CompliancePlus Consulting

Compliance Consulting • Funds Consulting
Regulatory Consulting • Compliance Training

Submission to the SFC Consultation Paper on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading

Josephine Chung

Director, CompliancePlus Consulting Limited

3 July 2017

For enquiries on this submission, please contact Josephine Chung at jchung@complianceplus.hk. CompliancePlus Consulting Limited understands and agrees that our name and/or submission may be published by the SFC.

CompliancePlus Consulting Limited
801, Two Exchange Square, 8 Connaught Place, Central, Hong Kong
Tel: (852) 3487 6903 www.complianceplus.hk

Introduction

The Securities and Futures Commission (the "**SFC**" or the "**Commission**") has issued a Consultation Paper in May 2017 (the "**Consultation Paper**") on the proposals to reduce and mitigate hacking risks associated with internet trading. The proposals incorporate new guidelines which set out baseline cybersecurity requirements for internet brokers to address hacking risks and vulnerabilities and to clarify expected standards of cybersecurity controls.

This submission is prepared in response to the SFC's Consultation Paper and our comments are set out below. Terms defined or given a particular construction in the Consultation Paper have the same meaning in this Response unless a contrary indication appears.

Consultation Questions

Question 1: The SFC is of the view that the proposed controls should be baseline requirements, which will also serve as an entry requirement for potential internet brokers. Do you agree with this approach?

We share the same view as the Commission that the proposed controls should be baseline requirements, as well as the entry requirement for potential internet brokers. As presented in the Consultation Paper, the financial service sector has become particularly prone to cyber-attacks as the industry shifts to a more technology-reliant landscape. We believe the strengthening of cybersecurity controls and the protection of investors and market integrity are of great significance.

In terms of the scope of the proposed controls, we note that the majority of the proposed baseline requirements are existing requirements in the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission ("**Code of Conduct**"), while the rest are in also line with some existing general principles in regard to cybersecurity management. We also agree, in general, that potential internet brokers who intend to be licensed in the future should be able to meet the same level of requirements as well.

We agree that the Commission's approach will effectively standardize and codify the cybersecurity control practices that internet brokers across the industry should adopt. With the introduction of the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (the "**draft guideline**"), we believe the industry will have unambiguous guidance on how to meet the Commission's expectations in relation to cybersecurity controls.

Furthermore, we acknowledge the Commission's consideration on the scales of different internet brokers and the flexibility allowed for internet brokers to determine the specific means to be adopted, considering their own circumstances and business models.

Question 2: The application of Paragraph 18 of and Schedule 7 to the Code of Conduct is expanded to cover the internet trading of securities that are not listed or traded on an exchange. Do you agree that the proposed expansion of the scope of the regulation of internet trading is appropriate? If yes, is the proposed wording sufficiently clear?

Considering the internet trading of securities that are not listed or traded on an exchange is also exposed to the same vulnerability or cyber-attacks, we, in principle, agree that the proposed expansion of the scope of the regulation of internet trading is appropriate. At the same time, we hope that in the relevant circular that the Commission plans to issue in due course, the proposed scope expansion would be clearly communicated. This is due to the fact that some licensed or registered persons who do not categorize themselves as traditional brokerage firms may also fall under the scope, for instance, asset management firms that distribute non-listed funds (that are securities) through the electronic means and the internet. We are also in the opinion that the proposed wording is sufficiently clear. Still, we welcome any further explanatory examples, if any, in subsequent circulars or FAQs issued by the Commission.

Questions 3: By not prescribing particular 2FA solutions, the proposed requirements should provide brokers with a measure of flexibility when providing additional safeguard against hacking risks. Do you agree that this approach is appropriate?

We agree with the Commission's approach in not prescribing particular two-factor authentication ("**2FA**") solutions for the proposed requirement of internet brokers implementing 2FA for logging into clients' internet trading accounts. As observed in the market, many internet brokers of an institutional or larger scale have already implemented 2FA by various means. By mandating the use of 2FA during client login without prescribing the 2FA solutions, we believe this approach would standardize the login security level among internet brokers in the market, without posing a discriminatory burden, both operational and financial, on certain smaller-sized internet brokers.

From the perspective of internet brokers, the Commission's approach effectively eliminates the unhealthy competition in the market for clients that seek convenience and speedy trade execution that come with not using any 2FA solutions, creating a more level playing field in the market. The flexibility offered by the Commission also allows internet brokers to select the 2FA solution(s) that is the most cost-effective (while fulfilling the requirement as set out in the proposed guidelines) and commensurate with their own business models. As for the clients, the Commission's approach provides a minimum level of security that is available to all clients regardless of their choice of internet brokers. We also believe the implementation of the 2FA requirement will substantially increase the level of client protection given that the login process is considered to be the very first line of defence against cyber-attacks.

Furthermore, given that there are various types of 2FA solutions that range in the level of sophistication and prices (for example, hardware tokens, software tokens, biometric devices, password cards), we are of the opinion that internet brokers should be reminded that in spite of the types and prices of 2FA solutions used, they should be responsible to ensure the implemented authentication methods meet the requirement nonetheless, even though flexibility is granted by the Commission.

Questions 4: Do you agree that for practical considerations, it will not be appropriate to mandate the monitoring of suspicious trading patterns?

With regard to the appropriateness to mandate the monitoring of suspicious trading patterns, we hold the same opinion as the Commission and we agree that it may not be feasible and practical to require internet brokers to, manually or with the assistance of automation, monitor trading patterns of clients. We echo the Commission's reasoning as stated in the Consultation paper that mandating such trade surveillance controls will pose material burdens, both operational and financial, on the internet brokers. In addition, we concur with the Commission's decision to list the monitoring of suspicious trading patterns as a good practice in future circular. We also believe internet brokers will continue to observe their current post-trade surveillance controls, which serve, in principle, a similar purpose.

Questions 5: Due to cost considerations, the proposals do not require internet brokers to assess and enhance their backup facilities (i.e. disaster recovery sites) for providing internet trading services or alternative arrangements for receiving clients' orders in an emergency so as to avoid disrupting services in an unacceptable manner. Do you agree with this approach?

We recognize the Commission's consideration on the possible costs that may incur to internet brokers in case they are required to assess and enhance their backup facilities. We also acknowledge the amount of managerial support, human resource, time and funding that a comprehensive assessment or test on backup facilities would require. However, we do wish to reiterate the importance of properly assessing and enhancing the effectiveness and readiness of backup facilities and any alternative arrangements, through the means of, for instance, simulation tests. Nevertheless, we are of the opinion that the relevant wordings in Section 2 "Infrastructure security management" of the proposed guidelines that is to be issued under Section 399(1) of the SFO has captured the significance of contingency planning and the responsibility of internet brokers to make reasonable effort to cover possible cyber-attack scenarios in the business continuity plan ("**BCP**") and crisis

management procedures, which should involve the regular testing and evaluation of backup facilities.

Questions 6: In your opinion, does the current level of service offered by your service providers enable you to comply with the proposed baseline requirements? Do you envisage any difficulty in negotiating higher service levels with your service providers?

The first part of the question is inapplicable to us given that we, as a compliance consulting firm, do not fall under the category of "internet broker" nor have we engaged any internet trading-related service providers. Nonetheless, we do anticipate the possibility for both existing internet brokers and companies that intend to become licensed to act as internet brokers in the future to encounter a certain level of challenge in negotiating higher service levels with their service providers. For existing internet brokers, many have already entered into a formal service-level agreement with their service providers. Such agreements may be standard packages where the terms and conditions may not have been tailored to the internet brokers' firm-specific operations. These internet brokers should review the current agreements and may need to negotiate a higher service levels, which could incur extra costs. As for future internet brokers, the challenge lies in finding the service providers that are equipped with sufficient competence and infrastructure to deliver the required level of service. We recommend internet brokers to carefully evaluate the service providers with due diligence, and clearly communicate the expected level of service before entering into an agreement with service providers. We are optimistic about the achievability of higher service levels as we observe some service providers in the market have already been, or are in the process of, enhancing their products in light of the increasing requirements on service levels.

Conclusion

In general, we share the same view as the Commission on the importance of mitigating the risks of cyber-attacks and hacking. We also, in principle, agree with the Commission's principle-based approach to standardize the cybersecurity control practices that are, for the

most part, already in the existing Code of Conduct. As the landscape of the cybersecurity threats is still transforming, we expect the effective controls to reduce the risk of hacking will continue to evolve. In the future, we expect the Commission to inform the public a timeline of the issuance of the draft guideline, so that internet brokers and service providers in the market could equip themselves with the knowledge and infrastructure necessary to meet the Commission's requirements.

- END -