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

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

May 2017

Table of Contents

Foreword

The Securities and Futures Commission (**SFC**) invites market participants and interested parties to submit written comments on the proposals discussed in this consultation paper or to comment on related matters that might have a significant impact upon the proposals by no later than 7 July 2017. Any person wishing to comment on the proposals on behalf of any organisation should provide details of the organisation whose views they represent.

Please note that the names of the commentators and the contents of their submissions may be published on the SFC's website and in other documents to be published by the SFC. In this connection, please read the Personal Information Collection Statement attached to this consultation paper.

You may not wish your name and/or submission to be published by the SFC. If this is the case, please state that you wish your name and/or submission to be withheld from publication when you make your submission.

Written comments may be sent as follows:

By mail to:	Securities and Futures Commission 35/F Cheung Kong Center 2 Queen's Road Central Hong Kong Re: Consultation Paper on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading
By fax to:	(852) 2284 4660
By online submission:	http://www.sfc.hk/edistributionWeb/gateway/EN/consultation/
By e-mail to:	2017_cybersecurityconsultation@sfc.hk

All submissions received before expiry of the consultation period will be taken into account before the proposals are finalised and a consultation conclusions paper will be published in due course.

Securities and Futures Commission
Hong Kong

8 May 2017

Personal Information Collection Statement

1. This Personal Information Collection Statement (**PICS**) is made in accordance with the guidelines issued by the Privacy Commissioner for Personal Data. The PICS sets out the purposes for which your Personal Data[1] will be used following collection, what you are agreeing to with respect to the SFC's use of your Personal Data and your rights under the Personal Data (Privacy) Ordinance (Cap. 486) (**PDPO**).

Purpose of collection

2. The Personal Data provided in your submission to the SFC in response to this consultation paper may be used by the SFC for one or more of the following purposes:

   (a) to administer the relevant provisions[2] and codes and guidelines published pursuant to the powers vested in the SFC;

   (b) in performing the SFC's statutory functions under the relevant provisions;

   (c) for research and statistical purposes; and

   (d) for other purposes permitted by law.

Transfer of personal data

3. Personal Data may be disclosed by the SFC to members of the public in Hong Kong and elsewhere as part of the public consultation on this consultation paper. The names of persons who submit comments on this consultation paper together with the whole or part of their submissions may be disclosed to members of the public. This will be done by publishing this information on the SFC's website and in documents to be published by the SFC during the consultation period or at its conclusion.

Access to data

4. You have the right to request access to and correction of your Personal Data in accordance with the provisions of the PDPO. Your right of access includes the right to obtain a copy of your Personal Data provided in your submission on this consultation paper. The SFC has the right to charge a reasonable fee for processing any data access request.

Retention

5. Personal Data provided to the SFC in response to this consultation paper will be retained for such period as may be necessary for the proper discharge of the SFC's functions.

[1] Personal Data means personal data as defined in the Personal Data (Privacy) Ordinance (Cap. 486).

[2] The term "relevant provisions" is defined in section 1 of Part 1 of Schedule 1 to the Securities and Futures Ordinance (Cap. 571) and refers to the provisions of that Ordinance together with certain provisions in the Companies (Winding Up and Miscellaneous Provisions) Ordinance (Cap. 32), the Companies Ordinance (Cap. 622) and the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615).

Enquiries

6. Any enquiries regarding the Personal Data provided in your submission on this consultation paper, or requests for access to Personal Data or correction of Personal Data, should be addressed in writing to:

   The Data Privacy Officer
   The Securities and Futures Commission
   35/F, Cheung Kong Center
   2 Queen’s Road Central
   Hong Kong

7. A copy of the Privacy Policy Statement adopted by the SFC is available upon request.

Introduction

1. The financial services sector is generally perceived to be most at risk from the various forms of cyber-attacks, including hacking, ransomware and denial of service, as the rapid development of technology-enabled business makes the industry and its clients more reliant on computer systems and internal networks which can be electronically accessed by, among other means, mobile applications and internet trading platforms. While awareness of the vulnerability of electronic access has improved, cyber-attacks have also become more frequent and sophisticated and the number of affected customers and their losses have increased sharply.

2. In Hong Kong, the number of cybersecurity incidents handled by the Hong Kong Computer Emergency Response Team Coordination Centre of the Hong Kong Productivity Council increased to 6,058 in 2016, up 23% from 2015[3]. For the 18 months ended 31 March 2017, 12 licensed corporations (**LCs**) reported 27 cybersecurity incidents, most of which involved hackers gaining access to customers' internet-based trading accounts with securities brokers resulting in unauthorised trades totalling more than $110 million[4] when some others involved DDoS[5] attacks targeting their websites accompanied by threats of extortion.

3. We have long recognised the importance of cybersecurity management. We introduced relevant requirements to the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (**Code of Conduct**) as part of a broader regulatory regime covering electronic trading which came into effect on 1 January 2014. Since then, we conducted thematic reviews and issued circulars to the industry sharing our findings and suggesting controls.

4. Given that hacking of internet trading appears to be the most serious cybersecurity risk faced by LCs in Hong Kong, we conducted a thematic review of the resilience to hacking risks of brokers engaged in internet trading[6] (**internet brokers**) with the assistance of an external cybersecurity expert[7] (**External Consultant**) in late 2016. The review identified certain basic cybersecurity controls that should help internet brokers to reduce and mitigate hacking risks, most of these controls are existing requirements in the Code of Conduct but require more detailed elaboration or have already been suggested in previous circulars.

5. This consultation paper proposes to incorporate these controls into guidelines to be issued under the Securities and Futures Ordinance (**SFO**). The SFC hopes that the proposed guidelines could, among other things, strengthen internet brokers' control practices to address hacking risks and vulnerabilities and provide clarity to internet brokers on the standards of cybersecurity controls which they are expected to implement when they engage in internet trading.

[3] Hong Kong Computer Emergency Response Team Coordination Centre. "HKPC Warns of Rising Trend of Cybercrime-as-a-Service". HKCERT Press Centre. Publication date: 16 January 2017. (https://www.hkcert.org/my_url/en/articles/17011601)

[4] SFC statistics.

[5] In a distributed denial-of-service (**DDoS**) attack, multiple compromised computer systems attack a server, website or other network resource, and cause a denial of service for its users.

[6] "Internet trading" for the purposes of this consultation paper adopts the same meaning as in Paragraph 18 of the Code of Conduct, being "an arrangement where order instructions are sent to a licensed or registered person through its internet-based trading facility".

[7] The external cybersecurity expert appointed by the SFC for the 2016 cybersecurity review, and all other internet trading and cybersecurity reviews prior to 2016, is a multinational professional service firm which has many years of experience advising the financial service industry and regulators on cybersecurity-related issues and has conducted many industry surveys in this regard. This firm has also provided cybersecurity control and technical assessment services to a number of local brokers over the years.

Hacking incidents and potential root causes

6. The hacking incidents reported by licensed internet brokers remain under Police investigation. However, the Police shared case studies suggesting that hackers used compromised internet trading accounts to carry out a pump-and-dump scheme which could lead to substantial financial losses. Such schemes typically follow these steps:

   (a) Hackers first gain control of clients' internet trading accounts (**hacked accounts**) which enables them to log into the accounts "legitimately" to effect unauthorised transactions;

   (b) Hackers then employ people to open other internet trading accounts to accumulate penny stocks;

   (c) Using the cash in the hacked accounts, or cash raised by selling off existing stock holdings in the hacked accounts, hackers then buy these penny stocks in order to pump up their stock prices; and

   (d) After the prices of the penny stocks go up, hackers off-load them and make a profit, leaving the owners of the hacked accounts to suffer significant losses.

7. As advised by the External Consultant, these hacking incidents could be the result of a number of weaknesses in internet brokers' trading systems and cybersecurity management frameworks, including:

   (a) **Internet brokers' lax password policies:** Clients' login passwords, particularly when they are too simple, could easily be cracked via a trial-and-error method used by application programmes to decode passwords (commonly known as a brute force attack). It should be noted that the enforcement of dual passwords is not a sufficient safeguard; in some cases hackers were able to access internet trading accounts which required dual passwords.

   This would indicate that single-factor authentication is not sufficient for protecting an internet trading account from being hacked.

   (b) **Low client awareness of cybersecurity:** Clients' login credentials for internet trading accounts could be stolen due to carelessness, such as failing to log off after using public internet access (eg, shared computers in commercial venues). In addition, social engineering, where clients are duped or manipulated into disclosing their confidential information, poses a major risk to brokers' security procedures.

   When a client accesses a broker's internet trading system using a compromised electronic device, ie, a computer, mobile phone or other device which has been hacked, the data passing through the device, including the login credentials for the client's internet trading account, could be captured through various hacking techniques such as keystroke logging[8] and man-in-middle attack[9].

[8] Keystroke logging allows malware to capture keystrokes when a user types into a specific application or a specific field on a web page (eg, password).

[9] In a man-in-the-middle attack, an attacker is able to intercept, read, interrupt and modify messages between two users or systems.

An information security survey published by PwC in 2016[10] reported that only 53% of the survey respondents provided cybersecurity training and awareness programmes to their users or employees.

(c) **Inadequate monitoring and surveillance mechanisms**: Timely and early detection by brokers of unauthorised access to their internet trading systems could help prevent losses. There were cases when brokers did not know about unauthorised transactions until clients discovered and reported them. This could delay the deactivation of the affected client internet trading accounts or the unwinding of unauthorised trades to minimise the incident's financial impact, as well as the process of investigating the incident, identifying any problems and taking appropriate steps to rectify them. According to the above-mentioned survey, only 48% of the survey respondents implemented active monitoring or analysis of threat intelligence.

(d) **Insufficient resources devoted to cybersecurity:** Additionally, the 2015 edition of the PwC survey found that survey respondents with revenues of less than US$100 million only spent 0.73% of revenue on information security.

Initiatives taken by the SFC to address cybersecurity risks

8. Cybersecurity management is a long-standing key priority for our supervision of LCs. Important cybersecurity-related regulatory principles and requirements are set out under Paragraph 18 of and Schedule 7 to the Code of Conduct. Please refer to Appendix A for a summary of these principles and requirements.

9. Since 2014, we have conducted a number of internet trading and cybersecurity reviews with assistance from the External Consultant, and issued circulars[11] to draw the industry's attention to the common deficiencies and vulnerabilities we identified. We suggested a wide range of control measures, including a self-assessment questionnaire, to supplement the existing principles and requirements in the Code of Conduct. The last of these reviews was the 2016 cybersecurity review which focused on hacking risks associated with internet trading.

10. In addition to assessing the cybersecurity features of selected brokers' internet trading systems as well as the industry's overall resilience to hacking risks, our 2016 cybersecurity review aimed to propose controls which could form the baseline cybersecurity requirements for internet brokers so as to reduce and mitigate such risks. Whilst the proposed controls are primarily designed to reduce and mitigate hacking risks, they are also relevant for addressing risks associated with other cyber-attacks. For example, the installation of anti-virus and anti-malware with updated signature files can help prevent ransomware.

[10] The Global State of Information Security® Survey prepared by PwC based on responses from over 10,000 executives in 127 countries.

[11] These circulars are (i) Alert for Cybersecurity Threats dated 26 January 2017; (ii) Cybersecurity dated 23 March 2016; (iii) Tips on Protection of Online Trading Accounts dated 29 January 2016; (iv) Internet Trading– Internet Trading Self-Assessment Checklist dated 11 June 2015; (v) Mitigating Cybersecurity Risks dated 27 November 2014; (vi) Internet Trading – Information Security Management and System Adequacy dated 26 November 2014; and (vii) Internet Trading - Reducing Internet Hacking Risks dated 27 January 2014 (collectively referred to as the "Circulars").

Proposed baseline requirements

Overall framework

11. The 2016 cybersecurity review consisted of:

    (a) A fact-finding survey on the cybersecurity aspects of 25 brokers' internet trading systems;

    (b) Onsite inspections of five brokers to review their information technology and other related management controls and assess the design and effectiveness of their systems for preventing and detecting cyber-attacks;

    (c) A benchmarking exercise against local[12] and overseas[13] regulatory requirements and market practices of financial institutions;

    (d) Discussions with selected system vendors to evaluate the feasibility, costs and benefits of different cybersecurity solutions; and

    (e) A review of existing cybersecurity-related regulations and guidance provided by the SFC in the Circulars to assess the need for clarification or additional guidance.

12. Based on the results of the 2016 cybersecurity review and the advice of the External Consultant, we propose to introduce Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (**draft Guidelines**) which contain a number of proposed baseline requirements (please refer to Appendix B). These requirements aim to:

    (a) Strengthen control practices to address known threats and vulnerabilities;

    (b) Standardise and codify common local cybersecurity control practices for their consistent adoption by internet brokers across the industry; and

    (c) Provide unambiguous and practical guidance to internet brokers with respect to the SFC's expectations on cybersecurity controls.

13. In compiling the draft Guidelines, we have considered (i) local and overseas market practices and regulatory requirements; (ii) the effectiveness and relevance of controls; (iii) the cost of implementation; and (iv) potential implications for the user experience. It is proposed that these baseline requirements will apply to all internet brokers, irrespective of the scale of their operations and their business model.

14. 17 of the 20 proposed baseline requirements are existing requirements in the Code of Conduct that warrant elaboration or have previously been suggested in the Circulars. They are now elaborated and consolidated in one place in the draft Guidelines. The remaining three are new and they are set out in the following sections. These baseline requirements will be implemented by means of guidelines issued under section 399(1) of the SFO.

[12] The banking sector in Hong Kong.

[13] Including Singapore, United Kingdom, United States, Japan, Australia and South Korea.

15. It is imperative to emphasise that:

(a) The proposed controls can only reduce and mitigate hacking risks associated with internet trading, but cannot eliminate them. For example, social engineering is a real threat where clients may succumb to duping or manipulation by hackers despite efforts by brokers to provide cybersecurity alerts and reminders;

(b) The proposed requirements typically do not specify the means to be adopted for implementing the requirements. These should be determined by internet brokers themselves, taking into account their own circumstances, such as scale of operations, extent of reliance on the internet for receiving client orders, client profiles, budget and resource constraints, future aspirations and strategic planning;

(c) The proposed requirements are minimum standards expected by the SFC. Internet brokers (particularly those with a large number of active internet trading clients and whose internet trading activities account for a large percentage of their turnover) should, at their own discretion, develop and implement additional control measures for better protection; and

(d) The proposed requirements are by no means exhaustive and have been developed to deal with hacking risks known to date.

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?

Scope of application

16. At present, the main cybersecurity-related regulatory principles and requirements are included in the Code of Conduct in Paragraph 18 and Schedule 7. These requirements apply to the electronic trading of securities and futures contracts which are listed or traded on an exchange, where “electronic trading” means the trading of securities and futures contracts electronically and includes internet trading, direct market access (**DMA**) and algorithmic trading. These regulatory principles and requirements currently apply to securities dealers, futures dealers, leveraged foreign exchange traders[14] and fund managers[15].

17. Some internet brokers may conduct internet trading of securities that are not listed or traded on an exchange, eg, authorised unit trusts and mutual funds. Given that the trading of these products through an internet trading system provides exposure to the same risks as the internet trading of securities that are listed or traded on an exchange, we propose expanding the scope of application of Paragraph 18 of and Schedule 7 to the Code of

[14] For the trading of leveraged foreign exchange contracts, “electronic trading” means the trading of such contracts electronically by means of internet trading (paragraph 66 of Schedule 6 to the Code of Conduct).

[15] For the avoidance of doubt, the existing regulatory principles and requirements in relation to electronic trading (as set out under paragraph 9 of the Fund Manager Code of Conduct) only apply to a fund manager to the extent that it conducts the electronic trading of securities and futures contracts that are listed or traded on an exchange on behalf of collective investment schemes managed by it. Furthermore, where a fund manager is engaged in online distribution of collective investment schemes through an internet-based trading facility, the requirements in respect of internet trading will apply.

Conduct to cover such activities. In this regard, it is proposed that Paragraph 18.1 of (and the Introduction of Schedule 7 to) the Code of Conduct be amended as follows:

> *"This paragraph applies to a licensed or registered person which conducts electronic trading of securities and futures contracts that are listed or traded on an exchange <u>or internet trading of securities that are not listed or traded on an exchange</u>."*

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?

18. Clients access brokers' internet-based trading facilities through various means, including computers or mobile devices. For the avoidance of doubt, we would also take the opportunity to clarify in Paragraph 18.2(f) of the Code of Conduct that an internet-based trading facility may be accessed through a computer, mobile device or other electronic device as follows:

> *""Internet trading" for the purposes of this paragraph means an arrangement where order instructions are sent to a licensed or registered person through its internet-based trading facility. <u>An internet-based trading facility may be accessed through a computer, mobile device or other electronic device.</u>"*

19. For the avoidance of doubt, given that the Code of Conduct applies to registered as well as licensed persons, the proposed requirements will also be applicable to banks that engage in internet trading.

Proposed requirements

20. The draft Guidelines set out various proposed cybersecurity requirements for internet trading under the following three categories:

    (a) Protection of clients' internet trading accounts;

    (b) Infrastructure security management; and

    (c) Cybersecurity management and supervision.

21. For the purpose of this consultation paper, these requirements are grouped into the following three types:

    (a) Preventive controls – To protect internet brokers' internal networks and internet trading systems, as well as client accounts, from cyber-attacks;

    (b) Detective controls – To detect suspected hacking activities and alert internet brokers and clients on a timely basis to mitigate their impact and reduce financial losses; and

(c) Other controls (including governance, policies and procedures) – To strengthen overall cybersecurity governance and management of internet brokers and the cybersecurity awareness of both brokers and their clients.

The following section discusses the proposed requirements in detail.

(I) Preventive controls

(i) Two-factor authentication (paragraph 1.1 of the draft Guidelines)

22. Currently, internet brokers are required to implement reliable measures to authenticate or validate the identity and authority of users to ensure that access to or use of their systems is restricted to persons approved to use them on a need-to-have basis[16]. Reliable techniques to authenticate or validate the identity and authority of each internet trading system user are essential to restrict system access to approved personnel. As such, authentication is one of the most important security controls to prevent cyber-attacks.

23. The most common way to authenticate the identity of a client is by the use of password at client login. Based on our 2016 cybersecurity review, all of the 25 brokers surveyed/ inspected[17] implemented either single or multiple password authentication for clients to log into their internet trading systems. However, based on recent reported hacking incidents, passwords alone are not a sufficient safeguard, even if there are stringent password policies and session timeout controls. On the other hand, no hacking incidents have been reported in cases where two-factor authentication (**2FA**) has been enforced.

24. 2FA refers to an authentication mechanism which utilises any two of the following factors: what a client knows (eg, password), what a client has (eg, hardware token, one-time-password that will expire in a short period of time), and who a client is (ie, biometrics). Requiring two separate authentication factors significantly enhances security protection by making hacking more difficult. For example, even though hackers may have stolen a person’s password, they then need to take control of the second factor, eg, by physically obtaining the hardware token or mobile phone receiving a one-time-password.

25. Of the 25 brokers surveyed/inspected, eight indicated that they plan to implement 2FA within the next 12 months. As 2FA will require clients to perform additional steps and may not always be welcome, these brokers are concerned that they may potentially lose their clients to brokers which choose not to implement 2FA. There were comments that the SFC should mandate 2FA across the industry to ensure a level playing field.

26. In respect of regulatory requirements, the Hong Kong Monetary Authority (**HKMA**) and Monetary Authority of Singapore (**MAS**) have long mandated 2FA for effecting pre-defined high-risk activities (eg, those involving fund movements to unregistered third parties). Since December 2016, MAS has gone further and has required all financial institutions to make 2FA available for all clients’ online trading accounts with the exception of institutional investors. At the same time, HKMA is conducting a consultation on mandating 2FA before bank customers perform online securities trading transactions.

27. While it is well understood that no single security solution is impervious to hackers, 2FA is currently considered to be an effective authentication mechanism to prevent hacking. Taking

[16] Paragraph 1.2.4(a) of Schedule 7 to the Code of Conduct.

[17] We surveyed 25 brokers and also inspected five of them.

all factors into consideration, we propose to include 2FA for client login as a baseline requirement. For the avoidance of doubt, it is proposed that 2FA be made a mandatory requirement for client login but not for placing of each order, as 2FA may affect the timeliness of order execution and this may not be in clients' best interest.

28. We have identified the more common 2FA controls (namely SMS one-time-password, hardware token, software token and digital certificate) and analysed their implementation cost, impact on user experience, advantages and disadvantages (please refer to Appendix D). The proposed requirements will not mandate any particular 2FA solution and brokers can choose to use any 2FA solution they deem appropriate, whether or not they are listed in Appendix D.

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

(ii) Security controls to help prevent against unauthorised intrusion and cyber-attacks (paragraphs 2.1, 2.4, 2.5, 2.6 and 2.7 of the draft Guidelines)

29. Internet brokers recognise the importance of protecting their critical systems from unauthorised intrusion or cyber-attacks. As a result, a wide range of security controls have been implemented by the brokers surveyed/inspected during the 2016 cybersecurity review. We now propose to codify these prevailing cybersecurity control practices and include them as proposed baseline requirements.

30. Under the proposed baseline requirements, internet brokers should:

    (a) Deploy a secure network infrastructure through proper network segmentation, ie, a Demilitarised Zone (**DMZ**) with multi-tiered firewalls[18];

    (b) Implement and update anti-virus and anti-malware solutions in a timely manner to detect malicious applications and malware on critical servers and workstations[19];

    (c) Implement controls to prevent unauthorised installation of hardware and software[18]; and

    (d) Establish physical security policies and procedures and prevent unauthorised physical access to the facilities hosting the internet trading system as well as the critical system components[19].

31. Internet brokers should also monitor and evaluate security patches or hotfixes released by software providers on a timely basis. Based on our 2016 cybersecurity review, the timeframe for the brokers surveyed/inspected to implement the latest security patches or hotfixes varies from one week to six months. More than half of these brokers implement them within one month. This timeframe is also in line with the practices of overseas financial institutions as noted in the benchmarking exercise. Under the proposal, subject to an

[18] This requirement reinforces the same control which was mentioned in the Circulars.

[19] This is a new requirement which was not mentioned in the Circulars.

evaluation of the impact of the security patch or hotfix release, they should be implemented within one month[20].

(iii) System and network access (paragraphs 2.2 and 2.3 of the draft Guidelines)

32. To reinforce internet brokers' controls over system access, we propose that internet brokers should have additional policies and procedures in place to ensure that system access is granted to users as needed. Furthermore, internet brokers should conduct a review, at least on a yearly basis[21], to ensure that access to or use of their systems remains restricted to persons approved to use them on a need-to-have basis.

33. Remote access by staff and third party service providers to the internal network of internet brokers could heighten the risk of cyber-attacks. First, remote access generally occurs over the internet (as opposed to a dedicated connection over a leased line) and internet brokers generally do not have any control over the security of external networks. Second, where remote access is made from public areas such as cafes, hackers may eavesdrop on sensitive data, as well as intercept and modify communications.

34. As such, we propose that internet brokers should only grant remote access to their internal network on a need-to-have basis, eg, to internal staff or a third party service provider. Additionally, internet brokers should implement security controls over remote access[18] from an external network to the internal network.

(iv) Data encryption (paragraph 1.4 of the draft Guidelines)

35. Currently, internet brokers have been required to implement reliable preventive measures to protect sensitive information (eg, client data files, passwords etc.)[22]. However, some brokers are concerned that the performance of their internet trading systems would significantly deteriorate if the entire database (including trade data and client information) were to be encrypted. While data encryption is a control requirement mentioned in the Circulars, we wish to clarify that only client login passwords stored in the system would need to be encrypted.

36. Separately, given the importance of protecting the confidentiality and integrity of information passed between internal and external networks, and to provide greater clarity to the industry, we propose that internet brokers should also encrypt sensitive information (including trade data) during transmission between internal networks and client devices (ie, end-to-end encryption).

(v) Client passwords and session timeout controls (paragraphs 1.5 and 1.6 of the draft Guidelines)

37. The use of client passwords is one of the most common methods for the authentication of a user's identity. Therefore, passwords should be delivered to clients in a secure manner during the account activation and password reset process[18].

38. In addition, as passwords are a first line of defence, internet brokers should set up stringent password policies[18], for example, minimum password length and maximum password age,

[20] The timeframe for implementing the security patches or hotfixes is a new requirement which was not mentioned in the Circulars.

[21] The requirement to perform user access review was mentioned in the Circulars. This is however expanded to specify the frequency of such review.

[22] Paragraph 1.2.4(b) of Schedule 7 to the Code of Conduct

in their internet trading systems to prevent passwords from being easily guessed or cracked by hackers. Also, as session timeout controls[23] limit the time period a hacker can launch attacks, internet brokers should implement appropriate session timeout controls to reduce hacking risks[18]. The common session timeout period in the marketplace ranges from two to five minutes.

(II) Detective controls

(i) Monitoring and surveillance mechanisms (paragraph 1.2 of the draft Guidelines)

39. While preventive controls can be regarded as the all-important first line of defence, monitoring and surveillance controls also play a key role. As cyber-attacks become more sophisticated, the pertinent question is not whether a cyber-attack is going to happen but when it will happen. Good detective controls are crucial to enable prompt escalation as well as remedial actions. It is therefore important for brokers to be able to detect cyber-attacks that target their networks or internet trading systems.

40. It has been observed in a number of reported hacking incidents that unauthorised access to client internet trading accounts and unauthorised trades were successfully detected via robust monitoring mechanisms. In these cases, the brokers were able to deactivate the internet trading accounts of affected clients and/or unwind unauthorised trades to minimise the financial impact as well as to report the matter to the Police for timely investigation and action.

41. Two major monitoring and surveillance mechanisms adopted by internet brokers to detect suspicious activities were noted in our 2016 cybersecurity review:

(a) Monitoring of unusual internet protocol (**IP**) addresses

Monitoring of unusual IP addresses can be performed in different ways. For example, an alert could be prompted manually (eg, system commands or queries on application access records) or through an automated programme (eg, batch script, real time monitoring system) when multiple clients' internet trading accounts are accessed by the same IP address or when there is an unusual change of the IP addresses accessing the same client's internet trading account in a short period of time (eg, from Hong Kong to London). The effectiveness of such monitoring is subject to the extent to which the frequency and the pattern of suspicious system activities can be captured.

(b) Identification of irregular trading patterns

Clients' trading activities are monitored and the internet brokers are duly alerted when abnormal trading activities take place. For example, when a client whose trading record indicates a buy-and-hold pattern for blue-chip stocks has been detected selling off his/her existing stock positions within a short span of time and using the proceeds to buy penny stocks, the monitoring system should set off an alarm. These monitoring activities can be performed manually (ie, by account executives who directly interact with clients) or systematically (ie, by the implementation of user behavioural analytics to identify irregular transactions).

[23] For the purpose of this consultation paper, "session timeout control" refers to the controls implemented in the internet trading systems to track idle sessions and automatically redirect the user to a login page after the lapse of a continual period of idle time. This requirement reinforces the same control which was mentioned in the Circulars.

42. Based on our 2016 cybersecurity review, it was noted that:

(a) Three out of five brokers inspected have implemented monitoring controls over (i) suspicious changes of IP addresses in a short period of time; and (ii) logging into multiple client accounts from the same IP address. The frequency of monitoring varies from real time to daily;

(b) 60% of the financial institutions covered in the benchmarking exercise have implemented some measures to monitor suspicious IP addresses and trading patterns; and

(c) Other regulators, such as the HKMA and the MAS, have required financial institutions to put in place robust monitoring and surveillance mechanisms to detect any abnormal system activities, transmission errors or unusual online transactions in a timely manner.

43. In view of the varying sizes and business models of internet brokers and the variety of monitoring and surveillance mechanisms available, we propose requiring internet brokers to implement monitoring and surveillance mechanisms to detect unauthorised access to clients' internet trading accounts that is commensurate with their business models without specifying the means to achieve it[18].

44. We have considered requiring the monitoring of irregular transactions such as unusual trading patterns as this is also known to be another effective detective tool. However, by its nature, client trading on an internet trading platform generally does not involve account executives and hence brokers may not be familiar with their clients' investment strategies and trading patterns. While it may not be realistic to expect brokers to review large volumes of trading data manually, automated monitoring of clients' trading patterns is also not feasible for most brokers as it requires significant investment in developing and implementing user behavioural analytic capabilities. As a result, this control will only be an example of good practice which will be included in a circular to be issued by the SFC in due course but not as a baseline requirement.

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

(ii) Prompt notification to clients[19] (paragraph 1.3 of the draft Guidelines)

45. In cases where hackers have logged into clients' internet trading accounts, prompt notification to clients can serve as an effective second line of defence for detection. In some of the reported hacking incidents, unauthorised access to and use of internet trading accounts to execute unauthorised transactions were uncovered and reported to the internet brokers by the affected clients when they received notifications of system login or trade execution.

46. Based on the 2016 cybersecurity review, we noted that:

(a) Two out of 25 brokers surveyed/inspected send notifications to clients after system login, while 14 brokers send notifications after order execution and seven send notifications after other activities such as changes of personal information have taken place in the clients' internet trading accounts. SMS messages and emails are the two most commonly used notification channels.

(b) Other regulators such as the HKMA, the MAS and the Australia Prudential Regulation Authority (**APRA**) require financial institutions to send clients prompt notifications of high risk transactions, eg, payments or fund transfers. Both the MAS and the APRA also require sending notifications through a second channel, ie, a separate channel from the one used for system login.

47. We therefore propose that internet brokers should notify clients promptly after certain activities have taken place in their internet trading accounts, including system login, trade execution, fund transfers to third parties, change of personal particulars and password reset.

48. The industry has a concern about possible high compliance costs if all notifications are to be sent by SMS. Taking note of this, we propose that internet brokers may send notifications by way of email, SMS or other push notifications as they deem appropriate[24]. However, notifications to clients should be sent through a channel which is different from the one used for system login so as to mitigate the risk of it being compromised by hackers. For instance, a client who uses a mobile phone to receive an SMS one-time-password should not also receive login notifications via SMS. This is to prevent a situation where, if a client's mobile phone has been hacked, a login notification sent via SMS could also be intercepted or disrupted by hackers.

49. In addition, the industry has also pointed out that some clients (particularly frequent traders) may not want to receive a large number of trade execution notifications. As such, under our proposal, clients may, subject to adequate safeguards such as risk disclosures and client acknowledgements, opt out of trade execution notifications. However, opting out is not an option for any other activities, eg, login or fund transfer to third parties.

(III) Other controls

(i) Roles and responsibilities of cybersecurity management (paragraph 3.1 of the draft Guidelines)

50. To enhance resilience to cyber-attacks, it is important for internet brokers to establish an appropriate cybersecurity risk management framework including clear ownership and accountability at the board or senior management level. We noted from the 2016 cybersecurity review that some brokers had only informally-defined roles and responsibilities for cybersecurity risk management, such as approval of cybersecurity policies and procedures and business continuity plans (**BCP**) by different operational units (eg, IT department), with no requirements for structured delegation and reporting. Potentially, there may be no ownership of certain critical cybersecurity risk management activities and this may expose the broker to a higher risk of cyber-attacks.

51. We propose that the responsible officers or executive officers responsible for the overall management and supervision of the internet trading system should define a cybersecurity risk management framework and set out key roles and responsibilities under cybersecurity

[24] It is nevertheless desirable to notify clients of system login as soon and effectively as practicable. On this note, automatic notification of system login by SMS may be recommended as a good practice which will be issued by the SFC in due course.

risk management[25]. However, these responsibilities can be delegated, in writing, to a designated committee or operational unit, albeit the overall accountability will rest with the responsible officers or executive officers.

(ii) Cybersecurity incident reporting (paragraph 3.2 of the draft Guidelines)

52. Cybersecurity incidents should be reported to the appropriate persons in a timely manner to ensure that issues can be addressed promptly and efficiently[18]. Under the proposal, internet brokers should establish written policies and procedures specifying the manner in which a suspected or actual cybersecurity incident should be escalated and reported internally and externally.

(iii) Backup and contingency planning (paragraphs 2.8 and 2.9 of the draft Guidelines)

53. Internet brokers are currently required to have arrangements in place to ensure that business records, client and transaction databases, servers and supporting documentation are backed up in an off-line medium[26]. In order to ensure that up-to-date trading data is available for an internet broker to continue its business in a crisis, we propose that internet brokers should back up these records and data on a daily basis. Separately, they should perform a full backup of the system and data before and after any major system changes[27].

54. The 2016 cybersecurity review revealed that most brokers surveyed/inspected have BCPs in place but nearly half of these BCPs do not cover cybersecurity scenarios. This is unsatisfactory as such scenarios require different contingency arrangements compared with those BCP scenarios covering situations where office premises and data centres cannot be physically accessed.

55. In order to ensure that appropriate contingency procedures can be effectively executed when cybersecurity situations occur, we propose that internet brokers should make all reasonable efforts to ensure that their BCP and crisis management procedures cover possible cyber-attack scenarios[18], such as DDoS and total loss of business records and client data resulting from cyber-attacks (eg, ransomware).

56. Despite recent DDoS attacks encountered by some securities brokers, we do not propose to mandate acquisition of DDoS solutions. Based on the feedback from the brokers inspected and External Consultant’s advice, the more affordable solutions available in the marketplace may not always be effective in the event of a DDoS attack on a large scale and on balance, it seems more appropriate to focus on robust BCP and crisis management procedures.

> Question 5: Due to cost considerations, the proposals do not require internet brokers to assess and enhance their backup facilities (ie, 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?

[25] Development of a cybersecurity management framework was mentioned in the Circulars. This requirement is however expanded to specify key roles and responsibilities of the responsible officers or executive officers responsible for the overall management and supervision of the internet trading system.

[26] Paragraph 1.2.6(b) of Schedule 7 to the Code of Conduct

[27] When backup of the system and data was mentioned in the Circulars, it is proposed to specify the backup cycle and also require it to be conducted before and after any major system changes.

(iv) Cybersecurity-related training and alerts (paragraphs 3.3 and 3.4 of the draft Guidelines)

57. Internal system users[28] play a key role in preventing cyber-attacks. However, the 2016 cybersecurity review found that some brokers have never provided any cybersecurity awareness training to their internal system users, while others have only provided such training on an ad hoc basis. This raises concerns as to whether internal system users are sufficiently aware of the evolving cybersecurity threats and the measures needed to prevent and defend against potential cyber-attacks. Under the proposal, to heighten cybersecurity awareness, internet brokers should provide cybersecurity training to all internal system users at least on a yearly basis[29]. These training programmes should be updated to include the latest cybersecurity-related rules and regulations and current and emerging cybersecurity threats and trends (eg, phishing, ransomware) as well as corresponding measures.

58. Separately, to help raise clients' cybersecurity awareness, internet brokers should take all reasonable steps to remind and alert clients of cybersecurity risks and recommended preventive and protection measures when using their internet trading systems[18]. For example, cybersecurity reminders may automatically pop up when clients log into internet trading systems.

(v) Management of third party service providers (paragraph 2.10 of the draft Guidelines)

59. Many internet brokers, particularly small and medium-sized brokers, currently implement internet trading systems provided by third party service providers or in some cases adopt an application service provider (**ASP**) model in offering internet trading services to clients.

60. As mentioned in the Circulars, if internet brokers have an arrangement to outsource any activities associated with their internet trading to a third party service provider, they should enter into a formal service agreement with the service provider which specifies the terms of service and the responsibilities of the provider. In particular, internet brokers should ensure that the services offered by the provider enable them to comply with the relevant regulatory requirements. In addition, service agreements should be regularly reviewed and revised, where appropriate, to reflect any change to the outsourcing arrangements or regulatory developments. Wherever possible, such agreements should provide sufficient levels of maintenance and technical assistance with quantitative details (eg, 99.9% system uptime or support services to be available within 30 minutes). We propose to codify the above for inclusion in the baseline requirements.

> Question 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?

[28] Internal system users refers to any permanent and contract staff who have access to the internal network and systems of an internet broker.

[29] Paragraph 1.2.4(d) of Schedule 7 to the Code of Conduct stipulates that appropriate steps should be taken to raise the awareness of system users about the importance of security precautions. This requirement is expanded to specify the frequency and content of these trainings.

Seeking comments and way forward

61. We welcome any comments from the public and the industry on the proposals made in this consultation paper, the draft Guidelines in Appendix B and the proposed amendments to the Code of Conduct in Appendix C. Please submit comments to the SFC in writing no later than 7 July 2017.

62. We aim to conclude this consultation and finalise the revised Code of Conduct and the new Guidelines in September/October 2017. To allow time for internet brokers to implement the baseline requirements, the Guidelines will only become effective 6 months from the publication of the consultation conclusions.

Appendix A

Existing Cybersecurity-Related Regulatory Principles and Requirements

Paragraph 18 of and Schedule 7 to the Code of Conduct[1] set out general principles for, and general and specific requirements on, electronic trading (which is defined to include internet trading) of securities and futures contracts that are listed or traded on an exchange.

Some of these principles and requirements also apply to licensed persons who engage in the trading of leveraged foreign exchange contracts electronically[2] and fund managers who conduct electronic trading of securities and futures contracts that are listed or traded on an exchange on behalf of collective investment schemes which they manage[3].

The key regulatory principles and requirements relevant to cybersecurity risks of internet trading can be summarised as follows:

(a) Protection of clients' internet trading applications and accounts (paragraph 18.5 of and paragraphs 1.2.4 (a), (b) and (c) of Schedule 7 to the Code of Conduct)

Firms should employ adequate and appropriate security controls to protect the electronic trading system from being abused. Minimum security controls should be:

(i) Reliable techniques to authenticate or validate the identity and authority of the system users to ensure that the access or the use of the system is restricted to persons approved to use the system on a need-to-have basis;

(ii) Effective techniques to protect the confidentiality and integrity of information stored in the system and passed between internal and external networks; and

(iii) Appropriate operating controls to prevent and detect unauthorized intrusion, security breach and security attack.

(b) Infrastructure security management (paragraph 18.5 of and introduction, paragraphs 1.2.4 (a), (b) and (c), 1.2.6, 1.2.7 and 1.2.8 of Schedule 7 to the Code of Conduct)

Firms should:

(i) establish a written contingency plan to cope with emergencies and disruptions related to the electronic trading system;

(ii) ensure that the contingency plan to deal with potential emergencies and disruptions is periodically tested and the plan is viable and adequate;

(iii) in a timely manner, ensure the material system delay or failure is rectified; and inform clients the causes or possible causes of the material system delay or failure and how client orders will be handled, where applicable; and

[1] Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (**Code of Conduct**)
[2] Paragraphs 66 to 67 of Schedule 6 to the Code of Conduct
[3] Paragraphs 9.1 and 9.2 of the Fund Manager Code of Conduct

(iv) perform appropriate due diligence, where the electronic trading system is provided by a third party service provider, to ensure that they meet the requirements set out in paragraph 18 of the Code of Conduct and Schedule 7 in their use of this system.

(c) Ownership of cybersecurity risk management (paragraph 18.4 of and paragraphs 1.1, 1.1.1(a), 1.1.1(d) and 1.2.4 (d) of Schedule 7 to and paragraph 12.5(e) of the Code of Conduct)

Firms should:

(i) effectively manage and adequately supervise the design, development, deployment and operation of the electronic trading system;

(ii) have at least one responsible officer or executive officer responsible for the overall management and supervision of the electronic trading system;

(iii) implement managerial and supervisory controls that are designed to manage the risks associated with the use of the electronic trading system by itself or by its clients;

(iv) take appropriate steps to raise the awareness of system users on the importance of security precautions they need to take in using the system; and

(v) report to the Commission immediately upon the happening of any material failure, error or defect in the operation or functioning of the trading system or equipment.

Appendix B

Proposed Guidelines for Reducing and Mitigating Hacking Risks associated with Internet Trading

Background

The Securities and Futures Commission (**SFC**) has proposed a number of baseline requirements for brokers (these can be securities dealers[1], futures dealers or leveraged foreign exchange traders[2] engaged in internet trading[3] (**internet brokers**) licensed by or registered with the SFC to reduce and mitigate hacking risks associated with internet trading.

These proposed requirements are to be made by way of issuing guidelines under section 399(1) of the Securities and Futures Ordinance (**SFO**) and should be read in conjunction with, among others, paragraphs 18.4 to 18.7 of the Code of Conduct and paragraphs 1.1, 1.2.2 to 1.2.8, 1.3 and 2.1 of Schedule 7 to the Code of Conduct.

The baseline requirements, which comprise 20 cybersecurity control practices, can be classified into three groups as follows:

- Protection of clients' internet trading accounts;
- Infrastructure security management; and
- Cybersecurity management and supervision.

It is imperative to emphasise that the proposed controls can only reduce and mitigate hacking risks associated with internet trading, but cannot eliminate them. Moreover, these are the minimum standards expected of internet brokers and are not meant to be exhaustive.

Detailed proposed requirements

The following wording is to be incorporated in the proposed guidelines to be issued under section 399(1) of the SFO.

1. Protection of clients' internet trading accounts

1.1. Two-factor authentication[4]

A licensed or registered person should implement two-factor authentication for login to clients' internet trading accounts.

A licensed or registered person should assess and implement a two-factor authentication solution which is commensurate with its business model.

[1] These include asset managers that distribute funds under their management through their internet-based trading facilities.

[2] For the avoidance of doubt, these baseline requirements shall only apply to leveraged foreign exchange traders licensed by the SFC.

[3] "Internet trading" for the purposes of these guidelines adopts the same meaning as in Paragraph 18 of the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (**Code of Conduct**), being "an arrangement where order instructions are sent to a licensed or registered person through its internet-based trading facility".

[4] Two-factor authentication refers to an authentication mechanism which utilizes any two of the following factors: what a client knows (eg, password), what a client has (eg, hardware token, one-time-password that will expire in a short period of time), and who a client is (ie, biometrics).

1.2. Implement monitoring and surveillance mechanisms

A licensed or registered person should implement an effective monitoring and surveillance mechanism to detect unauthorized access to clients' internet trading accounts. Examples include:

- Logging into multiple client accounts from the same internet protocol (**IP**) address; and

- Change of IP addresses for accessing the same client account (for example, from Hong Kong to London) in a short period of time.

1.3. Prompt notification to clients

A licensed or registered person should notify clients (eg, via email, short message service (**SMS**) or other push notifications) promptly after certain client activities have taken place in their internet trading accounts. These activities should at least include:

(a) System login;

(b) Password reset

(c) Trade execution;

(d) Fund transfer to third party; and

(e) Changes to client and account-related information.

The channel of notification to clients should be different from the one used for system login (as outlined in paragraph 1.1).

Clients may choose to opt out of "trade execution" notifications only. Under such circumstances, adequate risk disclosures should be provided by the licensed or registered person to the client and an acknowledgement should be executed by the client confirming that the client understands the risks involved in doing so.

1.4. Data encryption

A licensed or registered person should encrypt sensitive information such as client login credentials (ie, user ID and password) and trade data during transmission between internal networks and client devices, ie, end-to-end encryption. A licensed or registered person should also protect client login passwords stored in its internet trading system using a strong encryption algorithm.

1.5. Protection of client login passwords

A licensed or registered person should establish and implement effective policies and procedures to ensure that a client login password is generated and delivered to a client in a secure manner during the account activation and password reset processes. A client login password should be randomly generated by the system and sent to a client through a channel of communication which is free from human intervention and from tampering by staff of the licensed or registered person.

In a situation where a client login password is not randomly generated by the system, the licensed or registered person should implement adequate compensating security controls such as compulsory change of password upon the first login after client account activation.

1.6. Stringent password policies and session timeout controls

A licensed or registered person should set up stringent password policies and session timeout controls in its internet trading system, which include among others:

(a) Minimum password length;

(b) Maximum password age;

(c) Minimum password complexity (ie, alphanumeric) and history;

(d) Account lockout after multiple invalid login attempts; and

(e) Session timeout after a period of inactivity.

2. Infrastructure security management

2.1. Deploy a secure network infrastructure

A licensed or registered person should deploy a secure network infrastructure through proper network segmentation, ie, a Demilitarised Zone (**DMZ**) with multi-tiered firewalls, to protect critical systems (eg, internet trading system and settlement system) and client data against cyber-attacks.

2.2. User access management

A licensed or registered person should have policies and procedures in place to ensure that system access or the use of the systems are granted to users on a need-to-have basis. In addition, a licensed or registered person should review, at least on a yearly basis, the user access list of critical systems (eg, internet trading systems and settlement systems) and databases (eg, client data) to ensure that access to or use of the systems remain restricted to persons approved to use them on a need-to-have basis.

2.3. Security controls over remote connection

A licensed or registered person should grant remote access to its internal network on a need-to-have basis and implement security controls over such access.

2.4. Patch management

A licensed or registered person should monitor and evaluate security patches or hotfixes released by software provider(s) on a timely basis and, subject to an evaluation of the impact of the security patches or hotfix releases, implement the security patches or hotfixes within one month.

2.5. End-point protection

Anti-virus and anti-malware solutions (including the corresponding definition and signature files) should be implemented and updated on a timely basis to detect malicious applications and malware on critical system servers and workstations.

2.6. Unauthorized installation of hardware and software

A licensed or registered person should implement security controls to prevent unauthorized installation of hardware and software.

2.7. Physical security

A licensed or registered person should establish physical security policies and procedures to protect critical system components (eg, system servers and network devices) in a secure environment and to prevent unauthorized physical access to the facilities hosting the internet trading system as well as the critical system components.

2.8. System and data backup

A licensed or registered person should back up business records, client and transaction databases, servers and supporting documentation in an off-line medium on at least a daily basis. Full back up of the above should be performed before and after any major system changes.

2.9. Contingency planning for cybersecurity scenarios

In order to ensure that appropriate contingency procedures can be effectively executed when cybersecurity situations occur, a licensed or registered person should make all reasonable efforts to cover possible cyber-attack scenarios such as DDoS[5] and total loss of business records and client data resulting from cyber-attacks (eg, ransomware) in the business continuity plan (**BCP**) and crisis management procedures.

2.10. Third-party service providers

If a licensed or registered person has any arrangement to outsource any activities associated with its internet trading to a third-party service provider, it should enter into a formal service-level agreement with the service provider which specifies the terms of service and the responsibilities of the provider. In particular, a licensed or registered person should ensure that the services provided by the third-party service provider enable the licensed or registered person to comply with the relevant requirements set out in, among others, Paragraph 18 and Schedule 7 to the Code of Conduct and these guidelines. Service level agreements should be regularly reviewed and revised, where appropriate, to reflect any changes to the outsourcing arrangements or regulatory developments. Wherever possible, such agreements should provide sufficient levels of maintenance and technical assistance with quantitative details.

[5] In a distributed denial-of-service (**DDoS**) attack, multiple compromised computer systems attack a server, website or other network resource, and cause a denial of service for its users.

3. Cybersecurity management and supervision

3.1. Roles and responsibilities of cybersecurity management

The responsible officer(s) or executive officer(s) responsible for the overall management and supervision of the internet trading system should define a cybersecurity risk management framework (including but not limited to policies and procedures), and set out key roles and responsibilities. These responsibilities include, among others:

(a) Reviewing and approving cybersecurity risk management policies and procedures;

(b) Reviewing and approving the budget and spending on resources for cybersecurity risk management;

(c) Arranging to conduct a self-assessment of the overall cybersecurity risk management framework on a regular basis;

(d) Reviewing significant issues escalated from cybersecurity incident reporting;

(e) Reviewing major findings identified from internal and external audits and cybersecurity reviews; endorsing and monitoring the completion of remedial actions;

(f) Monitoring and assessing the latest cybersecurity threats and attacks;

(g) Reviewing and approving the BCP, which covers cybersecurity scenarios and corresponding contingency strategies, developed for the internet trading system; and

(h) Where applicable, reviewing and approving the service level agreement and contract with a third-party service provider relating to internet trading.

These responsibilities can be delegated, in writing, to a designated committee or operational unit, however overall accountability remains with the responsible officer(s) or executive officer(s).

3.2. Cybersecurity incident reporting

A licensed or registered person should establish written policies and procedures specifying the manner in which a suspected or actual cybersecurity incident should be escalated and reported internally (eg, to the responsible officer(s) or executive officer(s) in charge of internet trading) and externally (eg, to clients, the SFC and other enforcement body, where appropriate).

3.3. Cybersecurity awareness training for internal system users

A licensed or registered person should provide cybersecurity awareness training to all internal system users[6] at least on a yearly basis. Training programmes should be

[6] Internal system users refers to any permanent and contract staff who have access to the internal network and systems of a licensed or registered person.

updated to include the latest cybersecurity-related rules and regulations and current and emerging cybersecurity threats and trends as well as corresponding measures.

3.4. Cybersecurity alert and reminder to clients

A licensed or registered person should take all reasonable steps to remind and alert clients of cybersecurity risks and recommended preventive and protection measures when using the internet trading system, such as that login credentials should be properly safeguarded and cannot be shared.

Appendix C

Amendments to the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission

Paragraph 18 – Electronic trading

18.1 Application

This paragraph applies to a licensed or registered person which conducts electronic trading of securities and futures contracts that are listed or traded on an exchange or internet trading of securities that are not listed or traded on an exchange.

18.2 Interpretation

(f) “Internet trading” for the purposes of this paragraph means an arrangement where order instructions are sent to a licensed or registered person through its internet-based trading facility. An internet-based trading facility may be accessed through a computer, mobile device or other electronic device.

Schedule 7 – Additional requirements for licensed or registered persons conducting electronic trading

Introduction

Paragraph 18 of the Code stipulates the general principles that apply to a licensed or registered person which conducts electronic trading of securities and futures contracts that are listed or traded on an exchange or internet trading of securities that are not listed or traded on an exchange. This Schedule sets out the specific requirements in this regard.

Appendix D

Common Two-Factor Authentication Controls

Two-factor authentication (**2FA**) should be enforced for login to clients' internet trading accounts.

The following table summarizes the implementation cost, impact on user experience, the advantages and disadvantages of four types of common 2FA controls for reference purposes.

	SMS OTP (short message service one-time password)	**Digital certificate**	**Hardware token**	**Software token**
Implementation cost	Low	Medium	High	Low
Impact on user experience	Low	Low	High	Medium
Advantages	(i) SMS service is available for subscription and (ii) Users have widely adopted this approach	Technology proven and reliable	Users can initiate transaction regardless of their locations and end-point devices	(i) Users are not required to carry a physical token for authentication and (ii) Better interoperability with mobile devices
Disadvantages	Users must have active mobile network connectivity; roaming charges and delay may incur for users on cellular data network overseas	(i) Additional cost to maintain infrastructure for digital certificate management and certificate renewal and (ii) Not widely compatible with mobile devices	(i) Relatively higher implementation and maintenance cost and (ii) Users are required to physically carry the hardware token	Additional cost to maintain infrastructure for software token management