CHARLTONS
SOLICITORS

Hong Kong **November** 2017

Internet Trading Hacking Risks: New SFC Guidelines

Introduction

On 27 October 2017, the Securities and Futures Commission (**SFC**) issued Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading[1] (**the Guidelines**), following a public consultation. The Hong Kong Monetary Authority also issued a circular[2] requiring institutions registered with the SFC to conduct regulated activities to implement the Guidelines' requirements to enhance the security of their internet trading services.

The SFC Guidelines will require all SFC-licensed corporations and banking institutions registered with the SFC (together **intermediaries**) which are engaged in internet trading to implement 20 baseline requirements to enhance cybersecurity resilience and reduce and mitigate hacking risks.

Internet trading is defined as an arrangement where order instructions are sent to a licensed or registered person through its internet-based trading facility, the definition used in the Code of Conduct for Persons Licensed by or Registered with the SFC (the **Code of Conduct**) at paragraph 18.2(f). The Guidelines will apply to intermediaries conducting regulated activities Type 1 (dealing in securities), Type 2 (dealing in futures contracts), Type 3 (leveraged foreign exchange trading) and Type 9 (asset management) to the extent that they distribute funds under their management through internet-based trading activities. Failure to follow the Guidelines may affect an entity's fitness and properness to remain SFC-licensed or registered.

Timeline

The requirement for the implementation of two-factor authentication for clients to log into their internet trading accounts, will take effect on 27 April 2018. All other requirements will become effective on 27 July 2018.

Protection of clients' internet trading accounts

1. **Two-factor authentication**

   Intermediaries will be required to implement two-factor authentication for clients to log into their internet trading accounts. Two-factor authentication uses any two of the following factors: (i) what a client knows; (ii) what a client has; and (iii) who a client is. The authentication solution adopted should be commensurate with the intermediary's business model.

2. **Implement monitoring and surveillance mechanisms**

   An effective monitoring and surveillance mechanism will be required to be implemented in order to identify unauthorised access to clients' internet trading accounts.

1 http://www.sfc.hk/web/EN/assets/components/codes/files-current/web/guidelines/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading.pdf

2 http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2017/20171027e1.pdf

3. **Prompt client notification**

Clients must be notified promptly (e.g. by email, short message service or other push notifications) after certain client activities have occurred in their internet trading accounts which should include, at least the following: (i) system login; (ii) password reset; (iii) trade execution (iv) fund transfer to non-registered third party accounts; and (v) changes to client and account-related information.

Clients can opt out of trade execution notifications only. This is subject to the intermediary disclosing the risks of opting out to the client and the client's execution of an acknowledgement confirming his understanding of those risks. Client notifications must be made sent via a channel different to the one used for system login.

4. **Data encryption**

Intermediaries are required to use a strong data encryption algorithm to encrypt sensitive information, such as login credentials (user id and password) and trade data during transmissions between internal networks and client devices, and to protect client login passwords stored in their internet trading systems.

5. **Password protection**

The Guidelines require intermediaries to establish effective procedures for the generation of secure random passwords and their delivery to clients through a channel of communication which is free from human intervention and from tampering by intermediaries' staff. Where a client login password is not randomly generated, intermediaries will be required to implement compensating security control measures, such as a mandatory password change upon the first login after the account activation.

6. **Stringent password policies and controls on session timeout**

Stringent password policies and session timeout controls should be set up for the internet trading system, including: minimum password length; periodic reminders for clients who have not changed their passwords for a long period of time; minimum password complexity (i.e. alphanumeric) and history; appropriate controls on invalid login attempts and session timeouts.

Infrastructure security management

7. **Secure network infrastructure**

Intermediaries should deploy a secure network infrastructure via proper network segmentation, i.e. a demilitarized zone with multi-tiered firewalls, to protect critical systems (such as the internet trading and settlement systems) and client data against cyber-attacks.

8. **Management of user access**

System access to the network should be granted to users on a need-to-have basis. Intermediaries should review the user access list of critical systems (such as the internet trading and settlement systems) and databases (e.g. client data) at least annually to ensure that access to or use of the systems remain restricted to persons approved to use them on a need-to-have basis.

9. **Security controls over remote connection**

Remote access to intermediaries' internal network should also be given on a need-to-have basis with security controls over such access.

10. **Patch management**

Software providers' security patches or hotfixes will need to be monitored and implemented within one month following the completion of testing.

11. **End-point protection**

Anti-virus and anti-malware solutions will need to be implemented and updated on a timely basis to detect malicious applications and malware on critical system servers and workstations.

12. **Unauthorised installation of hardware and software**

Security controls will be required to prevent the unauthorised installation of hardware and software.

13. **Physical security**

Physical security policies and procedures will need to be established to protect critical system components and to prevent unauthorised physical access to the facilities hosting the internet trading system and critical system components.

14. **System and data backup**

Offline system and data backup will be required for business records, client and transaction databases, servers and supporting documentation at least daily. An appropriate recovery method will also need to be adopted to allow successful roll-back of major system changes.

15. **Contingency planning for cybersecurity scenarios**

Contingency plans and crisis management procedures will need to cover possible cyber-attack scenarios such as distributed denial-of-service attacks and total loss of business records and client data resulting from cyber-attacks (e.g. ransomware).

16. **Third-party service providers**

Third-party internet trading service providers should be engaged only via a formal service-level agreement with specified provider responsibilities and terms of service, which should be regularly reviewed. Services provided by the outsourcing company must enable the intermediary to comply with the relevant requirements of Paragraph 18 and Schedule 7 to the Code of Conduct and the Guidelines.

Cybersecurity management and supervision

17. **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 will need to define a cybersecurity risk management framework and set out key roles and responsibilities. The responsibilities will include:

a) reviewing and approving cybersecurity risk management policies and procedures and the cybersecurity risk management budget;

b) arranging regular self-assessments of the overall cybersecurity risk management framework;

c) reviewing significant issues escalated from cybersecurity incident reporting;

d) reviewing major findings identified from internal and external audits and cybersecurity reviews, and endorsing and monitoring the completion of remedial actions;

e) monitoring and assessing the latest cybersecurity threats and attacks;

f) reviewing and approving the contingency plan developed for the internet trading system; and

g) where applicable, reviewing and approving the service level agreement and contract with a third-party internet trading service provider.

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

18. **Cybersecurity incident reporting**

Written policies and procedures will need to specify how suspected or actual cybersecurity incidents should be escalated and reported internally (e.g. to the responsible/executive officer(s) in charge of internet trading) and externally (e.g. to clients, the SFC and any other relevant enforcement bodies).

19. **Cybersecurity awareness training for internal systems users**

Adequate cybersecurity awareness training will need to be provided to all internal system users at least annually, with the training content designed to reflect the type and level of cybersecurity risks faced by the intermediary.

20. **Cybersecurity alert and reminder to clients**

Intermediaries should take all reasonable steps to remind clients about, and to alert them to cybersecurity risks and recommended preventative and protective measures

when using the internet trading system, for example, that login credentials should be properly safeguarded and cannot be shared.

CHARLTONS

Boutique Transactional Law Firm of the Year 2017
Asian Legal Business Awards

This newsletter is for information purposes only.

Its contents do not constitute legal advice and it should not be regarded as a substitute for detailed advice in individual cases.

Transmission of this information is not intended to create and receipt does not constitute a lawyer-client relationship between Charltons and the user or browser.

Charltons is not responsible for any third party content which can be accessed through the website.

If you do not wish to receive this newsletter please let us know by emailing us at unsubscribe@charltonslaw.com

---

Hong Kong Office
Dominion Centre
12th Floor
43-59 Queen's Road East
Hong Kong
Tel: + (852) 2905 7888
Fax: + (852) 2854 9596

www.charltonslaw.com