify virtual asset

[161] For the purpose of paragraph 12.11.198, any reference to "ordering institution" and "the intermediary institution" in paragraphs 12.11.121 to 12.11.143 refers to "intermediary institution" and "another intermediary institution" respectively.

[162] A beneficiary institution should undertake the VA transfer counterparty due diligence measures on the ordering institution and, where applicable, the intermediary institution(s), as set out in paragraphs 12.13.

		transfers that lack the required information; and (b) having risk-based policies and procedures for determining: (i) whether and when to execute, suspend (i.e. prevent the relevant virtual assets from being made available to the recipient) a virtual asset transfer lacking the required information~~, and/~~ or, where appropriate, return the relevant virtual assets to the ~~originator's~~ account of the ordering institution or another intermediary institution (hereafter referred to as "instructing institution") from which the instructed institution receives the transfer instruction[163]; and (ii) the appropriate follow-up action.
s.13A(7)(a), Sch.2	12.11.23 ~~12.11.22~~	In respect of the risk-based policies and procedures referred to in paragraph 12.11.2~~2~~1, if an ~~ordering institution or another intermediary institution (hereafter referred to as "~~instructing institution~~") from which an instructed institution receives the transfer instruction~~ does not submit all of the required information in connection with the virtual asset transferred to the instructed institution, the instructed institution must as soon as reasonably practicable obtain the missing information from the instructing institution. If the missing information cannot be obtained, the instructed institution should either consider restricting or terminating its business relationship with the instructing institution in relation to virtual asset transfers, or take reasonable measures to mitigate the risk of ML/TF involved.

[163] An instructed institution should consider preventing the relevant virtual assets from being made available to the recipient until the missing information is obtained~~, and/~~ or, where appropriate, returning the relevant virtual assets to the ~~originator's~~ account of the instructing institution when there is no suspicion of ML/TF, ~~unless it is satisfied with the reasons for executing the virtual asset transfer that lacks the required information.~~ taking into account the results of the VA transfer counterparty due diligence (see paragraphs 12.13) and screening of the virtual asset transactions and the associated wallet addresses in relation to the virtual asset transfers (see paragraphs 12.7.2 to 12.7.4 and 12.7.6). Please also refer to risk mitigating measures in paragraph 12.8.3.

s.13A(7)(b), Sch.2	12.11.24 ~~12.11.23~~	If the instructed institution is aware that any of the information submitted to it that purports to be the required information is incomplete or meaningless, it must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved having regard to the procedures set out in paragraph 12.11.2~~21~~(b).
12.12 Virtual asset transfers – Technological solutions for travel rule compliance		
	12.12.1	An FI may adopt any technological solution to submit and/or obtain the required information ~~in~~for a virtual asset transfer provided that the solution enables the FI to comply with the travel rule as set out in paragraphs 12.11.5 to 12.11.2~~43~~, when it acts as an ordering institution, an intermediary institution or a beneficiary institution.
	12.12.2	Where an FI chooses to use a technological solution ~~for~~to ensur~~eing~~ travel rule compliance ~~(hereafter referred to as "solution")~~, ~~the FI~~it remains responsible for discharging its AML/CFT obligations in relation to travel rule compliance. The FI should conduct due diligence ~~on the solution~~ to satisfy itself that the solution enables it to comply with the travel rule in an effective and efficient manner. In particular, the FI should consider whether the solution enables it to: (a) identify VA transfer counterparties (see paragraphs 12.13); and (b) submit the required information immediately (see paragraph 12.11.1~~1~~) and securely (see paragraph 12.11.12) (i.e. whether the solution could protect the submitted information from

		unauthorised access, disclosure or alteration), and obtain the required information[164].
	12.12.3	In addition, an FI should consider a range of factors as ~~part of the~~appropriate when conducting due diligence on the technological solution for travel rule compliance, such as: (a) the interoperability of the solution with other similar solution(s) adopted by the VA transfer counterparties that the FI may deal with; (b) whether the solution allows the required information for a large volume of virtual asset transfers to be submitted ~~could submit~~ immediately and securely~~,~~ to and/or obtained~~, the required information to and~~ from multiple VA transfer counterparties ~~for a large volume of virtual asset transfers~~ in a stable manner; (c) whether the solution enables the FI to implement measures or controls for the effective scrutiny of virtual asset transfers to identify and report suspicious transactions (as set out in paragraphs 12.7.2 to 12.7.4 and 12.7.6), and screening of virtual asset transfers to meet the sanctions obligations (i.e. taking freezing actions and prohibiting virtual asset transfers with designated persons and entities) (as set out in paragraphs 12.8.1 to 12.8.3); ~~and~~ (d) whether the solution facilitates the FI in conducting VA transfer counterparty due diligence (see paragraphs 12.13) and requesting ~~for~~ additional information from the VA transfer counterparty as and when necessary~~.~~; and (e) whether the solution facilitates the FI in keeping the required information (see paragraph 12.9.2).

[164] In considering whether the solution enables the FI to obtain the required information, the FI should take into account whether ~~the solution~~it could identify situations where the required information provided by ordering institutions is incomplete or missing, which may ~~arise~~result from ~~nuances~~slight differences in travel rule requirements across the laws, rules and regulations of ~~relevant~~other jurisdictions, before conducting virtual asset transfers.

12.13 VA transfer counterparty due diligence and additional measures		
Introduction		
	12.13.1	When an FI conducts a virtual asset transfer referred to in paragraphs 12.11.5 to 12.11.243, the FI will be exposed to ML/TF risks associated with the institution which may be the ordering institution, intermediary institution or beneficiary institution involved in the virtual asset transfer (hereafter collectively referred to as "VA transfer counterparty"), which may vary depending on a number of factors, including: (a) the types of products and services offered by the VA transfer counterparty; (b) the types of customers to which the VA transfer counterparty provides services; (c) geographical exposures of the VA transfer counterparty and its customers; (d) the AML/CFT regime in the jurisdictions in which the VA transfer counterparty operates and/or is incorporated; and (e) the adequacy and effectiveness of the AML/CFT controls of the VA transfer counterparty.
	12.13.2	To avoid sending or receiving virtual assets to or from illicit actors or designated parties that had not been subject to the appropriate CDD and screening measures ~~of~~undertaken by a VA transfer counterparty and to ensure compliance with the travel rule, an FI should conduct due diligence on the VA transfer counterparty to identify and assess the ML/TF risks associated with the virtual asset transfers to or from the VA transfer counterparty and apply appropriate risk-based AML/CFT measures.
VA transfer counterparty due diligence measures		
	12.13.3	An FI should conduct due diligence measures on a VA transfer counterparty before conducting a

		virtual asset transfer, or making the transferred virtual assets available to the recipient. If an FI conducts virtual asset transfers with several VA transfer counterparties located in different jurisdictions but belonging to the same group, the FI, whilst conducting due diligence on each of the VA transfer counterparties independently, should also take into account that these counterparties belong to the same group in order to holistically assess the ML/TF risks posed by the counterparties.
	12.13.4	An FI does not need to undertake the VA transfer counterparty due diligence process for every individual virtual asset transfer when dealing with VA transfer counterparties that it has alreadypreviously conducted counterparty due diligence on previously, unless when there is a suspicion of ML/TF or when the FI is aware of any heightened ML/TF risks from its ongoing monitoring of virtual asset transfers with VA transfer counterparties (see paragraph 12.13.10).
	12.13.5	An FI should undertake reviews of VA transfer counterparty due diligence records on a regular basis or upon trigger events (e.g. when it becomes aware of a suspicious transaction or other information such as negative news from credible media, public information that the counterparty has been subject to any targeted financial sanction, ML/TF investigation or regulatory action). Based on the VA transfer counterparty due diligence results, the FI should determine if it should continue to conduct virtual asset transfers with, and submit the required information to, a VA transfer counterparty, and the extent of AML/CFT measures that it should apply in relation to virtual

		~~asset transfers with the VA transfer counterparty on a risk-sensitive basis[165].~~
	12.13.5 ~~12.13.6~~	VA transfer counterparty due diligence typically involves the following procedures: (a) determining whether the virtual asset transfer is or will be with a VA transfer counterparty or an unhosted wallet; (b) where applicable, identifying the VA transfer counterparty (e.g. by making reference to lists of licensed or registered VASPs or financial institutions in different jurisdictions); and (c) assessing whether the VA transfer counterparty is an eligible counterparty to deal with and to send the required information to (see paragraphs 12.13.67 to 12.13.910).
	12.13.6 ~~12.13.7~~	An FI should adopt an RBA in applying the following ~~VA transfer counterparty~~ due diligence measures on ~~before it conducts a virtual asset transfer with~~ a VA transfer counterparty, taking into account relevant factors such as those set out in paragraph 12.13.1: (a) collect sufficient information about the VA transfer counterparty to enable it to understand fully the nature of the VA transfer counterparty's business[166]; (b) understand the nature[167] and expected volume and value of virtual asset transfers with the VA transfer counterparty;

~~[165] Further guidance on risk mitigating measures is set out in paragraphs 12.13.11 to 12.13.13.~~

[166] While an FI should determine on a risk-sensitive basis the amount of information to collect about the VA transfer counterparty to enable it to understand the nature of the VA transfer counterparty's business, the FI should, among other things, endeavour to identify and verify the identity of the VA transfer counterparty using ~~reliable and independent source~~ documents, data or information provided by a reliable and independent source; and take reasonable measures to understand the ownership and control structure of the VA transfer counterparty, with the objective to follow the chain of ownerships to its beneficial owners.

[167] For example, the extent to which any of the virtual asset transfers and relevant underlying customers (who may be the originator or recipient of a virtual asset transfer) are assessed as high risk by the VA transfer counterparty.

		(c) determine from publicly available information the reputation of the VA transfer counterparty and the quality and effectiveness of the AML/CFT regulation and supervision over the VA transfer counterparty by authorities in the jurisdictions in which it operates and/or is incorporated which perform functions similar to those of the RAs; (d) assess the AML/CFT controls of the VA transfer counterparty and be satisfied that the AML/CFT controls of the VA transfer counterparty are adequate and effective; and (e) obtain approval from its senior management.
	12.13.7 ~~12.13.8~~	While a relationship with a VA transfer counterparty is different from a cross-border correspondent relationship referred to in paragraph 12.6.1, there are similarities in the due diligence approach which can be of assistance to an FI. By virtue of this, the FI should conduct the due diligence measures in paragraph 12.13.6~~7~~, with reference to the requirements set out in paragraphs 4.20.7 to 4.20.10 and 12.6.3 to 12.6.4[168].
	12.13.8 ~~12.13.9~~	As part of the VA transfer counterparty due diligence measures in relation to its AML/CFT controls, an FI should assess whether the VA transfer counterparty can comply with the travel rule, taking into account relevant factors such as: (a) whether the VA transfer counterparty is subject to requirements similar to the travel rule ~~similar to that~~ imposed under section 13A of Schedule 2 and this Chapter in the jurisdictions in which the VA transfer counterparty operates and/or is incorporated; and (b) the adequacy and effectiveness of the

[168] For the purposes of paragraph 12.13.7~~8~~, any reference to "cross-border correspondent relationship" and "respondent institution" in paragraphs 4.20.7 to 4.20.10 and 12.6.3 to 12.6.4 refers to "VA transfer counterparty relationship" and "VA transfer counterparty" respectively.

		AML/CFT controls that the VA transfer counterparty has put in place for ensuring compliance with the travel rule. In addition, the FI should assess whether the VA transfer counterparty can protect the confidentiality and integrity of personal data (e.g. the required originator and recipient information), taking into account the adequacy and robustness of data privacy and security controls of the VA transfer counterparty[169].
	12.13.9 ~~12.13.10~~	When assessing the ML/TF risks posed by a VA transfer counterparty, an FI should take into account relevant factors that may indicate a higher ML/TF risk, for example, a VA transfer counterparty that: (a) operates or is incorporated in a jurisdiction posing a higher risk or with a weak AML/CFT regime; (b) is not (or is yet to be) licensed or registered and supervised for AML/CFT purposes in the jurisdictions in which it operates and/or is incorporated by authorities which perform functions similar to those of the RAs; (c) does not have in place adequate and effective AML/CFT Systems, including measures for ensuring compliance with the travel rule; (d) does not implement adequate measures or safeguards for protecting the confidentiality and integrity of personal data; or (e) is associated with ML/TF or other illicit activities.
Ongoing monitoring		
	12.13.10	An FI should monitor the VA transfer counterparties on an ongoing basis, including:

[169] This is to ensure that, among other things, the required information is submitted in a secure manner as mentioned in paragraph 12.11.12.

		(a) adopting an RBA in monitoring virtual asset transfers with VA transfer counterparties with a view to detecting any unexpected or unusual activities or transactions and any changes in the risk profiles of the VA transfer counterparties, taking into account the transaction monitoring requirements in Chapter 5 and paragraphs 12.7.2 to 12.7.4 and 12.7.6; and (b) reviewing the information obtained by the FI from applying the VA transfer counterparty due diligence measures under paragraph 12.13.6 on a regular basis and/or upon trigger events (e.g. when the FI is aware of any heightened ML/TF risks from its ongoing monitoring of virtual asset transfers with VA transfer counterparties or other information such as negative news from credible media or public information that the counterparty has been subject to any targeted financial sanction, ML/TF investigation or regulatory action) and, where appropriate, updating its risk assessment of a VA transfer counterparty. Based on the VA transfer counterparty due diligence results, the FI should determine if it should continue to conduct virtual asset transfers with, and submit the required information to, a VA transfer counterparty, and the extent of AML/CFT measures that it should apply in relation to virtual asset transfers with the VA transfer counterparty on a risk-sensitive basis[170].
Other risk mitigating measures		
	12.13.11	An FI should assess how the ML/TF risks identified from the VA transfer counterparty due diligence may affect it, and take reasonable measures on a risk-sensitive basis to mitigate and manage the

[170] Further guidance on risk mitigating measures is set out in paragraphs 12.13.11 to 12.13.13.

		ML/TF risks posed by a VA transfer counterparty[171]. ~~For example, the FI may~~, which include: (a) perform enhanced and/or more frequent due diligence reviews; (b) conduct enhanced monitoring of virtual asset transfers with the VA transfer counterparty; and (c) (where appropriate) impose transaction limits, when dealing with a VA transfer counterparty that presents a higher ML/TF risk.
	12.13.12	An FI should also determine on a risk-sensitive basis whether to restrict or continue to deal with, or ~~reject~~refrain from executing or facilitating any virtual asset transfers to or from ~~or to~~, a VA transfer counterparty that presents higher ML/TF risks. If the FI cannot mitigate and manage the ML/TF risks posed by a VA transfer counterparty, it should refrain from executing or facilitating such virtual asset transfers.
	12.13.13	An FI must not conduct virtual asset transfers with a VA transfer counterparty that is a shell VASP or shell financial institution[172].
12.14 Virtual asset transfers to or from unhosted wallets		
	12.14.1	~~An FI should exercise extra care in respect of the risks posed by virtual asset transfers to or from unhosted wallets [173] and peer~~Peer-to-peer transactions associated with unhosted wallets[174], ~~which~~ may be attractive to illicit actors given the anonymity, and mobility ~~and usability~~ of virtual

[171] In particular, the FI should implement appropriate measures to mitigate and manage the risks posed by virtual asset transfers ~~to~~from or ~~from~~to originators or recipients that are third parties and ensure compliance with the requirements set out in Chapter 11 and paragraphs 12.10.

[172] An FI may refer to the guidance set out in paragraphs 4.20.16 and 12.6.7~~6~~ to determine if the counterparty is a shell VASP or shell financial institution.

~~[173] Refer to paragraph 12.1.8 for the meaning of "unhosted wallets".~~

[174] Refer to paragraph 12.1.9 for the meaning of "unhosted wallets".

		assets and that there is typically no intermediary involved in the peer-to-peer transactions to carry out AML/CFT measures such as CDD and transaction monitoring. An FI should comply with the requirements set out in paragraphs 12.14.2 and 12.14.3 when conducting virtual asset transfers to or from unhosted wallets so as to mitigate the associated ML/TF risks.
	12.14.2	Before an FI sends or receives virtual assets to or from an unhosted wallet on behalf of its customer (i.e. the originator or the recipient, as the case may be), the FI should obtain the following originator and recipient information from the customer[175] and record: (a) in relation to a virtual asset transfer to an unhosted wallet, (i) the originator's name; (ii) the number of the originator's account maintained with the FI and from which the virtual assets are transferred or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the FI; (iii) the originator's address, the originator's customer identification number or identification document number or, if the originator is an individual, the originator's date and place of birth; (iv) the recipient's name; and (v) the recipient's wallet address; (b) in relation to a virtual asset transfer from an unhosted wallet, (i) the originator's name;

[175] For the avoidance of doubt, an FI is not required to obtain the originator information (for a virtual asset transfer to an unhosted wallet) or the recipient information (for a virtual asset transfer from an unhosted wallet) from a customer that is the originator or recipient respectively for every individual virtual asset transfer to or from an unhosted wallet (unless doubts arise as to veracity or adequacy of the ~~evidence~~information previously obtained for the purposes of ~~CDD~~customer identification and verification). For the purposes of paragraph 12.14.2, an FI is not required to obtain the information in (a)(iii) and (b)(iii) set out therein for a virtual asset transfer to or from an unhosted wallet involving virtual assets that amount to less than $8,000.

		(ii) the originator's wallet address; (iii) the originator's address, the originator's customer identification number or identification document number or, if the originator is an individual, the originator's date and place of birth; (iv) the recipient's name; and (v) the number of the recipient's account maintained with the FI and to which the virtual assets are transferred or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the FI.
	12.14.3	An FI should also assess the ML/TF risks associated with virtual asset transfers to or from unhosted wallets and take reasonable measures on a risk-sensitive basis to mitigate and manage the ML/TF risks associated with the transfers[176]. ~~For example, the FI may~~, which include: (a) conduct enhanced monitoring of virtual asset transfers with unhosted wallets; (b) accept virtual asset transfers only to or from ~~or to~~ unhosted wallets that the FI has assessed to be reliable[177], having regard to the screening results of the virtual asset transactions and the associated wallet addresses (see paragraphs 12.7.2 to 12.7.4 and 12.7.6) and the assessment results of~~n~~ the ownership or control of the unhosted wallet [178] (see paragraphs 12.10.6 and 12.10.7); and

[176] In particular, the FI should implement appropriate measures to mitigate and manage the risks posed by virtual asset transfers to or from third parties and ensure compliance with the requirements ~~set out~~ in Chapter 11 and paragraphs 12.10.

[177] For example, an FI may implement controls to prevent the relevant virtual assets from an unhosted wallet being made available to its customer, or putting the transfer to an unhosted wallet on hold, unless the FI is satisfied that the relevant unhosted wallet is reliable.

[178] Where virtual assets are transferred to or from an unhosted wallet that has been whitelisted in accordance with the requirements in paragraph 12.10.5, an FI should ascertain the ownership or control of the unhosted wallet on a periodic and risk-sensitive basis, in particular, where the FI becomes aware of any heightened ML/TF risks from the ongoing monitoring of virtual asset transactions and the associated wallet addresses or additional customer information (see paragraphs 12.7.2 to 12.7.6).

		(c) (where appropriate) impose transaction limits ~~or prohibition~~[179].
12.15 Illustrative risk indicators for assessing ML/TF risks		
	12.15.1	In addition to the non-exhaustive illustrative risk indicators for institutional risk assessment and customer risk assessment set out in Appendix A, paragraphs 12.15 set out non-exhaustive illustrative risk indicators in relation to virtual assets.
Customer risk		
	12.15.2	Examples of customers[180] that may present higher ML/TF risk include: (a) where the origin of wealth is substantially derived from activities that may present higher risks, e.g. initial coin offerings which are known to associate with predicate offences for ML/TF or financial crimes; virtual asset activities conducted via VASPs that are unregulated or with lax AML/CFT controls; (b) a customer who appears to operate as an unregulated VASP on peer-to-peer platforms, particularly when the customer handles or conducts frequent and/or large virtual asset transfers or transactions on behalf of its underlying customer(s), and charges higher service fees ~~as~~ compared to other ~~exchanges~~VASPs; (c) a customer's wallet(s) used for deposit and withdrawal exhibit(s) patterns of virtual asset transactions associated with the use of

[179] For example, an FI may place appropriate limits on the amount of virtual asset transfers with unhosted wallets~~; or implement controls to prevent the relevant virtual assets from an unhosted wallet being made available to its customer, or putting the transfer to an unhosted wallet on hold, unless the FI is satisfied that the relevant unhosted wallet is reliable~~.

[180] These customer risk indicators are also relevant to FIs that are not SFC-licensed VAS Providers when, for example, the FI's customer is a VASP or derives its funds or wealth substantially from virtual assets.

		anonymity-enhancing technologies or mechanisms (e.g. mixers, tumblers) or peer-to-peer platforms; and (d) a customer who is a VASP sets up offices in, or moves offices to, jurisdictions ~~with~~for no apparent business reason or posing a higher risk (especially those that neither prohibit nor regulate virtual asset-related activities or services).
Product/service/transaction risk		
	12.15.3	Examples of products, services or transactions[181] that may present higher ML/TF risk include: (a) products or services that may inherently favour anonymity or obscure information about underlying customer transactions, especially those involving the use of anonymity-enhancing technologies or mechanisms, or that are not supported by any technological solutions adopted for screening of virtual asset transactions and the associated wallet addresses[182]; (b) deposits from or payments to unknown or unrelated third parties in the form of virtual assets; (c) virtual assets that have been associated with fraud, market abuse or other illicit activities; (d) the purchase of virtual assets using physical cash; and (e) virtual asset-related products or services funded by payments from or instructions given by unexpected third parties, particularly from jurisdictions posing a higher risk.

[181] These product, service and transaction risk indicators are also relevant to FIs that are not SFC-licensed VAS Providers when, for example, an FI offers products, services or transactions involving virtual assets.

[182] Guidance on technological solutions adopted for screening of virtual asset transactions and the associated wallet addresses is provided in paragraphs 12.7.3 and 12.7.4.

12.16 Illustrative indicators of suspicious transactions and activities		
	12.16.1	In addition to the non-exhaustive illustrative indicators of suspicious transactions and activities set out in Appendix B, paragraphs 12.16 set out non-exhaustive illustrative indicators of suspicious transactions and activities in relation to virtual assets.
Customer-related		
	12.16.2	(a) A customer who has no discernible reason for using the FI's services (e.g. a customer has opened an account for virtual asset trading services but only deposits fiat currency or virtual assets and subsequently withdraws the entire balance or a substantial portion of the deposited assets without other activity; or a customer located in a place outside Hong Kong who opens an account with the FI to trade virtual assets that are also available from VASPs located in that place[183]); (b) Requests by customers for virtual asset trading services or virtual asset transfers where the source of the funds is unclear or not consistent with the customers' profile and apparent standing; (c) A customer who enters an FI's platform and/or initiates transactions from an IP address that may present higher risks, for example: (i) from jurisdictions posing a higher risk; (ii) not in line with the customer's profile (e.g. IP address from a jurisdiction which is not the customer's place of residence or principal business); (iii) previously identified as suspicious by the FI; or (iv) associated with a darknet market or

[183] This may, for example, include situations where an FI acts as a respondent institution and provides trading services for virtual assets through a cross-border correspondent relationship with a correspondent institution (see paragraphs 4.20.1 and 12.6.1).

		software that increases anonymity or allows anonymous communications (e.g. proxies, unverifiable IP geographical location, virtual private networks, The Onion Router (Tor)); (d) A customer and other apparently unrelated customer(s) entering the FI's platform from the same IP or MAC address; (e) A customer who frequently changes contact information, e.g. email address, phone number, especially when those ~~that~~ are disposable or temporary[184]; and (f) A customer who frequently or over a short period of time, e.g. within a few hours, changes the IP address or device used to enter the FI's platform and/or conduct transactions ~~over a short period of time, e.g. within a few hours~~.
Trading-related		
	12.16.3	(a) Buying and selling of virtual assets with no discernible purpose or where the nature, size or frequency of the transactions appears unusual. For example, where a customer repeatedly conducts virtual asset transactions with a particular person or group of persons at a significant profit or considerable loss, which may indicate that the transactions are used to transfer value or obfuscate funds flow as part of a ML/TF scheme, or a potential account takeover; (b) Mirror trades or transactions involving virtual assets used for currency conversion for illegitimate or no apparent business purposes; (c) Converting virtual assets to fiat currency at a potential loss with no apparent commercial rationale regardless of, for example, the price fluctuations or high commission fees; and (d) Conversion of a large amount of fiat currency

[184] This may also indicate a potential account takeover against a customer (i.e. a fraudster poses as a genuine customer, gains control of an account and then conducts unauthorised transactions).

		or virtual assets into other or multiple types of virtual assets with no logical or apparent reason which obscures the flow of funds.
Market abuse activities-related		
	12.16.4	(a) Placing of buy and sell orders in close chronological sequence for accounts with the same beneficial owner or of connected persons in the same virtual assets which are thinly-traded; (b) Multiple new customers are referred by the same individual to open accounts for trading in the same virtual asset within a short period of time; (c) A customer engages in prearranged or other non-competitive trading in particular virtual assets; (d) The entry of matching buy and sell orders in ~~particular~~specific virtual assets ("wash trading"), creating the illusion of active trading with no change in the beneficial ownership of the virtual assets. Such wash trading does not result in a bona fide market position, which might also provide "cover" for a money launderer; (e) Accumulation of a virtual asset with small increments in price to gradually increase the price of the virtual asset over a period of time; (f) A customer makes large purchases of a virtual asset, particularly a virtual asset which is thinly-traded, within a short period of time, and the size of the transactions is incommensurate with the customer's profile; and (g) A group of customers sharing the same trading patterns (e.g. purchasing the same virtual asset at the same or similar time or price), particularly in relation to a virtual asset which is thinly-traded, authorise the same person or third party to operate their accounts and/or transfer fiat currency or virtual assets amongst their accounts.

Related to movement of funds and virtual assets		
	12.16.5	(a) A customer uses an FI to make payments or to hold funds or other property that are rarely used or are not being used to trade in virtual assets, i.e. the account appears to be used as a depositary account or a conduit for transfers; (b) Transfers of positions, funds, virtual assets or other property between accounts of parties that do not appear to be commonly controlled or have an apparent relationship; (c) Frequent funds, virtual assets or other property transfers or cheque payments to or from third parties that are unrelated or difficult to verify; (d) Transfers of funds or virtual assets to and from financial institutions or VASPs located in jurisdictions posing a higher risk[185], or, which are not consistent with the customer's declared place of residence, business dealings or interests, without reasonable explanation; (e) Transfers of funds or virtual assets to the same person from different parties, or to different persons from the same party without reasonable explanation; (f) Frequent changes of bank account or wallet address details or information for receiving funds or virtual assets; (g) Multiple transactions involving a high value of virtual assets where the nature, frequency or pattern of the transactions appears unusual, e.g. the transactions are conducted in short succession such as within a 24-hour period, or in a staggered and regular pattern followed by a long period of inactivity; transfer of virtual assets to another wallet, particularly a new wallet or wallet that has been inactive for a period of time, which may indicate possibility of ransomware attack or other cybercrimes; (h) Virtual assets are transferred from wallet

[185] For example, a VASP located in a jurisdiction that neither prohibits nor regulates virtual asset-related activities or services. Please also refer to guidance on jurisdictions posing a higher risk provided in paragraphs 4.13 for details.

		addresses which are known to hold stolen virtual assets, or are known to associate with holders of stolen virtual assets; (i) Deposits of virtual assets, including those from new customers, are immediately followed by transactions with no apparent legitimate purpose or commercial rationale which incur additional or unnecessary cost or fees (e.g. converting the deposited virtual assets to other or multiple types of virtual assets which obfuscates the trail of transactions, and/or withdrawing all or part of the deposited virtual assets to unhosted wallets immediately); (j) Transfers of virtual assets from multiple wallets in small amounts, in particular, those that are held by third parties, with subsequent transfer to another wallet or conversion of the entire amount to fiat currency; (k) Transactions involving virtual assets that provide higher anonymity such as anonymity-enhanced virtual assets (e.g. depositing a virtual asset that operates on a public blockchain and immediately converting it into a virtual asset that provides higher anonymity); (l) A customer uses an FI to convert an unusual amount (in terms of volume or number) of virtual assets from peer-to-peer platforms (e.g. a peer-to-peer platform with lax AML/CFT controls) into fiat currency ~~with~~for no logical or apparent reason; (m) Transfers of virtual assets to or from wallet addresses presenting higher risks, for example, wallet addresses that are directly and/or indirectly associated with illicit or suspicious activities/sources or designated parties[186];

[186] Guidance on identifying transactions involving wallet addresses that are directly and/or indirectly associated with illicit or suspicious activities/sources or designated parties is provided in paragraph 12.7.3.

		(n) Transfers of virtual assets that have been associated with chain-hopping[187]; (o) Frequent and/or large transactions involving virtual assets from virtual asset automatic teller machines or kiosks, especially those located in jurisdictions posing a higher risk; (p) Information or message transmitted with a virtual asset transfer indicates that the transaction may be used to finance or assist illicit activities; (q) A customer who is a financially vulnerable person and/or has no prior knowledge of virtual assets engages in frequent and/or large transactions (in particular, deposits and withdrawals of funds and/or virtual assets) through an FI, which may be ~~indicative~~ signs indicating ~~of a~~ money mule or scam victim; (r) Deposits of large amounts of virtual assets followed by conversion to fiat currencies, where the source of the funds is unclear and the size of transactions is not in line with the background of the customer, which may suggest that the deposited virtual assets are stolen assets; (s) A customer's funds or virtual assets originate from, or are sent to, a financial institution or VASP that (i) is not registered or licensed in the jurisdiction that it operates from (or where the customer to whom it offers products and/or services resides or is located), or (ii) operates from (or the customer to whom it offers products and/or services resides or is located in) a jurisdiction that neither prohibits nor regulates virtual asset-related activities or services; (t) The required information in a virtual asset transfer is inaccurate or incomplete, for example, in the case of an ordering institution, discrepancies were noted between the

[187] Refer to paragraph 12.1.~~87~~ for the meaning of "chain-hopping".

		recipient's information provided by its customer and the information maintained by the beneficiary institution which may have resulted in a rejection of the virtual asset transfer request or return of the relevant virtual assets by the beneficiary institution, or ~~(where applicable)~~ the information noted from the screening of the recipient's wallet address associated with the virtual asset transfer (see paragraphs 12.7.2 to 12.7.4 and 12.7.6); (u) A customer with limited or no other assets at the FI receives a transfer of large amounts of thinly-traded virtual assets; and (v) A customer deposits virtual assets and requests to credit them to multiple accounts that do not appear to be related, and to sell or otherwise transfer ownership of the virtual assets.
12.17 Miscellaneous illustrative examples and further guidance		
Examples of possible enhanced measures in relation to RBA		
	12.17.1	In addition to the examples of possible enhanced measures in relation to RBA set out in paragraph 2 of Appendix C, paragraph 12.17.2 sets out other examples relevant to virtual assets.
Para. 2.1, 2.13, 4.1.2 & 4.9.3 of this Guideline	12.17.2 ~~12.17.1~~	~~In addition to the e~~Examples of possible enhanced measures ~~in relation to RBA set out in paragraph 2 of Appendix C, examples~~ relevant to virtual assets include: (a) where the customer is a financial institution or VASP [188] , obtaining additional or more particular information about the financial institution or VASP's underlying customer base and its AML/CFT controls; and

[188] For the avoidance of doubt, where the provision of services by an FI to a customer that is a financial institution or VASP located in a place outside Hong Kong constitutes a cross-border correspondent relationship having regard to paragraphs 4.20.1 and 12.6.1 of this Guideline, the FI should also comply with the relevant provisions in paragraphs 4.20 and 12.6.

		(b) evaluating the information provided by the customer with regard to destination of funds or virtual assets involved in the transaction and the reason for the transaction to better assess the risk of ML/TF.

APPENDIX A Illustrative risk indicators for assessing ML/TF risks

The following is a list of non-exhaustive illustrative risk indicators for institutional risk assessment and customer risk assessment. These examples of indicators associated with each risk factor mentioned in paragraphs 2.6 and 2.17 may indicate higher or lower ML/TF risks as the case may be.

1	**Country risk**
	Examples of countries or jurisdictions[189] that may present higher ML/TF risk include: (a) countries or jurisdictions that have been identified by the FATF as jurisdictions with strategic AML/CFT deficiencies; (b) countries or jurisdictions subject to sanctions, embargos or similar measures issued by, for example, the UN; (c) countries or jurisdictions which are more vulnerable to corruption[190]; and (d) countries or jurisdictions that are believed to have strong links to terrorist activities. Examples of countries or jurisdictions that may be considered to carry lower ML/TF risk include: (a) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT Systems; and (b) countries or jurisdictions identified by credible sources as having a low level of corruption or other criminal activity.

[189] Guidance on jurisdictions posing a higher risk is provided in paragraphs 4.13.

[190] When assessing which countries are more vulnerable to corruption, FIs may make reference to publicly available information or relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations (an example of which is Transparency International's "Corruption Perceptions Index", which ranks countries according to their perceived level of corruption).

2	**Customer risk**
	Examples of customers that may present higher ML/TF risk include: (a) the business relationships established in unusual circumstances (e.g. a customer instructs an FI to set up a discretionary management agreement for an investment vehicle owned by the customer but requests the FI to buy and sell particular securities for the investment vehicle only according to the customer's instructions); (b) non-resident customers who have no discernible reasons for opening an account with FIs in Hong Kong; (c) the use of legal persons or arrangements as personal asset-holding vehicles without any commercial or other valid reasons; (d) companies that have nominee shareholders, nominee directors, bearer shares or bearer shares ~~in bearer form~~warrants; (e) customers that engage in, or derive wealth or revenues from, cash-intensive businesses; (f) the ownership structure of a company appears unusual or excessively complex having considered the nature of the company's business; (g) the customer or the family member or close associate of a customer is a PEP (including where a beneficial owner of a customer is a PEP); (h) customers that have been mentioned in negative news reports from credible media, particularly those related to predicate offences for ML/TF or financial crimes; (i) nature, scope and location of business activities generating the funds[191] may be related to high risk activities or jurisdictions posing a higher risk; (j) customers that have sanction exposure; (k) where the origin of wealth (for high risk customers and PEPs) or ownership cannot be easily verified; and (l) a customer introduced by an overseas financial

[191] Consideration should be given to the risks inherent in the nature of the activity of the customer and the possibility that the transaction may itself be a criminal transaction.

	institution, affiliate or other investor, both of which are based in jurisdictions posing a higher risk[192]. Examples of customers that may be considered to carry lower ML/TF risk include: (a) specific types of customers that may be eligible for SDD as specified in paragraph 4.8.3 or simplified measures as specified in paragraph 4 of Appendix C; (b) customers who are employment-based or with a regular source of income from a known legitimate source which supports the activity being undertaken; and (c) the reputation of the customer, e.g. a well-known, reputable private company, with a long history that is well documented by independent sources, including information regarding its ownership and control.
3	**Product/service/transaction risk**
	Examples of products, services or transactions that may present higher ML/TF risk include: (a) products or services that may inherently favour anonymity or obscure information about underlying customer transactions; (b) products that have the ability to pool underlying customers/funds; (c) deposits from or payments to unknown or unrelated third parties; (d) the products or services offered to customers associated with jurisdictions posing a higher risk (e.g. where a customer resides in a jurisdiction posing a higher risk or where the customer's source of funds or source of wealth is mainly derived from jurisdictions posing a higher risk); (e) products with unusual complexity or structure and with no obvious economic purpose; (f) products or services that permit the unrestricted or anonymous transfer of value (by payment or change of asset ownership) to an unrelated third party, particularly

[192] Guidance on jurisdictions posing a higher risk is provided in paragraphs 4.13.

	from jurisdictions posing a higher risk; (g) use of new technologies or payment methods not used in the normal course of business by the FI; (h) products that have been particularly subject to fraud and market abuse, such as low-priced/small-cap and thinly-traded stocks; (i) the purchase of securities using physical cash; and (j) securities-related products or services funded by payments from or instructions given by unexpected third parties, particularly from jurisdictions posing a higher risk. Examples of products, services or transactions that may be considered to carry lower ML/TF risk include: (a) specific types of products that may be eligible for SDD as set out in paragraph 4.8.15.
4	**Delivery/distribution channel risk**
	Examples of delivery/distribution channels that may present higher ML/TF risk include: (a) business relationships established using a non-face-to-face approach or transactions conducted by customer through non-face-to-face channels, where increased risks (e.g. impersonation or identity fraud) could not be adequately mitigated and/or are more susceptible to risk situations such as unauthorised trading and related ML/TF abuse; and (b) products or services distributed or sold through intermediaries (i.e. business relationship between an FI and the end customer may become indirect), especially if the intermediaries are: (i) suspected of criminal activities, particularly financial crimes or association with criminal associates; (ii) located in a higher risk country or in a country with a weak AML/CFT regime; (iii) serving high risk customers without appropriate risk mitigating measures; or (iv) with a history of non-compliance with laws or regulation or that have been the subject of relevant negative attention from credible media or law

	enforcement. Examples of delivery/distribution channels that may be considered to carry lower ML/TF risk include: (a) business relationships established or transactions conducted by customers through channels that are less susceptible to risk situations such as unauthorised trading and related ML/TF abuse; and (b) products or services distributed or sold directly to the customer.

APPENDIX B Illustrative indicators of suspicious transactions and activities

The following is a list of non-exhaustive illustrative indicators of suspicious transactions and activities that may help assess whether or not transactions and activities might give rise to grounds of ML/TF suspicion.

1	**Customer-related**
	(a) A customer who has no discernible reason for using the FI's services (e.g. a customer has opened an account for discretionary management services but directs the FI to carry out his own investment decisions or a customer located in a place outside Hong Kong who uses local accounts to trade on stock or futures exchanges located in that place); (b) A customer who has requested, without reasonable explanation, transactions that are out of the ordinary range of services normally requested, or are outside the experience of the financial services business in relation to the particular customer; (c) Extensive use of trusts or offshore structures in circumstances where the customer's needs are inconsistent with the use of such services; (d) A legal person customer with bearer shares constituting a large part of its issued capital; (e) A customer who has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason; (f) A customer's legal or mailing address is associated with other apparently unrelated accounts; or does not seem connected to the customer; (g) Requests by customers for dealing or investment management services (with regard to securities, futures contracts or leveraged foreign exchange contracts) where the source of the funds is unclear or not consistent with the customers' profile and apparent standing; (h) A customer who refuses to provide the information

	requested without reasonable explanation or who otherwise refuses to cooperate with the CDD and/or ongoing monitoring process; (i) A customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation; (j) A customer who exhibits unusual concern with the FI's AML/CFT Systems including policies, controls, monitoring or reporting thresholds; (k) A customer who does not exhibit any concern with the cost of transactions or fees; and (l) A customer who is known to have criminal, civil or regulatory proceedings against it for corruption, misuse of public funds, other financial crimes or regulatory non-compliance, or is known to associate with such persons.
2	**Trading-related**
	(a) Transactions or instructions which have no apparent legitimate purpose or commercial rationale or involve apparently unnecessary complexity; (b) The size or pattern of transactions is not in line with the background of the customer or its past transaction volume/pattern; (c) Buying and selling of securities, futures or leveraged foreign exchange contracts with no discernible purpose or where the nature, size or frequency of the transactions appears unusual. For example, where a customer frequently purchases securities at a high price and subsequently sells them at a considerable loss to the same party. This may indicate transferring value from one party to another; (d) A number of transactions by the same customer in small amounts relating to the same investment, each purchased for cash and then sold in one transaction, the proceeds being paid to a person other than that customer; (e) Mirror trades or transactions involving securities used for currency conversion for illegitimate or no apparent business purposes; (f) Securities, futures or leveraged foreign exchange

	contracts transactions occur across many jurisdictions, and in particular jurisdictions posing a higher risk; (g) Securities intended to be held-to-maturity are unwound before maturity in the absence of volatile market conditions or other logical or apparent reason; and (h) Suspected front-running of other pending customer orders.
3	**Selected indicators of market manipulation[193] and insider dealing**
	(a) Making a large purchase or sale of a security, or option on a security, shortly before news or a significant announcement is issued that affects the price of the security, which may be suggestive of potential insider trading or market manipulation; (b) A request to execute or clear a buy order and sell order in close chronological sequence for accounts with the same beneficial owner or of connected persons in the same securities which are thinly-traded; (c) Multiple new customers are referred by the same individual to open accounts for trading in the same security within a short period of time; (d) A customer engages in prearranged or other non-competitive trading in particular securities or futures contracts; (e) The entry of matching buy and sell orders in particular securities or futures contracts ("wash trading"), creating the illusion of active trading. Such wash trading does not result in a bona fide market position, which might also provide "cover" for a money launderer; (f) Transfers of positions between accounts that do not appear to be commonly controlled; (g) Accumulation of a security with small increments in price throughout the trading day to increase the price of the security; (h) Executing purchase or sale orders for one or more accounts in a security regularly at or near the close of

[193] FIs are expected to take appropriate steps to ensure that proper safeguards exist to prevent the firm from acting in a way which would result in the firm perpetrating any conduct which constitutes market misconduct under section 274, 275 or 278 of the SFO, or any criminal offence under section 295, 296 or 299 of the SFO.

	market trading hours that alter the closing price of the security; and (i) Placing multiple buy or sell orders and cancelling some or all of them before execution regularly.
4	**Related to deposits of securities**
	(a) The customer's explanation regarding the method of acquiring the physical share certificates deposited at the FI does not make sense or changes; (b) A customer has a pattern of depositing physical share certificates or receiving incoming share transfers, forthwith selling the shares and transferring out the proceeds; (c) A customer with limited or no other assets at the FI receives a transfer of large amounts of thinly-traded securities; and (d) A customer deposits securities and requests to credit them to multiple accounts that do not appear to be related, and to sell or otherwise transfer ownership of the securities.
5	**Related to settlement and movement of funds and securities**
	(a) Large or unusual settlements of transactions in cash or bearer form or where a customer only deals with an FI in cash; (b) A customer uses an FI to make payments or to hold funds or other property that are rarely used or are not being used to trade in securities, futures contracts or leveraged foreign exchange contracts, i.e. account appears to be used as a depositary account or a conduit for transfers; (c) Non-resident customer's account with very large account movements and subsequent fund transfers to offshore financial centres; (d) Transfers of positions, funds or other property between securities accounts of parties that do not appear to be commonly controlled or have an apparent relationship; (e) Frequent funds or other property transfers or cheque payments to or from third parties that are unrelated or difficult to verify;

	(f) Transfers to and from jurisdictions posing a higher risk without reasonable explanation, which are not consistent with the customer's declared business dealings or interests; (g) The involvement of offshore companies on whose accounts multiple transfers are made, especially when they are destined for a tax haven, and to accounts in the name of offshore companies of which the customer may be a shareholder; (h) Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring threshold; (i) Transfers of funds or securities to the same person from different parties, or to different persons from the same party without reasonable explanation; (j) Funds are transferred to other FIs in different jurisdictions from the FI where the funds were initially received; and (k) Frequent changes of bank account details or information for receiving investment sale proceeds.
6	**Employee-related**
	(a) Changes in employee characteristics, e.g. lavish life styles or avoiding taking holidays without reasonable cause; (b) Unusual or unexpected increase in the sales performance of an employee; (c) The employee's supporting documentation for customers' accounts or orders is incomplete or missing; and (d) The use of an address which is not the customer's home or office address, e.g. utilisation of an employee's address for the dispatch of customer documentation or correspondence.

APPENDIX C Miscellaneous illustrative examples and further guidance

~~2.1~~ ~~2.13~~ ~~4.1.2~~	1	**Examples of possible simplified measures in relation to RBA**
Para. 2.1, 2.13 & 4.1.2 of this Guideline		Examples include: (a) limiting the type or extent of CDD measures, such as altering the type or range of documents, data or information used for verifying the identity of a customer; (b) reducing the frequency of review of the existing CDD records; (c) reducing the degree of ongoing monitoring and scrutiny of transactions based on a reasonable monetary threshold; or (d) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and intended nature from the type of transactions or business relationship established.
~~2.1~~ ~~2.13~~ ~~4.1.2~~ ~~4.9.3~~	2	**Examples of possible enhanced measures in relation to RBA**
Para. 2.1, 2.13, 4.1.2 & 4.9.3 of this Guideline		Examples include: (a) obtaining additional information from a wide variety of sources [194] on the customer and (where appropriate) the beneficial owner of the customer before the establishment of the business relationship, and for performing ongoing customer risk assessment; (b) increasing the frequency of review of the existing CDD records; (c) obtaining additional information and

[194] Examples of additional information include occupation, volume of assets, reputation and background of the customer and (where appropriate) the beneficial owner. Examples of sources include the internet and publicly or commercially available databases.

		corroborating it with other available sources on the purpose and intended nature of the business relationship or transaction; (d) obtaining additional information and corroborating it with other available sources on the customer's source of wealth or source of funds involved in the transaction or business relationship[195]; (e) increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination; (f) where the customer is a financial institution[196], obtaining additional or more particular information about the financial institution's underlying customer base and its AML/CFT controls; (g) evaluating the information provided by the customer with regard to destination of funds involved in the transaction and the reason for the transaction to better assess the risk of ML/TF; (h) requiring that investment sale proceeds are paid to the customer's bank account from which the funds for investment were originally transferred; or (i) where an FI is being appointed by a customer that is an asset management company located in a place outside Hong Kong (the "delegating asset management company") to provide discretionary asset management services in relation to an investment vehicle and does not have a business relationship with the investment vehicle, where appropriate, obtaining additional customer information such as a general

[195] Guidance on source of wealth and source of funds are provided in paragraphs 4.11.13 and 4.11.14. For the avoidance of doubt, for a customer or beneficial owner of a customer that is a ~~foreign~~ non-Hong Kong PEP, ~~domestic~~ a Hong Kong PEP or an international organisation PEP, and in any situation that by its nature presents a higher risk of ML/TF, the respective special requirements set out in paragraphs 4.11 and 4.9 apply.

[196] For the avoidance of doubt, where the provision of services by an FI to a customer that is a financial institution located in a place outside Hong Kong constitutes a cross-border correspondent relationship having regard to paragraph 4.20.1 of this Guideline, the FI should also comply with the relevant provisions in paragraphs 4.20.

		understanding of the delegating asset management company's customer base (e.g. the types of funds it transacts for; these funds' investor bases in their entirety; and the jurisdictions where these funds are offered), the reputation of the delegating asset management company (e.g. whether it has or had been subject to any targeted sanctions, ML/TF investigations or regulatory actions) and its AML/CFT controls; obtaining senior management approval and understanding respective AML/CFT responsibilities clearly.
~~4.2.6~~	3	**Examples of possible measures in relation to the verification of the name, legal form and current existence of a customer that is a legal person**
Para. 4.2.6 of this Guideline		Examples of possible measures to verify the name, legal form and current existence of a legal person: for a locally incorporated company: (a) performing a search of file at the Hong Kong Company Registry to obtain a company report (or obtaining from the customer a certified true copy of a company search report issued and certified by a company registry or professional person); for a company incorporated overseas: (b) performing a similar company search enquiry of the registry in the place of incorporation to obtain a company report; (c) obtaining a certificate of incumbency or equivalent issued by the company's registered agent in the place of incorporation (or accepting a certified true copy of a certificate of incumbency certified by a professional person); or (d) obtaining a similar or comparable document to a company search report or a certificate of incumbency certified by a professional person in

		the relevant jurisdiction.
~~4.2.14~~	4	**Examples of simplified and enhanced measures in verifying the identity of a customer that is a legal person, trust or other similar legal arrangement**
Para. 4.2.14 of this Guideline		Simplified measures Where the assessed ML/TF risks are lower, an FI may consider to accept documents, data or information other than the examples provided in paragraphs 4.2.6 and 4.2.11, when verifying the name, legal form and current existence of the customer, or powers that regulate and bind the customer. Examples of such other documents, data or information include: (a) where the customer is (i) an FI as defined in the AMLO; or (ii) other FI that is incorporated or established in an equivalent jurisdiction, carry on a business similar to that carried out by an FI as defined in the AMLO, and subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF;[17] a proof that the customer is a licensed (and supervised) FI in the jurisdiction concerned; (b) where the customer is a listed company, a proof of its listed status; (c) where the customer is the government or a public body in Hong Kong or in an equivalent jurisdiction, a proof that the customer is the government or a public body; and (d) where the customer is a collective investment scheme authorised for offering to the public in Hong Kong or in an equivalent jurisdiction, a proof of its authorisation status. Enhanced measures Where the assessed ML/TF risks are higher, in

		addition to verifying the name, legal form and current existence of the customer, and powers that regulate and bind the customer in accordance with paragraphs 4.2.6 and 4.2.11, an FI should decide whether additional information in respect of the customer, its operation and the individuals behind it should be obtained and the extent of further verification that is required.
~~4.3.13~~	5	**Examples of information which may be collected to identify the intermediate layers of the corporate structure of a legal person with multiple layers in its ownership structure**
Para. 4.3.13 of this Guideline		If the customer's ownership structure consists of multiple layers of companies, an FI should determine on a risk-sensitive basis the amount of information in relation to the intermediate layers to be collected, which may include obtaining a director's declaration incorporating or annexing an ownership chart describing the intermediate layers (the information to be included should be determined on a risk-sensitive basis but at a minimum should include company name and place of incorporation, and where applicable, the rationale behind the particular structure employed). FIs need not, as a matter of routine, verify the details of the intermediate companies in the ownership structure of a company. Complex ownership structures (e.g. structures involving multiple layers, different jurisdictions, trusts, etc.) without an obvious commercial purpose pose an increased risk and may require further steps to ensure that the FI is satisfied on reasonable grounds as to the identities of the beneficial owners. The need to verify the intermediate corporate layers of the ownership structure of a company will therefore depend upon the FI's overall understanding of the structure, its assessment of the risks and whether the information available is adequate in the circumstances for the FI to consider

		if it has taken adequate measures to identify the beneficial owners. Where the ownership is dispersed, the FI may concentrate on identifying and taking reasonable measures to verify the identities of those who exercise ultimate control over the management of the company.
~~4.5.3~~	6	**Examples of procedures to establish whether the identification documents offered by customers are genuine, or have been reported as lost or stolen**
Para. 4.5.3 of this Guideline		If suspicions are raised in relation to any identification document offered by customers, FIs should take whatever practical and proportionate steps that are available to establish whether the document offered is genuine, or has been reported as lost or stolen. This may include: (a) searching publicly available information; (b) approaching relevant authorities (such as the Immigration Department through its hotline); or (c) requesting corroboratory evidence from the customer. Where suspicion cannot be eliminated, the document should not be accepted and consideration should be given to making a report to the authorities.

~~4.10.4~~	7	**Use of an independent and appropriate person to certify identification documents**
Para. 4.10.5 of this Guideline	7.1	Use of an independent[197] and appropriate person to certify verification of identification documents guards against the risk that documentation provided does not correspond to the customer whose identity is being verified. However, for certification to be effective, the certifier will need to have seen the original documentation.
	7.2	The following is a list of non-exhaustive examples of appropriate persons to certify verification of identification documents: (a) an intermediary specified in section 18(3) of Schedule 2; (b) a member of the judiciary in an equivalent jurisdiction; (c) an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity; (d) a Justice of the Peace; and (e) other professional person[198] such as certified public accountant, lawyer, notary public and chartered secretary[199].
	7.3	The certifier should sign and date the copy document (printing his/her name clearly in capitals underneath) and clearly indicate his/her position or capacity on it. The certifier should state that it is a true copy of the original (or words to similar effect).

[197] In general, it is not sufficient for the copy documents to be self-certified by the customer. However, an FI may accept the copy documents certified by a professional person within a legal person customer if that professional person is subject to the professional conduct requirements of a relevant professional body, and has certified the copy documents in his or her professional capacity.

[198] An FI may accept other appropriate professional person as certifier. The FI should have due consideration to paragraph 7.4 of Appendix C in similar manner to other types of appropriate certifiers being used.

[199] A chartered secretary refers to a current member of The Chartered Governance Institute (formerly The Institute of Chartered Secretaries and Administrators) who has attained the chartered status.

	7.4	FIs remain liable for failure to carry out prescribed CDD and therefore should exercise caution when considering accepting certified copy documents, especially where such documents originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction. In any circumstances where an FI is unsure of the authenticity of certified documents, or that the documents relate to the customer, FIs should take additional measures to mitigate the ML/TF risk.
~~5.2~~	8	**Examples of trigger events upon which existing records of customers should be reviewed**
Para. 5.2 of this Guideline		Examples of trigger events include: (a) when a significant transaction[200] is to take place; (b) when a material change occurs in the way the customer's account is operated[201]; (c) when the FI's customer documentation standards change substantially; or (d) when the FI is aware that it lacks sufficient information about the customer concerned.

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

[201] Reference should also be made to section 6 of Schedule 2 "Provisions relating to Pre-Existing Customers".

GLOSSARY OF KEY TERMS AND ABBREVIATIONS

Terms / abbreviations	Meaning
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)
FATF	Financial Action Task Force
FI(s)	Financial institution(s)
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)
PPTA	Person purporting to act on behalf of the customer
Proliferation financing or PF	Financing of proliferation of weapons of mass destruction

RA(s)	Relevant authority (authorities)
RBA	Risk-based approach
Schedule 2	Schedule 2 to the AMLO
Senior management	Senior management means directors (or board) and senior managers (or equivalent) of a firm who are responsible, either individually or collectively, for management and supervision of the firm's business. This may include a firm's Chief Executive Officer, Managing Director, Responsible Officer, Manager-In-Charge of Core Function(s) or other senior operating management personnel (as the case may be).
SFO	Securities and Futures Ordinance (Cap. 571)
STR(s)	Suspicious transaction report(s); also referred to as reports or disclosures
UNATMO	United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575)
UNSO	United Nations Sanctions Ordinance (Cap. 537)
VASP(s)	Virtual asset service provider(s)
WMD(CPS)O	Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap. 526)

SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

Prevention of Money Laundering and Terrorist Financing Guideline issued by the Securities and Futures Commission for Associated Entities of Licensed Corporations and SFC-licensed Virtual Asset Service Providers

~~September 2021~~June 2023

April 2012 first edition
March 2018 second edition
November 2018 third edition
September 2021 fourth edition
June 2023 fifth edition

Published by
Securities and Futures Commission
54/F, One Island East
18 Westlands Road
Quarry Bay
Hong Kong
Tel : (852) 2231 1222
Fax : (852) 2521 7836
E-mail : enquiry@sfc.hk
SFC website : www.sfc.hk

Prevention of Money Laundering and Terrorist Financing Guideline issued by the Securities and Futures Commission for Associated Entities of Licensed Corporations and SFC-licensed Virtual Asset Service Providers

Introduction		
s.399, SFO, s.53ZTK, AMLO	1	This Guideline is published under section 399 of the Securities and Futures Ordinance, Cap. 571 (the SFO) and section 53ZTK of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap. 615 (the AMLO).
	2	~~Following the enactment of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap. 615 (the AMLO) and subsequent amendments to the AMLO in 2022, t~~The ~~Securities and Futures Commission (SFC) has prepared a~~ Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset Service Providers) (the Guideline for LCs and SFC-licensed VAS Providers) issued by the Securities and Futures Commission (SFC) ~~which~~ sets out the relevant anti-money laundering and counter-financing of terrorism (AML/CFT) statutory and regulatory requirements, and the AML/CFT standards which licensed corporations (LCs) and virtual asset service providers licensed by the SFC under the AMLO (SFC-licensed VAS Providers) should meet in order to comply with the statutory requirements under the AMLO and the SFO.
	3	The Guideline for LCs and SFC-licensed VAS Providers 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 LCs and SFC-licensed VAS Providers, 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.
	4	Terms and abbreviations used in this Guideline shall be interpreted by reference to the definitions set out in the Glossary part of the Guideline for LCs and SFC-licensed VAS Providers. Where applicable, interpretation of other words or phrases should follow those set out in the AMLO or the SFO (as the case may be).
Associated Entities to comply with the Guideline for LCs and SFC-licensed VAS Providers		
	5	This Guideline is intended for use by associated entities (AEs) that are not authorized financial institutions and their officers and staff.
	6	The Guideline for LCs and SFC-licensed VAS Providers provides a comprehensive explanation of the AML/CFT legislation in Hong Kong and practical guidance in designing and implementing policies, procedures and controls so as to meet the relevant AML/CFT statutory and regulatory requirements and the AML/CFT standards. AEs that are not authorized financial institutions are expected to have regard to the provisions of the Guideline for LCs and SFC-licensed VAS Providers as if they were themselves LCs and/or SFC-licensed VAS Providers.
	7	An AE that is an authorized financial institution should have regard to the provisions of the Guideline

		on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) issued by the Hong Kong Monetary Authority for use by authorized institutions, and any of the following provisions of the Guideline for LCs and SFC-licensed VAS Providers that ~~is~~ are applicable: paragraph 4.1.6 ~~about~~ for the definition of "customer" for the securities, futures and leveraged foreign exchange businesses (hereafter collectively referred to as "securities sector" ~~or "securities businesses"~~); paragraphs 4.20 ~~about~~ for the provision on cross-border correspondent relationships applicable to the securities sector; Chapter 12 for the provisions in relation to virtual assets, and Appendix B ~~about~~ for illustrative indicators of suspicious transactions and activities in the securities sector.
	8	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 and the Guideline for LCs and SFC-licensed VAS Providers indicates that it is a mandatory requirement. Given the significant differences that exist in the organisational and legal structures of different AEs, and the LCs with which they are in a controlling entity relationship or the SFC-licensed VAS Providers of which they are wholly owned subsidiaries, as well as the nature and scope of the business activities conducted by them, there exists no single set of universally applicable implementation measures. The content of this Guideline and the Guideline for LCs and SFC-licensed VAS Providers is not intended to be an exhaustive list of the means of meeting the statutory and regulatory requirements. AEs therefore should use this Guideline and the Guideline for LCs and SFC-licensed VAS Providers as a basis to develop measures appropriate to their structure and business activities.

	9	The Guideline for LCs and SFC-licensed VAS Providers will assist AEs to meet their AML/CFT legal and regulatory obligations when tailored by AEs to their particular business risk profile.
s.399, SFO, s.53ZTK, AMLO	10	A failure by any person to comply with any provision of this Guideline does not by itself render the person liable to any judicial or other proceedings but, in any proceedings under the AMLO or the SFO before any court, this Guideline is admissible in evidence; and if any provision set out in this Guideline appears to the court to be relevant to any question arising in the proceedings, the provision must be taken into account in determining that question.
s.53ZTK(6), AMLO	11	Any failure by an AE to have regard to the provisions of the Guideline for LCs and SFC-licensed VAS Providers may reflect adversely on its fitness and properness and the fitness and properness of the intermediary ~~of~~ with which the AE is in a controlling entity relationship or the SFC-licensed VAS Providers of which the AE is a wholly owned subsidiary.
	12	Any failure by an AE that is an authorized financial institution to have regard to the provisions of the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) issued by the Hong Kong Monetary Authority for use by authorized institutions, or to paragraphs 4.1.6 and 4.20 of, Chapter 12 of, and Appendix B to the Guideline for LCs and SFC-licensed VAS Providers may reflect adversely on its fitness and properness and the fitness and properness of the intermediary ~~of~~with which the AE is in a controlling entity relationship.
	13	The relevance and usefulness of this Guideline will be kept under review and it may be necessary to issue amendments from time to time.

SFC Disciplinary Fining Guidelines

Part 5B of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance Considerations relevant to the level of a disciplinary fine

These guidelines are made under section 53ZSS(1) of Part 5B of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Ordinance) to indicate the manner in which the Securities and Futures Commission (SFC) proposes to exercise the disciplinary power to impose a pecuniary penalty (fine) on a regulated person under section 53ZSP(3)(c). Section 53ZSS(3) requires the SFC to have regard to these guidelines in exercising its power of fining under section 53ZSP(3)(c). Factors that the SFC proposes to take into account in exercising its fining power are included in the considerations set out below.

Under section 53ZSP of the Ordinance, where a regulated person is, or was at any time, guilty of "misconduct", or the SFC is of the opinion that a regulated person is or was not a fit and proper person to be or to remain the same type of regulated person, the SFC may, either on its own or together with other disciplinary sanctions, impose a fine up to a maximum of HK$10 million or three times of the profit gained or loss avoided as a result of the misconduct or other conduct which leads the SFC to form the opinion, whichever is the greater.

"Misconduct" is defined in section 53ZSR of the Ordinance and includes a contravention of a material requirement[1], or an act or omission relating to the provision of any VA service[2] by a regulated person which, in the opinion of the SFC, is or is likely to be prejudicial to the interests of the investing public or to the public interest.

"Misconduct" may, depending on its nature and characteristics, consist of a number of culpable acts or culpable omissions. Even if they are of the same generic nature, they may attract multiple penalties.

The SFC may use the number of persons affected by the misconduct as the multiplier in assessing the appropriate level of pecuniary penalty, for example, the SFC may impose a fine not exceeding HK$10 million for each affected person. Using the number of affected persons as the multiplier may not be appropriate in every case. The appropriate approach in each case will depend on its facts.

The SFC regards a fine as a more severe sanction than a reprimand. The SFC will not impose a fine if the circumstances of a particular case only warrant a public reprimand. As a matter of policy, the SFC will publicise all fining decisions.

When considering whether to impose a fine under section 53ZSP(3)(c) and the size of any fine, the SFC will consider all the circumstances of the particular case, including the Specific Considerations described below.

A fine should deter non-compliance with the requirements of the Ordinance and related regulatory requirements, so as to protect the reputation of Hong Kong as an international financial centre.

Although section 53ZSP(3)(c)(ii) states that one alternative maximum level of fine that can be imposed is three times the profit gained or loss avoided, the SFC will not automatically link the fine imposed in any particular case with the profit gained or loss avoided.

---

[1] "Material requirement" is defined to mean any provision of the Ordinance or any condition of a licence or any other conditions imposed under or pursuant to any provision of Part 5B of the Ordinance.

[2] "VA service" is defined to mean any of the services specified in Schedule 3B of the Ordinance.

The more serious the conduct, the greater the likelihood that the SFC will impose a fine and that the size of the fine will be larger. In cases where the "misconduct" attracts multiple pecuniary penalties, the SFC will look at the totality of the penalties to ensure it is not disproportionate to the gravity of the conduct in question.

In determining the seriousness of conduct, in general, the SFC views some considerations as more important than others. The General Considerations set out below describe conduct that would be generally viewed as more or less serious. In any particular case, the General Considerations should be read together with the Specific Considerations in determining whether or not the SFC will impose a fine and, if so, the amount of the fine.

General considerations

The SFC generally regards the following conduct as more serious:

- conduct that is intentional or reckless
- conduct that brings the reputation of Hong Kong as an international financial centre into disrepute
- conduct that facilitates or increases the risks of money laundering or terrorist financing
- conduct that damages market integrity
- conduct that causes loss to, or imposes costs on, others
- conduct which provides a benefit to the firm or individual engaged in that conduct or any other person.

The SFC generally regards the following conduct as less serious and so generally deserving a lower fine:

- negligent conduct – however, the SFC will impose disciplinary sanctions including fines for negligent conduct in appropriate circumstances
- conduct which only results in a technical breach of a regulatory requirement or principle in that it:

  + causes little or no damage to market integrity and/or the reputation of Hong Kong as an international financial centre; and

  + causes little or no loss to, or imposes little or no costs on, others
- conduct which produces little or no benefit to the firm or individual engaged in that conduct and their related parties.

These are only general considerations. These considerations together with the other circumstances of each individual case including the Specific Considerations described below will be determinative.

Specific considerations

The SFC will consider all the circumstances of a case, including:

The nature and seriousness of the conduct

- the impact of the conduct on market integrity and/or the reputation of Hong Kong as an international financial centre

- whether significant costs have been imposed on, or losses caused to others, especially clients, market users or the investing public generally
- whether the conduct was intentional, reckless or negligent, including whether prior advice was sought on the lawfulness or acceptability of the conduct either by a firm from its advisors or by an individual from his or her supervisors or relevant compliance staff of the firm or group that employs him or her
- the duration and frequency of the conduct
- whether the conduct is widespread in the relevant industry (and if so, for how long) or there are reasonable grounds for believing it to be so widespread
- whether the conduct was engaged in by the firm or individual alone or whether as part of a group and the role the firm or individual played in that group
- whether a breach of fiduciary duty was involved
- in the case of a firm, whether the conduct reveals serious or systematic weaknesses, or both, in respect of the management systems or internal controls in relation to all or part of that firm's business
- whether the SFC has issued any guidance in relation to the conduct in question
- whether the conduct has facilitated or occasioned any offence or whether an offence is attributable to the conduct

The amount of profits accrued or loss avoided

- a firm or individual and related parties should not benefit from the conduct

Other circumstances of the firm or individual

- a fine should not have the likely effect of putting a firm or individual in financial jeopardy. In considering this factor, the SFC will take into account the size and financial resources of the firm or individual. However, if a firm or individual takes deliberate steps to create the false appearance that a fine will place it, him or her in financial jeopardy, eg, by transferring assets to third parties, this will be taken into account
- whether a firm or individual brings its, his or her conduct to the SFC's attention in a timely manner. In reviewing this, the SFC will consider whether the firm or individual informs the SFC of all the conduct of which it, he or she is aware or only part, and the manner in which the disclosure is made and the reasons for the disclosure
- the degree of cooperation with the SFC and other competent authorities[3]
- any remedial steps taken since the conduct was identified, including any steps taken to identify whether clients or others have suffered a loss and any steps taken to sufficiently compensate those clients or others, any disciplinary action taken by a firm against those involved and any steps taken to ensure that similar conduct does not occur in future
- the previous disciplinary record of the firm or individual, including an individual or firm's previous similar conduct particularly that for which it, he or she has been disciplined before or previous good conduct
- in relation to an individual, his or her experience in the industry and position within the firm that employed him or her

[3] See Guidance Note on Cooperation with the SFC published by the SFC.

Other relevant factors, including

- what action the SFC has taken in previous similar cases – in general similar cases should be treated consistently
- any punishment imposed or regulatory action taken or likely to be taken by other competent authorities
- result or likely result of any civil action taken or likely to be taken by third parties – successful or likely successful civil claims may reduce the part of a fine, if any, that is intended to stop a person benefiting from their conduct.

Appendix E

List of respondents

(in alphabetical order)

1. Accumulus GBA Technology (Hongkong) Co., Ltd.
2. Aimichia Technology Co., Ltd.
3. Alphalex Capital Management (HK) Limited
4. Amber Group
5. Angus Sze
6. Animoca Brands Limited
7. Asia Crypto Alliance
8. Asia Securities Industry and Financial Markets Association
9. Authento
10. Baker & McKenzie
11. BGE
12. Binance.com
13. BitGo
14. Bitquant Digital Services
15. Boswell Capital Management Limited
16. BTC Shop Hong Kong
17. CFA Society Hong Kong
18. Cherry Wong
19. Chi Zhang
20. Coded Solution
21. Coinbase Global, Inc.
22. ComplianceOne Consulting Limited
23. CompliancePlus Consulting Limited
24. Consumer Council

25. Crypto HK Limited
26. Custonomy Company Limited
27. DAB Kowloon City Branch
28. Daniel Lui
29. DEFINIS
30. DLA Piper Hong Kong
31. Elliptic
32. Fangda Partners
33. Financial Services Research Group
34. FinTech Association of Hong Kong
35. Fireblocks
36. FORMS Syntron Information (HK) Co. Ltd.
37. Hao Cui
38. Hauzen LLP
39. Henry Yu & Associates
40. Hex Trust Limited
41. Hippo Financial Services Limited and the Gate group of companies
42. HKBA.Club
43. HKFAEx Group Limited
44. HKVAEX
45. Hong Kong Digital Asset Ex Limited
46. Hong Kong Digital Asset Society
47. Hong Kong Digital Assets Group in Deloitte Touche Tohmatsu and Beosin Technology Limited
48. Hong Kong General Chamber of Commerce
49. Hong Kong Institute of Certified Public Accountants
50. Hong Kong Securities and Futures Professionals Association
51. Hong Kong Securities Association

52. Huobi
53. Institute of Financial Planners of Hong Kong
54. ISACA China Hong Kong Chapter
55. iSunCrowd Limited
56. Joseph Chow, Du Jinsong and Iu Kwan Yuen
57. Kaiko
58. Kaiser Securities Limited
59. King & Wood Mallesons
60. KPMG Advisory (Hong Kong) Limited
61. Latham & Watkins LLP
62. Linklogis International Company Limited
63. MaiCapital Limited
64. Man Ho Allen Au, Xiapu Luo and Paul Li
65. Matrixport
66. Mikołaj Barczentewicz
67. Mr. Chan
68. Mr. Hinson
69. Mulana Investment Management Limited
70. New Huo Technology Holdings Limited
71. Newton Wong
72. Nicholas Lo
73. Norton Rose Fulbright
74. Notabene Inc.
75. OKG Technology Holdings
76. OKX Hong Kong Fintech Company Limited
77. OneDegree Hong Kong Limited
78. OSL Digital Securities Limited

79. PricewaterhouseCoopers and Tiang & Partners
80. Prosynergy Consulting Limited
81. QReg Advisory Limited
82. Rakkar Digital (Hong Kong) Limited
83. Ripple Labs Inc.
84. Safeheron
85. Shawn Chang
86. Stevenson, Wong & Co.
87. Stratford Finance Limited
88. Thales
89. The Alternative Investment Management Association
90. The British Chamber of Commerce in Hong Kong
91. The Capital Markets Company Ltd.
92. The Chinese Gold and Silver Exchange Society
93. The Hong Kong Chartered Governance Institute
94. The Hong Kong Licensed Virtual Asset Association
95. The Law Society of Hong Kong
96. TKX Capital and Mura Consultancy
97. UD Blockchain
98. Vaultavo Inc.
99. Venture Smart Financial Holdings Limited
100. VerifyVASP
101. Victory Securities Group and Hong Kong Digital Assets Group in Deloitte Touche Tohmatsu
102. Vincent Tam
103. Xiang Li
104. Yuky Yu
105. zkMe Technology Limited

106. 白展堂

107. 谷炎

108. 東方文化控股有限公司

109. 香港南雅貨幣交易所

110. 章濤

111. 張明德

112. 張健恩

113. 貴州美酒鏈科技有限公司

114. 譚先生

115. Submissions of 25 respondents are published on a “no-name” basis upon request

116. Submissions of 13 respondents are withheld from publication upon request