

## STATEMENT OF DISCIPLINARY ACTION

---

### The Disciplinary Action

1. The Securities and Futures Commission (**SFC**) has reprimanded and fined Zhonghui International Futures Company Limited (**ZIFC**)<sup>1</sup> \$5,000,000 pursuant to section 194 of the Securities and Futures Ordinance (**SFO**)<sup>2</sup>.
2. The disciplinary action is taken because ZIFC failed to:
  - (a) perform adequate due diligence on the customer supplied systems (**CSSs**)<sup>3</sup> used by clients for placing orders, and assess and manage the associated money laundering and terrorist financing (**ML/TF**) and other risks;
  - (b) take reasonable steps to establish the true and full identity of its clients and their ultimate beneficial owners, and make proper enquiries before approving clients' requests to set up third party operated accounts;
  - (c) establish effective ongoing monitoring system to detect unusual money movements and suspicious trading patterns in client accounts; and
  - (d) 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 a complaint against various licensed corporations (**LCs**) for allowing clients to place orders to their broker supplied systems (**BSS**)<sup>4</sup> through a software called Xinguanjia (**XGJ**)<sup>5</sup>. 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. ZIFC is one of the LCs subject to the complaint. Between May 2017 and July 2018 (**Relevant Period**), ZIFC has permitted 26 clients to use their designated CSSs (including XGJ) for placing orders<sup>6</sup>. From June 2017 to July 2018, the

---

<sup>1</sup> ZIFC is licensed to carry on Type 2 (dealing in futures contracts) regulated activities under the SFO.

<sup>2</sup> The SFC has also prohibited Mr Chu Chun Wai, a former responsible officer and executive director of ZIFC, for seven months. Please see the SFC's press release dated 30 December 2021.

<sup>3</sup> 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.

<sup>4</sup> 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.

<sup>5</sup> XGJ was developed and/or provided by Hengxin Software Limited.

<sup>6</sup> The CSSs were connected to ZIFC'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).

number of futures contracts transacted by ZIFC clients through orders placed via CSSs accounted for 94.07% to 99.99% of its monthly turnover.

*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 each of the CSSs to be connected to its BSS, ZIFC would:
  - (a) review the CSS user manual provided by the client and check if there were any functions (e.g. sub-account, margin financing, or simultaneous logins by multiple devices) that might not be in compliance with the prevailing regulations;
  - (b) conduct online keyword search for any negative news on the CSS; and
  - (c) require the client to perform a connection test to ensure that the CSS was compatible with its BSS and submit the connection test result to its BSS provider<sup>7</sup>.

According to ZIFC, based on its review of the CSS user manuals, none of the CSSs used by its clients has the function of creating sub-accounts.

6. ZIFC's due diligence on the CSSs was inadequate in that:
  - (a) The steps taken by ZIFC (including reviewing the CSS user manuals and conducting online keyword searches) were not sufficient to enable it to identify and be cognizant of all the features and functions of the CSSs.
  - (b) The connection tests were limited to checking if the CSSs supported certain functions such as login/logout, order placing, order cancelling, order confirmation and trade confirmation. Other than validating the test results submitted by the clients, the BSS provider did not (nor did ZIFC request it to) perform any due diligence on the CSSs or seek to ascertain other functions that might be offered by the CSSs.
7. Without thorough knowledge of the features and functions of the CSSs, ZIFC 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. Further, despite ZIFC's claim that none of the CSSs has the function of creating sub-accounts, the evidence suggests that some of the CSSs allowed multiple traders to place orders in the same client account. Such function is susceptible to misuse for the following reasons:
  - (a) ZIFC has no or limited control and monitoring over the login activities under CSSs;
  - (b) the clients could allow other investors to trade through their accounts via the CSSs without ZIFC's knowledge; and

---

<sup>7</sup> During the Relevant Period, ZIFC only required its clients to perform the connection test when the CSS was first introduced to ZIFC. Once the CSS was approved by ZIFC, other clients who subsequently wished to use the same CSS were not required to conduct the connection test again.

- (c) the identity of the person ultimately responsible for originating the orders in the client account could be easily disguised through the use of CSSs.
- 9. In the absence of proper control over the use of CSSs by its clients, ZIFC 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 take reasonable steps to establish the true and full identity of its clients and their ultimate beneficial owners and make proper enquiries before approving clients' requests to set up third party operated accounts*
- 10. The SFC identified that eight clients have authorized three to 25 third parties to place orders for their accounts via CSSs. The relationships between the clients and relevant authorized persons were stated to be "partnership", "colleague" or "employment relationship".
- 11. Third party operated accounts are susceptible to higher risks of fraud and other unauthorized or improper activities because the identity of the clients can be more easily disguised, and when suspicious activity occurs in the accounts, it is difficult for the LCs to identify who is responsible for such activity. These risks are heightened in this case as some of the clients have authorized multiple third parties to trade in their accounts via CSSs. Such third party authorization arrangements cast doubt on whether the client accounts might have been operated as nominee accounts to conceal the true beneficial ownership or to facilitate other illegitimate activities.
- 12. Despite the risks associated with these third party operated accounts, ZIFC failed to take reasonable steps to establish the true and full identity of its clients and their ultimate beneficial owners, and make proper enquiries before approving the clients' requests to set up the third party operated accounts:
  - (a) ZIFC failed to take reasonable steps to verify the purported relationships between the clients and their authorized persons;
  - (b) ZIFC did not make any or sufficient enquiries on, and critically evaluate, the clients' reasons for authorizing multiple third parties to place orders for their accounts before accepting their third party authorization requests<sup>8</sup>; and
  - (c) apart from their identity documents and contact numbers, ZIFC did not obtain other relevant information about the authorized persons such as their occupation, investment experience and education level for assessing the reasonableness of the authorization arrangements.

---

<sup>8</sup> In a circular of the SFC dated 5 February 2016 entitled "Circular to Licensed Corporations Licensed for Dealing in Securities - Protecting Client Assets Against Internal Misconduct", LCs have been reminded to have measures in place to protect their clients' assets. Paragraph 2(a) of Appendix 2 to this circular provides that LCs should only approve the opening of third party operated accounts on an exceptional basis after (i) making proper enquiries, such as the client's relationship with the third party and the reason of such arrangement; and (ii) diligently reviewing the evidence of the client's written authorization.

- D. *Failure to establish effective ongoing monitoring system to detect suspicious money movements and trading patterns in client accounts*
13. During the Relevant Period, ZIFC failed to have in place proper systems and controls to monitor its clients' activities and detect any unusual or suspicious transactions.
14. The SFC's review of the transactions in sample client accounts showed that there were:
- (a) unusual money movements in three client accounts where the clients' accumulated net deposit exceeded their declared net worth for a period of three to six months between January and August 2018 (**Unusual Deposits**); and
  - (b) 1,052 instances of self-matched trades (ie, the client's order matched with his/her own order in the opposite direction) (**Matched Trades**) in two client accounts between March and May 2018.

ZIFC did not detect the Unusual Deposits and Matched Trades at the material time.

15. According to ZIFC, it implemented a trade monitoring system for monitoring and detecting suspicious transactions such as Matched Trades in June 2018. Prior to that, it merely relied on its execution brokers to identify and notify it of any Matched Trades.
- E. *Failure to implement 2FA for clients to login to their internet trading accounts via CSSs*
16. 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.
17. Contrary to this requirement, ZIFC failed to implement 2FA for clients logging into their internet trading accounts through CSSs until October 2018, ie, six months after the effective date of the 2FA requirement.

### **The SFC's findings**

18. ZIFC'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 provides 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) Section 23 of Schedule 2 to the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (**AMLO**) and paragraphs 2.1, 2.2 and 2.3 of the Guideline on Anti-Money Laundering and Counter-Terrorist Financing (April 2015 and March 2018 editions) (**AML Guideline**), which require an LC to (1) establish and implement adequate and appropriate internal anti-money laundering (**AML**) and counter-financing of terrorism (**CFT**) policies, procedures and controls to mitigate the risks of ML/TF and prevent contravention of any customer due diligence and record keeping requirements under the AMLO and (2) 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.
- (d) 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.
- (e) Section 2(1)(b) of Schedule 2 to the AMLO and paragraphs 4.1.3 and 4.3<sup>9</sup> of the AML Guideline, which require an LC to (i) identify any beneficial owner in relation to a client and take reasonable measures to verify the beneficial owner's identity; and (ii) in respect of a client who is an individual, make appropriate enquiries where there are indications that the client is not acting on his own behalf.
- (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.
- (h) Paragraph 7.11 of the AML Guideline, which provides that where a transaction is inconsistent in amount, origin, destination, or type with a client's known, legitimate business or personal activities, the

---

<sup>9</sup> Sections 4.3.1 and 4.3.4 of the April 2015 edition of the AML Guideline and sections 4.3.1 and 4.3.3 of the March 2018 edition of the AML Guideline.

transaction should be considered as unusual and the LC should be put on alert<sup>10</sup>.

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

## **Conclusion**

- 19. Having considered all relevant circumstances, the SFC is of the opinion that ZIFC is guilty of misconduct and its fitness and properness to carry on regulated activities have been called into question.
- 20. In deciding the disciplinary sanction set out in paragraph 1 above, the SFC has taken into account all of the circumstances, including:
  - (a) ZIFC'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) the necessity of a strong deterrent message that such failures are not acceptable;
  - (c) ZIFC has taken remedial measures to enhance its internal systems and controls;
  - (d) ZIFC's financial situation;
  - (e) ZIFC cooperated with the SFC in resolving the SFC's concerns; and
  - (f) ZIFC's otherwise clean disciplinary record.

---

<sup>10</sup> Examples of situations that might give rise to suspicion are given in paragraphs 7.14 and 7.39 of the AML Guideline, such as (i) transactions or instructions which have no apparent legitimate purpose and/or appear not to have a commercial rationale; (ii) requests by customers for investment management services where the source of the funds is unclear or not consistent with the customers' apparent standing; (iii) buying and selling of securities/futures with no discernible purpose or where the nature, size or frequency of the transactions appears unusual; and (iv) 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.