STATEMENT OF DISCIPLINARY ACTION

The Disciplinary Action

1. The Securities and Futures Commission (**SFC**) has reprimanded and fined Rifa Futures Limited (previously known as iSTAR International Futures Co. Limited) (**Rifa**)[1] $9,000,000 pursuant to section 194 of the Securities and Futures Ordinance (**SFO**).

2. The disciplinary action is taken because Rifa failed to:

   (a) perform adequate due diligence on the customer supplied systems (**CSSs**)[2] used by clients for placing orders, and assess and manage the associated money laundering and terrorist financing (**ML/TF**) and other risks;

   (b) conduct adequate ongoing monitoring of clients' fund movements to ensure they were consistent with the clients' nature of business, risk profile and source of funds; and

   (c) implement two-factor authentication (**2FA**) for clients to login to their internet trading accounts via CSSs.

Summary of Facts

A. Background

3. The SFC received complaints against various licensed corporations (**LCs**) for allowing clients to place orders to their broker supplied systems (**BSS**)[3] through a software called Xinguanjia (**XGJ**)[4]. The complainant alleged that XGJ permitted the LCs' clients to create sub-accounts under their accounts maintained with the LCs, and the clients had solicited investors in Mainland China to trade through the sub-accounts via XGJ without having to open separate securities accounts with the LCs in Hong Kong.

4. Rifa is one of the LCs subject to the complaint. Between May 2016 and October 2018, Rifa has permitted 310 clients to use CSSs (including XGJ) for placing orders[5]. It is estimated that over 61% of the futures contracts transacted by Rifa's clients from July 2016 to August 2018 were through orders placed via XGJ.

B. Failure to perform adequate due diligence on the CSSs and assess and manage the associated ML/TF and other risks

5. Prior to allowing the CSSs to be connected to its BSS, Rifa would require its clients to:

   (a) apply for a certificate from the vendor of the BSS (**BSS Vendor**); and

   (b) send a request to Rifa for final approval to use the CSS.

---

[1] Rifa is licensed to carry on Type 2 (dealing in futures contracts) regulated activity under the SFO.

[2] CSSs are trading software developed and/or designated by the clients that enable them to conduct electronic trading through the Internet, mobile phones and other electronic channels.

[3] BSSs are trading facilities developed by exchange participants or vendors that enable the exchange participants to provide electronic trading services to investors through the Internet, mobile phones, and other electronic channels.

[4] XGJ was developed and/or provided by Hengxin Software Limited.

[5] The CSSs were connected to Rifa's BSS through application programming interface (a set of functions that allows applications to access data and interact with external software components or operating systems).

6. Rifa did not perform any due diligence or testing on the CSSs used by its clients. It only carried out a walkthrough test on the connectivity between the CSSs and its BSS. Although Rifa claimed that it relied on the BSS Vendor to conduct due diligence on the CSSs, the BSS Vendor stated that Rifa had never instructed it to, and it did not, conduct any due diligence or test on the CSSs to examine their design and functions.

7. Without thorough knowledge of the features and functions of the CSSs, Rifa was not in a position to properly assess the ML/TF and other risks associated with the use of the CSSs and implement appropriate measures and controls to mitigate and manage such risks.

8. In the absence of proper controls over the use of CSSs by its clients, Rifa has exposed itself to the risks of improper conduct such as unlicensed activities, money laundering, nominee account arrangement and unauthorized access to client accounts.

C. Failure to conduct adequate ongoing monitoring of clients' fund movements to ensure they were consistent with the clients' nature of business, risk profile and source of funds

9. The SFC's investigation revealed that the amounts of deposits made into the accounts of 5 clients (**5 Clients**) were incommensurate with their financial profiles, including their income and net worth, declared in their account opening documents, which were unusual and/or suspicious.

10. Rifa had performed periodical and ad hoc reviews (monthly review, quarterly review, annual update and event-driven review etc.) to update client information (including their financial positions). Rifa also conducted quarterly review on clients' fund movements in respect of its top 50 clients by trading volume by comparing their aggregate fund deposits with the total net worth declared in their account opening documents and conducting know your client (**KYC**) checks to know more about the background of these clients.

11. With respect to the deposits made into the accounts of the 5 Clients, Rifa had made telephone calls to the relevant clients, informing them that their deposits had exceeded their declared net worth (**Telephone Calls**). Rifa only asked 4 of the 5 Clients for the reasons for the deposits. The clients' responses were that the excess was attributed to an increase in their income derived from their investment, business and rent. Rifa accepted the clients' answers without asking any further questions or requiring any supporting documents to substantiate what clients had said.

12. Rifa failed to demonstrate that these monitoring measures were adequate:

    (a) the KYC checks were superficial since it consisted of only name searches on Dow Jones Risk & Compliance and the SFC's public register of licensed persons and registered institutions which would unlikely throw light on the source of such deposits;

    (b) the Telephone Calls suggest that Rifa did not make proper enquiries with the clients regarding the source and original of the large and frequent deposits;

    (c) even when Telephone Calls were made, they were not made on a timely basis – the Telephone Calls were made 4 to 16 months after the accumulated deposits in the client's account exceeded his/her declared net worth; and

    (d) Rifa did not have clear policies and procedures to conduct ongoing monitoring of deposits of the clients. Some of the Telephone Calls were prompted by an email from the settlement department while some were not.

D. Failure to implement 2FA for clients to login to their internet trading accounts via CSSs

13. Paragraph 1.1 of the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (**Cybersecurity Guidelines**) issued by the SFC on 27 October 2017 requires an LC to implement 2FA for login to clients' internet trading accounts. This requirement took effect on 27 April 2018.

14. Contrary to this requirement, Rifa failed to implement 2FA for clients logging into their internet trading accounts through CSSs from April 2018. Rifa required clients to sign a declaration which specifically stated it could not provide the 2FA login function and that clients would be liable for any losses incurred as a result of lack of the same.

The SFC's findings

15. Rifa's failures set out above constitute a breach of:

    (a) General Principle (**GP**) 2 of the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (**Code of Conduct**), which requires an LC to act with due skill, care and diligence, in the best interests of its clients and integrity of the market in conducting its business activities.

    (b) GP 3 and paragraph 4.3 of the Code of Conduct, which provide that an LC should have and employ effectively the resources and procedures which are needed for the proper performance of its business activities and have internal control procedures and operational capabilities which can be reasonably expected to protect its operations and clients from financial loss arising from theft, fraud, and other dishonest acts, professional misconduct or omissions.

    (c) Paragraph 5.1 of the Code of Conduct which requires an LC to take all reasonable steps to establish the true and full identity of each of its clients, and of each client's financial situation, investment experience, and investment objectives.

    (d) Section 23 of Schedule 2 to the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (**AMLO**) and paragraph 2.1 of the Guideline on Anti-Money Laundering and Counter-Terrorist Financing (April 2015 and March 2018 editions) (**AML Guideline**), which require an LC to:

        (i) establish and implement adequate and appropriate internal anti-money laundering (**AML**) and counter-financing of terrorism (**CFT**) policies, procedures and controls pursuant to paragraph 2.2 of the AML Guideline; and

        (ii) assess the risks of any new products and services (especially those that may lead to misuse of technological developments or facilitate anonymity in ML/TF schemes) before they are introduced and ensure appropriate additional measures and controls are implemented to mitigate and manage the associated ML/TF risks pursuant to paragraph 2.3 of the AML Guideline.

    (e) Section 5(1)(a) of Schedule 2 to the AMLO and paragraphs 4.7.12 and 5.1(a) of the AML Guideline, which require an LC to review from time to time client information to ensure that they are up-to-date and relevant when a significant transaction is to take place or a material change occurs in the way the client's account is operated.

    (f) Section 5(1)(b) of Schedule 2 to the AMLO and paragraph 5.1(b) of the AML Guideline, which require an LC to continuously monitor its business relationship

with the clients by monitoring their activities to ensure that they are consistent with its knowledge of the clients and the clients' nature of business, risk profile and source of funds.

(g) Section 5(1)(c) of Schedule 2 to the AMLO and paragraphs 5.1(c), 5.10 and 5.11 of the AML Guideline, which require an LC to identify transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose, make relevant enquiries to examine the background and purpose of the transactions, document the enquiries made (and their results), and report the findings to the Joint Financial Intelligence Unit where there is any suspicion of ML/TF. Pursuant to paragraph 7.11 of the AML Guideline, where a transaction is inconsistent in amount, origin, destination, or type with a client's known, legitimate business or personal activities, the transaction should be considered as unusual and the LC should be put on alert[6].

(h) Paragraph 1.1 of the Cybersecurity Guidelines, which requires an LC to implement 2FA for login to clients' internet trading accounts.

Conclusion

16. Having considered all relevant circumstances, the SFC is of the opinion that Rifa is guilty of misconduct and its fitness and properness to carry on regulated activities have been called into question.

17. In deciding the disciplinary sanction set out in paragraph 1 above, the SFC has taken into account all of the circumstances, including:

(a) Rifa's failures to diligently monitor its clients' activities and put in place adequate and effective AML/CFT systems and controls are serious as they could undermine public confidence in, and damage the integrity of, the market;

(b) a strong deterrent message needs to be sent to the market that such failures are not acceptable; and

(c) Rifa has previously been disciplined by the SFC for similar AML-related failures[7].

[6] Examples of situations that might give rise to suspicion are given in paragraphs 7.14 and 7.39 of the AML Guideline, such as (a) transactions or instructions which have no apparent legitimate purpose and/or appear not to have a commercial rationale; (b) buying and selling of securities/futures with no discernible purpose or where the nature, size or frequency of the transactions appears unusual; and (c) the entry of matching buys and sells in particular securities or futures or leveraged foreign exchange contracts (wash trading), creating the illusion of trading. Such wash trading does not result in a bona fide market position and might provide "cover" for a money launderer.

[7] Please refer to the SFC press release dated 12 April 2017.