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

Report on the review of licensed corporations providing online brokerage, distribution and advisory services

August 2022

Contents

I) Executive summary

1. The Securities and Futures Commission (SFC) conducted a review of licensed corporations (LCs) which provide brokerage, distribution and advisory services via online platforms. In particular, the review focused on LCs' compliance with regulatory requirements when onboarding clients and distributing or advising on investment products via their online platforms. The review was conducted in various ways including via a fact-finding survey, desktop analysis and inspections.

2. By publishing this report, the SFC wishes to share the observations and findings of the review with the industry so that LCs may benchmark themselves against their peers and be mindful of the deficiencies identified from the review. LCs are also reminded of the regulatory standards expected of them when providing these services online.

3. The SFC's key observations of the LCs' business models are set out in Part II of this report and summarised below:

    - 96% of new accounts opened by the 50 surveyed LCs within a 12-month period were through non-face-to-face (Non-FTF) client onboarding approaches;

    - apart from commonly traded products such as equities, exchange traded funds (ETFs), collective investment schemes (CISs), and futures and options contracts, some LCs offered other services through their online platforms such as small-value cash investments and robo-advisory;

    - for a better customer experience, some LCs' online platforms featured special functions, including technical analysis of stocks to facilitate investors' market research and investments in a self-directed environment, as well as game-like features to interest investors in using their platforms. The use of social media platforms for marketing and communication was also popular; and

    - LCs conducting regulated activities online generally invested more heavily in their platforms and systems and charged lower trading fees. On the other hand, LCs which were less online-centric put more emphasis on personalised client services, as evidenced by their higher average numbers of licensed staff per client.

4. Compliance issues identified from the review are set out in Part III of this report. Key concerns include:

    - failure to conduct proper client identity verification procedures to mitigate impersonation risks when onboarding clients through online platforms, for example, deficiencies in recognising clients' designated bank accounts in Hong Kong and not adopting independently assessed technology to authenticate clients' identity documents when onboarding overseas clients;

    - despite already implementing mechanisms to fulfil their suitability obligations, some LCs appeared to have excluded their potential suitability obligations by including clauses and statements in client agreements and risk disclosures, and requesting their clients to make a blanket acknowledgement that no solicitation or recommendation was provided by the LCs. This may be seen as attempting to restrict

clients' rights, exclude the obligations of the LCs, or misdescribe the actual services provided to the clients;

- insufficient product due diligence (PDD) to properly assess the key features and risks of the products and failure to observe the selling restrictions or additional regulatory requirements when distributing certain investment products, such as virtual asset-related products[1] (VA-related products);

- inadequate measures to identify and assess inconsistent client information or to detect abnormal frequent updates of client's risk profile questionnaire during the know your client (KYC) process;

- lack of proper monitoring mechanism in reviewing the information and commentaries posted by an LC or its affiliates on the online platform so as to ensure that they are accurate and not misleading; and

- failure to implement adequate mechanisms to mitigate cybersecurity risks, including the factors adopted for two-factor authentication (2FA), monitoring and surveillance to detect unauthorised access to clients' internet trading accounts, channels to promptly notify clients after certain client activities, and session timeout.

5. As more retail investors use online platforms for investing, it is crucial for LCs to ensure that their online platforms are properly designed, secured and operate in compliance with all applicable rules and regulations. LCs should be mindful of the compliance issues noted by the SFC and observe the expected standards as set out under Part IV of this report.

6. The SFC will keep abreast of market developments and emerging risks associated with LCs conducting regulated activities online and will provide further guidance when necessary.

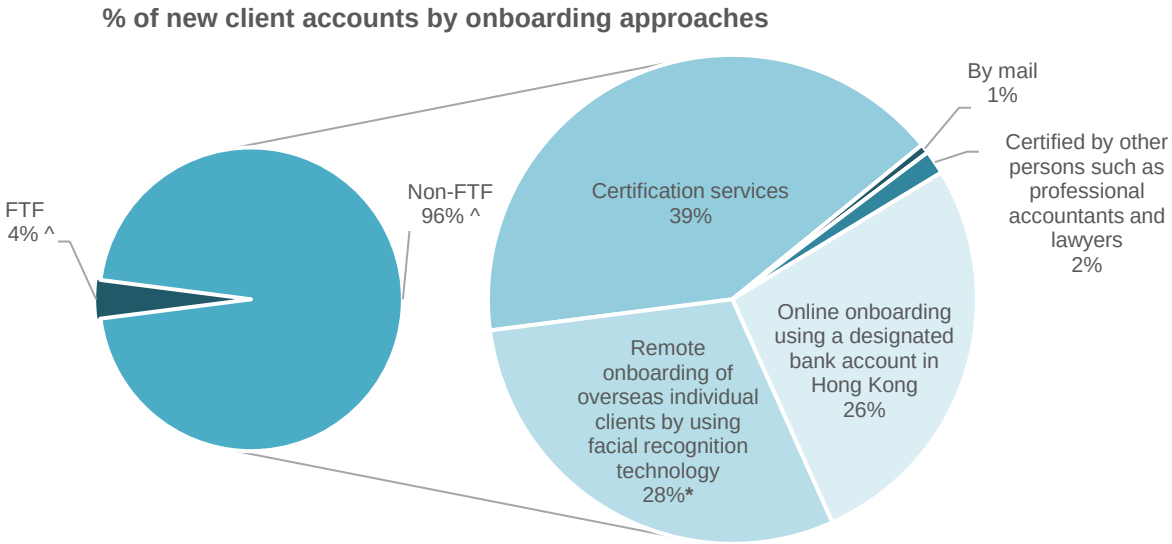
[1] Please refer to the Joint circular on intermediaries' virtual asset-related activities issued on 28 January 2022 (VA Circular) for the definitions of "virtual asset" and "virtual asset-related products".

II) Licensed corporations' business models

7. The SFC conducted a survey of 50 LCs which provided brokerage, distribution and advisory services online to retail investors to understand their business models. Observations are as follows:

A. Client onboarding

(i) A total of over 3,000,000 new client accounts were opened by the surveyed LCs from July 2020 to June 2021 (Relevant Period). Non-FTF client onboarding approaches were popular among the surveyed LCs. About 96% of the new accounts were opened using these approaches.



^ Face-to-face (FTF) approach means that account opening documents were executed in the presence of an employee of an LC. Non-FTF approach means that these documents were not executed in the presence of an employee of the LC.

* This refers to the remote onboarding approach set out in the circular to intermediaries on 28 June 2019. The 28% is mainly contributed by one LC.

(ii) Among the Non-FTF approaches adopted by the LCs, the use of certification services, the designation of a bank account in Hong Kong and the application of facial recognition technology to match clients' biometric data against their identity documents were preferred by investors in the age group of 25 to 34.

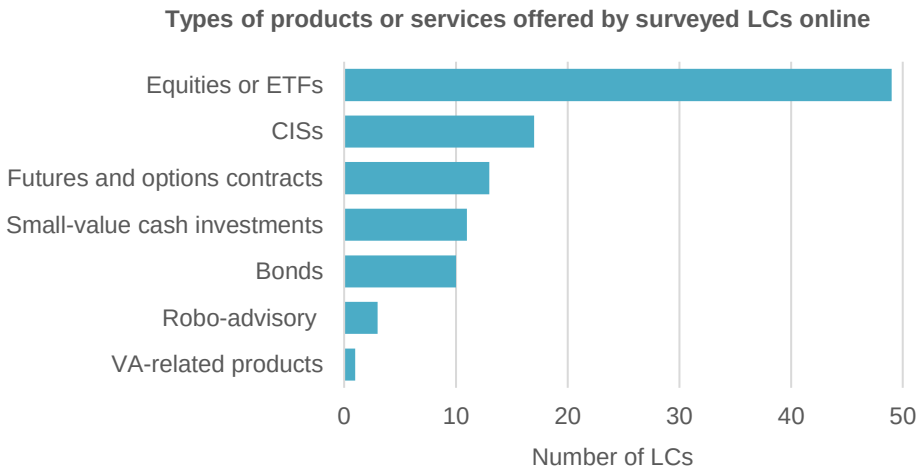
(iii) The surveyed LCs provided various types of incentives (such as commission rebate, fee discount, cash reward and gift stocks) to attract new clients and commission rebate was most common. A total of 45 (or 90%) of them also provided online account opening channels to facilitate efficient client onboarding.

(iv) For the top five surveyed LCs in terms of the number of new client accounts opened during the Relevant Period, they opened a total of over 2,000,000 new client accounts, of which 98% were opened using Non-FTF client onboarding

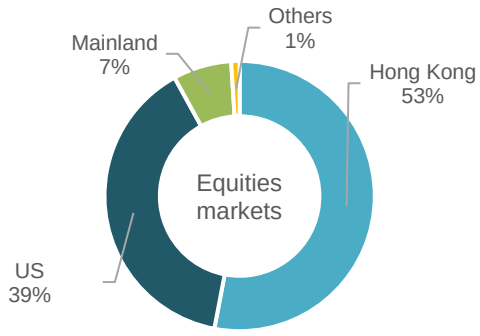
approaches. On average, each of these LCs opened over 10,000 new client accounts every month during the Relevant Period.

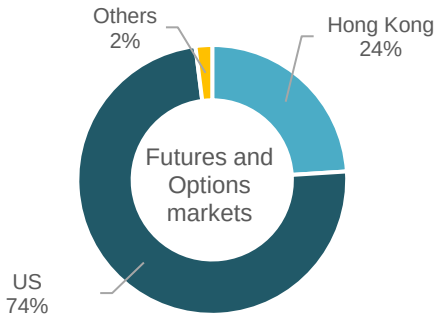
B. Online trading, distribution and marketing

(a) Products and markets



(i) 49 LCs surveyed (or 98%) supported online trading of equities or ETFs, of which 13 LCs also provided online trading of futures and options contracts. The major equities markets participated by the surveyed LCs included Hong Kong, the US and Mainland which represented about 53%, 39% and 7% of the total turnover respectively. The major futures and options markets were the US and Hong Kong, accounting for 74% and 24% of the total number of contracts executed respectively.





(ii) 22 LCs surveyed (or 44%) conducted selling and distribution of CISs or bonds through their online platforms.

(iii) 11 LCs surveyed (or 22%) offered small-value cash investment service via online platforms for clients who wanted to invest their idle cash for a short period of time. Most of these LCs placed clients' excess cash in money market funds authorised by the SFC.

(iv) Three LCs provided robo-advisory services on CISs or ETFs via their online platforms.

(b) Special functionalities

LCs offered special functionalities on their online platforms to improve customer experience and attract more investors to use these platforms.

(i) *Market data and analysis*
Over half of the surveyed LCs provided information of listed companies, financial news, market or data analytical tools (eg, technical analysis of stocks and trend analysis of market fund flow), and market commentaries via their online platforms. Other popular features included IPO stock analysis, stock price or trading volume alerts, risk profiling and investment filtering. This helped investors conduct research and do their own analysis for investment purpose.

(ii) *Instant customer services*
27 LCs surveyed provided live chat functions and 14 of them provided automated artificial intelligence (AI) chatbots in addition to traditional customer services via hotlines and email.

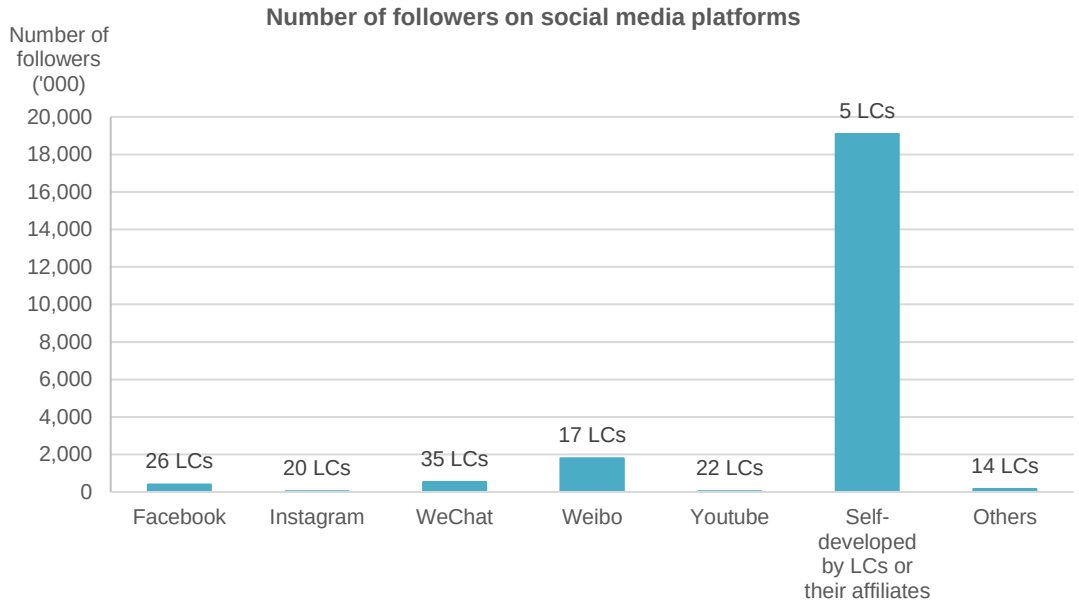
(iii) *Gamification features*
The SFC noted an emerging trend of LCs embedding game-like features (commonly referred to as gamification) to raise users' interest in using online platforms, and social media functions which allow LCs' staff and affiliates as well as other investors to create online communities to share information, ideas, personal messages and other contents (eg, videos).

(c) Social media platforms

The SFC observed that LCs increasingly used social media platforms for marketing and communication purposes.

(i) 43 LCs surveyed (or 86%) used self-developed or third-party operated social media platforms for communication with clients and marketing activities, such as posting commentaries or information relating to investment products; and

(ii) the most popular platform was Weibo, followed by WeChat and Facebook in terms of numbers of followers, aside from self-developed platforms of five LCs.



C. Comparison of business models of Pure Online Brokers and Hybrid Brokers

The use of online platforms provided a self-directed and user-friendly environment which enhanced customer experience. It was noted that half of the surveyed LCs had over 80% of client orders and total turnover derived from their online platforms during the Relevant Period.

The SFC observed the following by comparing the business models of 13 LCs of which over 98% client orders were received online (Pure Online Brokers) and 11 LCs of which less than 50% client orders were received online (Hybrid Brokers):

(i) Many Pure Online Brokers indicated that having a powerful, efficient and user-friendly online trading platform was their competitive edge. To support system development and maintenance, including cybersecurity controls of their online systems, Pure Online Brokers generally invested more heavily in information technology (IT) as reflected from their relatively higher average IT budget (26% of their total annual budget as compared to 15% for Hybrid Brokers);

(ii) About 70% of Pure Online Brokers deployed live chats or AI chatbots on top of telephone hotlines and emails in providing customer support services while only 36% of Hybrid Brokers deployed similar technology;

(iii) Pure Online Brokers charged clients relatively lower average commission rates or trading fees (around 0.07% on Hong Kong listed stocks) as compared to Hybrid Brokers (0.14%); and

(iv) Hybrid Brokers with a longer history viewed good reputation as their strength. They generally placed more emphasis on maintaining client relationship by providing personalised services to clients. Hybrid Brokers employed more staff to carry out regulated activities. On average, a licensed staff served around 200 active clients for Hybrid Brokers as compared to about 4,000 for Pure Online Brokers.

Hybrid Broker A	Hybrid Broker B	Hybrid Broker C	Observations	Pure Online Broker D	Pure Online Broker E	Pure Online Broker F
Good reputation	Good reputation	Good reputation	**Top competitive edge viewed by the LC**	Powerful and user-friendly platform	Powerful and user-friendly platform	Powerful and user-friendly platform
13%	6%	1%	**% of IT budget to total annual budget**	54%	20%	60%
0.2%	0.16%	0.15%	**Average commission rate for Hong Kong listed stocks**	0.03%	0.05%	0.09%
124	102	48	**Average number of active clients served by each licensed person of the LC**	24,236	4,614	2,461

III) Compliance issues

8. The SFC wants to highlight the following compliance issues identified from the review.

A. Client onboarding

9. As mentioned in paragraph 7(A) of Part II, many LCs onboarded clients by adopting a Non-FTF account opening approach. Clients not physically present for onboarding generally pose a higher risk of impersonation and LCs should conduct proper procedures for client identity verification as specified in the acceptable account opening approaches published on the SFC website[2] to ensure compliance with paragraph 5.1 of the Code of Conduct[3]. For example,

   (a) when onboarding clients through a transfer of an initial deposit of not less than $10,000 from a bank account in a client's name maintained with a licensed bank in Hong Kong and execute all future deposits and withdrawals for the client through this designated bank account (Designated Bank Account Approach), reliance has been placed on the client identity verification performed by the licensed bank with which the designated bank account is maintained. Therefore, it is necessary for clients to complete the initial fund transfer and have all their subsequent deposits and withdrawals conducted through these designated bank accounts; and

   (b) where LCs adopted the approach of remote onboarding of overseas individual clients[4] (Overseas Clients Remote Onboarding Approach), reliance has been placed on the independent assessment conducted by qualified assessors to confirm that the adopted processes and technologies are appropriate and effective for establishing the true identities of clients. A proper pre-implementation assessment is necessary to ensure the technologies adopted by LCs can perform proper client identity verification and guard against security or fraudulent attacks such as identity theft.

(i) Deficiencies relating to client onboarding

Deficiencies and non-compliance
Designated Bank Account Approach (a) Failure to conduct deposits and withdrawals through a designated bank account in Hong Kong (i) An LC failed to identify some clients' initial fund transfers were from their bank accounts outside Hong Kong and accepted these overseas bank accounts as the clients' designated bank accounts for subsequent deposits and withdrawals.

[2] Please refer to the "Rules and standards > Account opening" section of the SFC website.
[3] Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (Code of Conduct).
[4] Approach referred in the circular to intermediaries regarding remote onboarding of overseas individual clients dated 28 June 2019 (Remote Onboarding Circular).

Deficiencies and non-compliance

(ii) Some LCs allowed their clients to conduct deposits and withdrawals through bank accounts other than their designated bank accounts in Hong Kong subsequent to account opening.

(b) Failure to obtain bank account details for client identity verification

An LC failed to obtain bank account details from its clients to confirm the ownership of the bank accounts from which the clients' initial transfers were made. In one case, the information provided by the receiving bank of the LC did not include the account number of a client's bank account held with the paying bank and the payment slip generated by the paying bank did not show the client's name or his full bank account numbers. The LC accepted the bank account as the client's designated bank account without obtaining further supporting evidence from the client (eg, the client's bank statement showing the full account name and account number).

Overseas Clients Remote Onboarding Approach

(c) Failure to authenticate the client's identity document (ID Document)

In adopting the Overseas Clients Remote Onboarding Approach, an LC matched the photo image on the clients' ID Document with the facial image of the clients in its facial recognition process without first checking the security features and hence the authenticity of the clients' ID Document.

(d) Failure to properly follow-up with clients who did not pass facial recognition tests

An LC onboarded clients who did not pass facial recognition tests in the account opening process without carrying out appropriate procedures to verify the clients' identity. The LC's staff merely conducted visual comparison of the facial image of the clients against the photo image on the ID Documents uploaded by the clients, instead of adopting other account opening approaches to verify these clients' true and full identity.

(e) Failure to make initial deposits or conduct future deposits and withdrawals through clients' designated overseas bank accounts

An LC did not require its clients to make an initial deposit of not less than $10,000 or equivalent amount in other currencies from the clients' bank account in an eligible jurisdiction or require the clients to conduct all future deposits and withdrawals of their investment accounts through their designated overseas bank accounts.

(f) Failure to procure proper pre-implementation assessment of remote onboarding processes and technologies

(i) An LC failed to engage an independent and qualified assessor to perform a pre-implementation assessment to evaluate the appropriateness and effectiveness of the processes and technologies it

Deficiencies and non-compliance

adopted for remote onboarding. Some other LCs conducted the assessment by their internal staff instead.

(ii) An LC has outsourced the procedures of client identity verification to a third-party service provider. However, the pre-implementation assessment performed by the LC's independent assessor failed to cover the facial recognition technology used by the service provider. Therefore, the reliability of the facial recognition technology and hence the appropriateness and the effectiveness of the adopted processes and technologies of the LC to establish the true identities of clients were not ascertained.

Use of certification services (Certification Service Approach)

(g) Use of certification authorities (CA) that were not recognised

An LC employed a certification service that was not provided by CA recognised under the Electronic Transactions Ordinance (ETO) nor by overseas CA whose electronic signature certificates have obtained mutual recognition status accepted by the HKSAR Government for client identity verification.

Other matters

(h) Approval of accounts opening prior to completion of client identity verification

Some LCs approved new client accounts before completing the identity verification procedures for onboarding. For example,

(i) an LC using the Certification Service Approach for client onboarding directed its clients to apply for electronic signature certificates from CA for identity verification after the LC had approved the clients' account opening; and

(ii) some LCs using Designated Bank Account Approach notified clients about the success or the completion of their account opening before the clients transferred the required initial deposits of not less than $10,000 from their bank accounts in Hong Kong to the LCs' bank accounts.

(i) Absence of client address verification

When onboarding clients online, some LCs failed to obtain address proof from clients before executing their orders involving securities and futures contracts listed or traded on a recognised market[5].

[5] Paragraph 5.4(a) of the Code of Conduct and paragraph 30 of the guidelines set out in the Client Identity Rule Policy published by the SFC.

B. Online trading, distribution and marketing

10. In an environment of self-directed trading created by online platforms, retail investors would navigate the information available and place orders by themselves. As investors may heavily rely on the information provided on the online platforms in making investment decisions, it is crucial for LCs to ensure that the information is accurate and not misleading.

11. LCs should adhere with the requirements under the Guidelines on Online Distribution and Advisory Platforms (Online Platform Guidelines) when conducting regulated activities in providing order execution, distribution or advisory services in respect of investment products via online platforms, particularly on the six core principles covering (i) proper design, (ii) information for clients, (iii) risk management, (iv) governance, capabilities and resources, (v) review and monitoring and (vi) record keeping.

12. While LCs may operate different websites, platforms and other channels such as social media accounts for posting information about investment products and transacting in them, the SFC will take into account activities targeting Hong Kong investors conducted by LCs via all channels in their totality in considering the LCs' compliance with the requirements in the Online Platform Guidelines[6].

(a) Suitability and disclosure obligations

13. Under certain circumstances, suitability obligations may also be triggered on the online platform environment. Therefore, LCs should be mindful of their representations to clients in this regard, and take all necessary steps to comply with the requirements related to suitability obligations.

14. The SFC hereby highlights the following non-compliance issues in relation to suitability obligations and information to clients.

(i) Inappropriate clauses and statements under client agreement and acknowledgement of risk disclosure

15. For some of the inspected LCs, the design and overall impression created by the content of their online platforms appeared to indicate that these LCs had made solicitations or recommendations to the clients. Although these LCs had implemented mechanisms to fulfil their suitability obligations, they had also requested their clients to make a blanket acknowledgement that the LCs did not make any solicitations or recommendations to the clients in the client agreements and risk disclosure statements upon onboarding, before allowing the clients to view certain pages of the online platforms, or before they can proceed to trade execution. This approach appears to be an attempt to exclude any potential suitability obligations that the LCs may have over their activities on the online platforms. This may result in a breach of paragraph 6.3[7] of the Code of Conduct.

---

[6] The Note to paragraph 1.1 of the Online Platform Guidelines.

[7] Paragraph 6.3 of the Code of Conduct requires a licensed or registered person to ensure it complies with its obligations under a Client Agreement, as defined in the Code of Conduct, and that a Client Agreement does not operate to remove, exclude or restrict any rights of a client or obligations of the licensed or registered person under the law.

16. Whether an LC has made a "solicitation" or "recommendation" on its online platform is a question of fact which should be assessed in light of all the circumstances leading up to the point of sale or advice in each specific case. Where a solicitation or recommendation has in fact been made, the aforementioned client's acknowledgement would be inappropriate and misdescribe the actual services provided to clients. This may result in a breach of paragraph 6.5[8] of the Code of Conduct.

Deficiencies and non-compliance

(a) <u>Clauses and statements which might have restricted client's rights, excluded LC's obligations, or misdescribed LC's services</u>

Some LCs have adopted the following practices which may amount to provision of solicitations or recommendations:

(i) two LCs applied some internal assessment and shortlisted funds to be made available on certain parts of their platforms after taking into account various factors such as scoring of the funds, number of client views, comments and subscriptions;

(ii) some LCs offered predefined model investment portfolios on the online platforms; and

(iii) an LC would post commentaries to the "news" or "commentary" page of the online platform with specific investment products tagged, which could direct a client to the product page and then the order execution page where the client could place an order to purchase the tagged investment product.

While these LCs have implemented mechanisms to fulfil their suitability obligations, eg, conducted suitability assessment via their online platforms prior to trade executions, they would also add terms, clauses or statements in the client agreements and risk disclosures which stated, for example:

[8] Paragraph 6.5 of the Code of Conduct stipulates that a licensed or registered person should not incorporate any clause, provision or terms in the Client Agreement, as defined in the Code of Conduct, or in any other document signed or statement made by the client at the request of the licensed or registered person which is inconsistent with its obligations under the Code of Conduct or misdescribes the actual services to be provided to the client.

Deficiencies and non-compliance

(i) information provided cannot be used as a basis for making any investment decision;

(ii) the materials or information provided shall not, by themselves, constitute solicitation or recommendation; or

(iii) any information provided by the LC is for general reference only and is not intended as investment advice or for any other purpose,

and requested clients to provide a blanket acknowledgement.

These would appear to restrict the clients' rights to make decisions based on the information provided, exclude the LCs' potential suitability obligations, or misdescribe the actual services provided to clients, and are contrary to paragraphs 6.3 and 6.5 of the Code of Conduct.

(b) Failure to include minimum content of client agreement

An LC failed to include certain clauses in the client agreement as stipulated under paragraph 6.2(h) of the Code of Conduct and paragraph (f) of Appendix 1 to the Fund Manager Code of Conduct regarding the minimum content of a client agreement and a discretionary client agreement, respectively.

(c) Inadequate modification of "suitability clause" under the Code of Conduct

An LC had modified the required wording of the "suitability clause" under paragraph 6.2(i) of the Code of Conduct in its client agreement which may result in deviation from the substance of the clause.

(ii) Insufficient PDD

17. In selecting investment products to be made available on online platforms, it is crucial for LCs to conduct proper due diligence to understand the investment products, taking into account their features and risks. Our review found that some inspected LCs failed to conduct adequate PDD on certain investment products. As a result, the product risk rating might not be an accurate reflection of the underlying risks of the products being offered.

Deficiencies and non-compliance

(a) An LC determined the risk ratings of bonds based on the credit ratings, yield to maturity (YTM) and some special features of the bonds. However, it did not take into account other factors such as the financial conditions of the product issuer and guarantor. Also, the benchmark for YTM was set so high that in general, only distressed debts with a dramatic drop in price would be classified as "high" risk.

Deficiencies and non-compliance
(b) An LC failed to provide rationale or justification for supporting its conclusion of including a bond on its approved product list, despite the various risks identified during the PDD (eg, the issuer was a non-operating firm and the guarantor incurred significant drop in sales, increasing indebtedness and deteriorating liquidity). The bond issuer announced its default on some of its loans three months after the LC approved and made available the bond on its online platform. The LC then removed the bond from its approved product list. (c) For an unauthorised fund with a complex structure, an LC was unable to demonstrate that it had assessed certain key aspects of the fund, including the investment and risk management processes of the fund manager, the valuation and safe custody arrangements of the fund, and some of the underlying risks of the fund. (d) In assessing the risk rating of a bond fund, an LC would take into account the lowest credit rating of the permissible bonds in a bond fund. It, however, did not take into account factors such as the fund's investment objectives and strategies. As a result, a high-yield bond fund and a non-high-yield bond fund issued by the same fund house were rated as "low" risk by the LC.

(iii) Failure to observe selling restrictions or additional regulatory requirements applicable to specific products

18. As mentioned in paragraph 7(B)(a) under Part II, LCs offer different types of products on their online platforms and retail investors could have access to these products easily on the platforms. Unless authorised by the SFC, private funds can only be sold to professional investors. LCs should also observe the applicable restrictions when distributing bonds, eg, non-retail bonds are distributed relying on the exemptions for prospectus-related provisions under the Companies (Winding Up and Miscellaneous Provisions) Ordinance. However, some LCs failed to observe the selling restrictions or additional regulatory requirements when distributing complex or unauthorised products to investors.

19. The SFC noted that one of the inspected LCs offered some VA-related products trading through overseas over-the-counter markets on its online platform to retail investors and failed to observe the relevant regulatory requirements. Given there are various risks associated with investing in virtual assets which are not reasonably likely to be understood by retail investors under certain circumstances, LCs are required to implement additional investor protection measures. For example, LCs should observe the requirements as set out under the VA Circular when distributing VA-related products to investors, including the selling restrictions and virtual asset-knowledge test.

(iv) Inadequate client risk profiling

20. As part of the KYC process to assess clients' risk appetite, some LCs adopted a client risk profiling tool, including a risk-scoring questionnaire, to help clients determine their risk tolerance levels and make investment decisions. However, some LCs failed to put in

place proper mechanisms to identify and assess inconsistent client information or to prevent or detect frequent abnormal changes to clients' risk profile questionnaires (RPQs) as illustrated under the "*Deficiencies and non-compliance*" boxes below. Performing client risk profiling based on inaccurate or insufficient client information would cast doubts on the tool's effectiveness in assessing the risk tolerance levels of clients.

Deficiencies and non-compliance

(a) Inconsistent client information

Many LCs required their clients to complete more than one questionnaire or form during the KYC process, either in the web-based or paper format, or a combination of both. It was noted that some questionnaires or forms contain similar questions but with different choices available to clients. This resulted in some clients providing inconsistent information to the LCs. Some LCs were not aware of these inconsistencies and failed to take any follow-up actions.

(b) Frequent updates of RPQ by clients with conflicting information

Some clients of an LC seemed to be able to game the risk profiling tool in order to get access to high-risk products. In one extreme case, an investor had updated the RPQ eight times within one hour and provided inconsistent information in each round of update. Ultimately, the investor was able to obtain a higher risk tolerance classification and purchase investment products rated as higher risk. The LC has failed to implement an effective mechanism to prevent or detect abnormal frequent updates on the RPQ or inconsistent information provided by clients. It is questionable whether the risk profiling process has properly functioned to reflect the genuine risk tolerance levels of clients.

(v) Other matters related to disclosure of information to clients

Deficiencies and non-compliance

(a) Insufficient disclosure of product information and risk rating methodology

(i) An LC failed to provide sufficient information on the key nature, features and risks of an unauthorised fund which was treated as a complex product[9], in particular the risks associated with its underlying investments.

(ii) Another LC failed to make available information of the methodology adopted for assessing and assigning ratings to investment products and categorising clients.

(b) Improper disclosure of monetary and non-monetary benefits

(i) Some LCs made uniform disclosure of the maximum percentage of trailer fees receivable by them based on all funds on their distribution

[9] As defined under paragraph 6.1 of the Online Platform Guidelines.

Deficiencies and non-compliance
lists instead of making specific disclosure for a particular fund on a transaction basis. (ii) An LC disclosed the maximum percentage of commission rebates receivable by it based on all bonds on its distribution list instead of individual bonds.

(b) Additional functionalities and use of social media to enhance client experience

21. Paragraph 7(B)(b) and (c) of Part II illustrated that LCs are applying various innovative ways to distribute investment products and market their online platforms. While these new features and approaches may bring convenience to retail investors, certain risks or issues associated with them were noted.

(i) Risk of posting inaccurate and misleading information and commentaries on online platforms

22. Our review found that an inspected LC could not demonstrate that it had a proper mechanism in place to ensure any commentaries or information posted by its staff or affiliates on its online platform are accurate and not misleading.

Deficiencies and non-compliance
The staff of an LC and its affiliated companies would post commentaries on its online platform. In some occasions, specific investment products were tagged in the commentaries which could direct clients to the product and then the order execution pages. However, the LC failed to provide any documentation demonstrating that it had a mechanism in place to ensure these commentaries, representations made and information provided are accurate and not misleading.

(ii) Potential compliance issues relating to solicitation of overseas clients

23. Some LCs might have promoted their services or solicited new clients outside Hong Kong through online platforms or applications provided and operated by unregulated third parties. Depending on the arrangements of each case, these practices may amount to cross-border solicitation of clients, opening of client accounts or marketing of investment products, which may constitute unlicensed activities in the relevant overseas jurisdictions. LCs failing to consider how the law of the other jurisdiction applies to the particular activities before conducting those activities may expose themselves to the risk of breaching the requirements of that jurisdiction.

C. <u>Cybersecurity</u>

24. As LCs are providing more and more value-added functionalities to clients on the online platforms, clients will likely build up a significant level of loyalty and reliance in using these platforms. Consequently, any information security breaches or system operation interruptions could be detrimental to the reputation or sustainability of the operation of

LCs and may cause losses and damages to clients. In this regard, the SFC wants to highlight the following issues noted from the review.

Deficiencies and non-compliance
(a) LCs are expected to implement 2FA for login to clients' internet trading accounts[10]. Some LCs adopted email OTP as the second authentication factor, that is, "what a client has" for logging into the clients' internet trading accounts of the online platforms. However, LCs should not deliver OTPs via email because security protection for email accounts is generally inadequate. An email OTP can be delivered to multiple devices and may not always be directed to the client. If the transaction is being conducted via an online platform, LCs should use an alternative means to deliver the password[11]. Separately, some LCs only required clients to activate the internet trading function after session timeout by inputting the login password without implementing 2FA. (b) An LC failed to implement any monitoring and surveillance mechanism such as the use of exception reports and real-time alerts to detect unauthorised access to clients' internet trading accounts[12]. Another LC failed to explain the basis supporting the appropriateness of the parameters and thresholds used in the monitoring tools to generate exception reports to detect unauthorised access to clients' internet trading accounts. (c) In providing prompt notifications to clients after certain client activities[13], some LCs did not use a different notification channel from the one used for delivering OTP for system login. (d) Some LCs allowed clients to either disable the session timeout after a period of inactivity or choose a long idle timeout period (eg, over 30 minutes after a period of inactivity). This is not satisfactory because there is an increased risk of unauthorised access when an attacker has unlimited time or an unduly long period of time for hacking attempts.

[10] 2FA refers to an authentication mechanism which utilises any two of the following factors: what a client knows (eg, user ID and password), what a client has (eg, one-time password (OTP) delivered via short messaging service to a client's designated mobile device, OTP generated from hardware token provided to a client, or device binding or registration), and who a client is (eg, biometric authentication).

[11] Please refer to paragraphs 11 and 12 of the Report on the 2019-20 thematic cybersecurity review of internet brokers (Cybersecurity Thematic Review Report) for details.

[12] These include detecting abnormal changes in the internet protocol addresses from which clients login, for example from a different country or city within a short period of time.

[13] Including system login, password reset, changes to client and account related information and trade execution.

IV) Expected standards

25. To address the issues and concerns mentioned above, LCs should be mindful in adhering with the SFC requirements when conducting their regulated activities on the online platforms, in particular:

    (a) the relevant requirements stated in the acceptable account opening approaches published on the SFC website and the Remote Onboarding Circular;

    (b) the Online Platform Guidelines and related Frequently Asked Questions (FAQs); and

    (c) the relevant requirements regarding cybersecurity, in particular the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (Cybersecurity Guidelines)[14], the Circular to licensed corporations on review of internet trading cybersecurity and the Cybersecurity Thematic Review Report[15].

26. LCs are reminded to meet our expected standards in relation to the issues and concerns mentioned above. They should appropriately review all the activities conducted on the online platforms as part of their ongoing supervision and monitoring obligation[16] and ensure compliance with the requirements.

A. Client onboarding

(i) Deficiencies relating to client onboarding

Expected regulatory standards
LCs should take all reasonable steps to establish the true and full identity of each client[17] and make reference to the requirements in the acceptable client onboarding approaches as published on the SFC website. In particular, for the deficiencies described under Part III of this report, LCs are reminded to comply with the following regulatory standards: ***Designated Bank Account Approach*** (a) implement appropriate measures to ensure proper designation of a bank account through successful transfers of an initial deposit of not less than $10,000 from a bank account in the client's name maintained with a licensed bank in Hong Kong to the LC's bank account, and conduct all future deposits and withdrawals for the client's trading account through that designated bank account[18]; (b) obtain satisfactory evidence to confirm any transfer of initial deposit is made from the relevant client's bank account[19];

[14] Including the FAQs on Cybersecurity published by the SFC on 27 October 2017.
[15] Published by the SFC in September 2020.
[16] Paragraph 2.6 of the Online Platform Guidelines.
[17] Paragraph 5.1 of the Code of Conduct.
[18] Paragraphs 4(ii) and (iii) of the acceptable account opening approaches published on the SFC website.
[19] Footnote 6 of the acceptable account opening approaches published on the SFC website.

Expected regulatory standards

Overseas Clients Remote Onboarding Approach

(c) employ appropriate and effective processes and technologies to authenticate ID Documents of clients[20];

(d) use appropriate and effective processes and technologies to identify and verify client's identity against authenticated ID Documents;

(e) procure the transfer of an initial deposit of not less than $10,000 or an equivalent amount in other currencies to the LC's bank account from an overseas bank account in client's name maintained with a bank which is supervised by a bank regulator in an eligible jurisdiction[21]. The client should conduct all future deposits and withdrawals for his or her investment account through that designated overseas bank account[22];

(f) conduct a comprehensive assessment by competent and qualified assessors to evaluate the appropriateness and effectiveness of the adopted processes and technologies prior to implementation and at least annually after implementation, and ensure that the minimum scope of assessment set out in the Remote Onboarding Circular are properly covered in the pre-implementation assessment report[23]. The SFC generally expects the pre-implementation assessment to be performed by independent assessors;

Certification Service Approach

(g) employ certification services provided by certification authorities recognised by ETO or obtained mutual recognition status accepted by the HKSAR Government[24];

Other matters

(h) Approval of client account opening

LCs should approve the opening of new client accounts only after completing proper client identity verification and other KYC procedures; and

(i) Verification of client address

LCs should be satisfied on reasonable ground about the address of a person or entity ultimately responsible for originating the instructions for a transaction which involves securities or futures contracts listed or traded on a recognised market or a derivative written over these securities or futures contracts, and keep a record of the details[25].

[20] Paragraph 1 of the Remote Onboarding Circular.
[21] The list of eligible jurisdictions is available on the SFC's website.
[22] Paragraph 4 of the Remote Onboarding Circular.
[23] Paragraph 7 of the Remote Onboarding Circular.
[24] Paragraph 2 of the acceptable account opening approaches published on the SFC website.
[25] Paragraph 5.4 of the Code of Conduct.

B. Online trading, distribution and marketing

(a) Suitability and disclosure obligations

(i) Inappropriate clauses and statements under client agreement and acknowledgement of risk disclosure

Expected regulatory standards

(a) Clauses and statements which might have restricted client's rights, excluded LC's obligations, or misdescribed LC's services

The question of whether there has been a "solicitation" or "recommendation" triggering the suitability obligations is a question of fact which should be assessed in light of all the circumstances leading up to the point of sale or advice. The context (eg, the manner of presentation) and content of product-specific materials posted on an online platform coupled with the design and overall impression created by the content of the online platform would determine if the suitability obligations are triggered[26].

Where a solicitation or recommendation has in fact been made, the client's acknowledgement that no solicitation or recommendation is made by the LC would be inappropriate.

Even if there is no solicitation or recommendation, the client agreement or risk disclosure statement of the LC should not state that the information provided cannot be used as a basis for making any investment decision.

LCs need to ensure that any information provided to the client is accurate and not misleading in accordance with paragraph 2.1 of the Code of Conduct, as clients may use that information as a basis for making investment decisions. LCs cannot restrict the clients' rights to make their own investment decision based on the information provided.

LCs should review their client agreements and other client documentations to ensure that the clauses contained therein would not restrict any rights of their clients, exclude the LCs' obligations under the law, or misdescribe the actual services provided to clients[27].

(b) Failure to include minimum content of client agreement

LCs should also make reference to the requirements as stipulated under the Code of Conduct and the Fund Manager Code of Conduct[28] when determining the clauses and statements to be included in the client agreement and risk disclosure.

[26] Paragraph 5.3 of the Online Platform Guidelines.
[27] Paragraphs 6.3 and 6.5 of the Code of Conduct.
[28] Paragraph 6.2 of the Code of Conduct and the Minimum Content of Discretionary Client Agreement section of Appendix 1 to the Fund Manager Code of Conduct.

(ii) Insufficient PDD

Expected regulatory standards
LCs should act with due skill, care and diligence when selecting investment products to be made available on their online platforms and when posting any information and materials on their online platforms[29]. In particular, LCs are reminded to comply with the Suitability FAQs[30] and the Circular to intermediaries regarding distribution of complex and high-risk products[31]. They should conduct their own PDD and arrive at their own assessment of the products by taking into account all relevant information which is appropriate and reasonably available for a fair assessment.

(iii) Failure to observe selling restrictions or additional regulatory requirements applicable to specific products

Expected regulatory standards
LCs should be mindful of the statutory requirements and regulatory expectations when distributing investment products. For example, they should observe the requirements as set out under the VA Circular when distributing VA-related products to investors.

(iv) Inadequate client risk profiling

Expected regulatory standards
LCs are required to, among other things, exercise due skill, care and diligence to ensure the methodology for risk profiling its clients is properly designed[32]. LCs are also required to establish appropriate governance and supervisory mechanisms for the client profiling tool provided on their online platforms, if any, and identify the key elements of information necessary to accurately profile a client[33]. In addition, where a client provides inconsistent answers in any online client profiling tool, the LCs should have a proper mechanism in place to identify the inconsistencies[34]. If a client provides conflicting or incomplete information, a licensed or registered person should alert the client and seek clarification from the client before performing suitability assessment[35].

[29] Paragraph 2.2(ii)(a) of the Online Platform Guidelines.
[30] Answer to question 4 of the Frequently Asked Questions on Compliance with Suitability Obligations by Licensed or Registered Persons (Suitability FAQs).
[31] Issued by the SFC on 7 December 2018.
[32] Paragraph 2.2(iv) and Chapter 5 of the Online Platform Guidelines. Also see the answer to question 3 of the Suitability FAQs.
[33] Paragraph 5.9(i) of the Online Platform Guidelines.
[34] Paragraph 5.9(iv) of the Online Platform Guidelines.
[35] Answer to question 2 of the Suitability FAQs.

Expected regulatory standards
Furthermore, LCs should implement appropriate measures in detecting any abnormal frequent changes to client profiles and ensure appropriate actions will be taken on these exceptions[36].

Examples of good practices
(a) To facilitate clients in completing their risk profiles, some LCs have designed the online RPQ in a way which will auto-populate answers to certain questions, subject to the information provided by the client in previous RPQ questions and other KYC forms. (b) To prevent abnormal frequent updates of RPQ, some LCs set a daily limit on the number of times their clients can update the RPQ. An LC will also send a warning message to the clients and suggest them to call the customer service hotline to better understand the questions if they have frequently updated their RPQs within a specified timeframe.

(v) Other matters related to disclosure of information to clients

Expected regulatory standards
LCs should make reference to paragraphs 2.3 (information for clients) and 6.7 of the Online Platform Guidelines and paragraphs 8.3 and 8.3A (disclosure of monetary and non-monetary benefits) of the Code of Conduct. In particular, for the deficiencies mentioned in Part III, LCs are reminded to comply with the following requirements: (a) <u>Information related to the investment products offered</u> (i) LCs should make available information on the methodology adopted for assessing and assigning ratings to investment products and categorising clients on their online platforms, if any. The information should also be accompanied by an explanation of the risk profiles of investment products and clients[37]. (ii) LCs should ensure that their online platforms provide sufficient information on the key nature, features and risks of a complex product to enable clients to understand the product before making an investment decision[38]. (b) <u>Disclosure of monetary benefits</u> Where an LC or any of its associates explicitly receives monetary benefits from a product issuer (directly or indirectly) for distributing an investment product, the LC should disclose the monetary benefits receivable by it or any

[36] Paragraph 5.9 of the Online Platform Guidelines.
[37] Paragraph 2.3(iv) of the Online Platform Guidelines.
[38] Paragraph 6.7 of the Online Platform Guidelines.

Expected regulatory standards
of its associates as a percentage ceiling of the investment amount or the dollar equivalent[39]. Where the monetary benefits are not quantifiable prior to or at the point of entering into a transaction, the LC should disclose the existence and nature of the benefits and the maximum of the monetary benefits receivable per year[40].

Examples of good practices
Two LCs disclosed on their online platforms the objective criteria for shortlisting investment products, including the quantitative and qualitative factors such as past performance, indicative ratio and investment strategy.

(b) Additional functionalities and use of social media to enhance client experience

(i) Risk of posting inaccurate and misleading information and commentaries on online platforms

Expected regulatory standards
LCs should put in place a proper mechanism to ensure any commentaries, representations made and information or materials posted by the staff of the LC and its affiliates on the online platforms are accurate and not misleading[41].

(ii) Potential compliance issues relating to solicitation of overseas clients

Expected regulatory standards
LCs have a general obligation to observe legal and regulatory requirements which apply to the activities conducted by the LCs whether in or outside Hong Kong, with respect to all applicable requirements of any relevant regulatory authority. Where clients located outside Hong Kong are involved, LCs should be mindful of the requirements imposed by the domestic regulatory authorities applicable to, among other things, the solicitation of clients and the opening of client accounts as well as remittance of funds for investment purpose. LCs should seek legal advice as to how the law of the other jurisdictions apply to them, for example, whether they need a licence or approval from or registration with the domestic regulatory authorities, before conducting the activities[42].

[39] Paragraph 8.3 Part A (a)(i) of the Code of Conduct.
[40] Paragraph 8.3 Part A (b)(ii) of the Code of Conduct. Also see the FAQs on Disclosure of Transaction Related Information issued by the SFC on 15 June 2018.
[41] Paragraph 2.1 of the Code of Conduct and Paragraph 2.2(ii)(a) of the Online Platform Guidelines.
[42] Circular to Licensed Corporations – Regulatory compliance regarding cross-border business activities issued by the SFC on 28 January 2014.

C. Cybersecurity

Expected regulatory standards
According to the Online Platform Guidelines[43], LCs should refer to guidance on cybersecurity issued by the SFC from time to time to ensure the system security of their online platforms. Specifically, LCs should comply with the following requirements in relation to the deficiencies mentioned in Part III: (a) implement effective 2FA for login to clients' internet trading accounts on the online platforms[44]; (b) implement an effective monitoring and surveillance mechanism to detect unauthorised access to clients' internet trading accounts[45]; (c) provide prompt notifications to clients through a channel which is different from the one used for system login[46]; and (d) disallow clients from disabling session timeout and limit the idle timeout period subject to prior assessment and ongoing monitoring[47].

[43] Paragraph 2.4(vi) of the Online Platform Guidelines.
[44] Paragraph 1.1 of the Cybersecurity Guidelines and paragraphs 10 to 15 of the Cybersecurity Thematic Review Report.
[45] Paragraph 1.2 of the Cybersecurity Guidelines. Also see paragraph 16 of the Cybersecurity Thematic Review Report.
[46] Paragraph 1.3 of the Cybersecurity Guidelines.
[47] Please refer to paragraph 30 of the Cybersecurity Thematic Review Report for details.