Hong Kong SFC and HKMA Issue New Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading

November 1, 2017

On October 27, 2017, the Hong Kong Securities and Futures Commission ("SFC") issued Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (the "Guidelines"),[1] a set of baseline cybersecurity requirements that all persons licensed or registered with the SFC and engaged in internet trading will be required to implement. The Hong Kong Monetary Authority ("HKMA") simultaneously issued a circular to CEOs of Registered Institutions requiring them to apply the Guidelines.[2]

The new guidelines should be viewed as requirements for securities and futures dealers and asset managers registered with the SFC and banks supervised by the HKMA (which include a number of foreign banks that operate branches in Hong Kong). For e-commerce firms and other companies that do business in or have connections to Hong Kong, the new guidelines should additionally be viewed as relevant guidance for best practices in cybersecurity.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors:

WASHINGTON

Katherine Mooney Carroll
+1 202 974 1584
kcarroll@cgsh.com

Nowell Bamberger
+1 202 974 1752
nbamberger@cgsh.com

NEW YORK

Jonathan S. Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

HONG KONG

Freeman Chan
+852 2532 3788
fchan@cgsh.com

1 Hong Kong Securities And Futures Commission Circular, Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (October 27, 2017), 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 Hong Kong Monetary Authority Circular, "Security Controls for Internet trading services" (October 27, 2017), http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2017/20171027e1.pdf.

I. The Guidelines Requirements

The Guidelines require all licensed or registered persons engaged in internet trading to implement 20 baseline requirements covering three broad categories:[3]

1. Protection of clients' internet trading accounts;

2. Infrastructure security management; and

3. Cybersecurity management and supervision.

Many of the requirements follow international standards of best-practice that most firms already follow, but all potentially-affected firms should conduct an analysis to ensure they are in compliance with the Guidelines at least by their effective dates. One specific requirement – the requirement to use two-factor authentication for all internet trading sites – takes effect on April 27, 2018. The remaining requirements enter force on July 27, 2018, although the SFC and HKMA will expect non-system related changes to be made well before the effective date.

Important features of the Guidelines include the obligations to:

— Implement two-factor authentication, mirroring a recommendation made by the HKMA in a May 26, 2016 circular,[4]

— Designate an officer responsible for cybersecurity management who, by virtue of that designation, assumes responsibility for self-assessing the firm's cybersecurity risk, reviewing incident reports, and approving cybersecurity risk-management policies and procedures,

— Provide cybersecurity awareness training for internal system users, and

— Ensure the effectiveness of the controls used by third-party service providers, including by entering into a service-level agreement with such providers that provides for compliance with the Guidelines (and any other related SFC Code of Conduct provisions).

Appendix A contains a more detailed summary of the Guidelines requirements. The SFC also published a detailed FAQ addressing questions that may arise as firms implement the Guidelines requirements. Firms that operate in Hong Kong, and particularly those subject to SFC or HKMA supervision, should consider these requirements as part of a periodic evaluation of their cybersecurity risk management policies. For firms not directly subject to the requirements, the Guidelines provide useful guidance reflecting international best practices for cybersecurity.

II. Regulatory Framework

While the Guidelines do not have the formal force of law, they were adopted by the SFC pursuant to its authority under Section 399 of the Hong Kong Securities and Futures Ordinance, which empowers the SFC to adopt guidelines applicable to entities it supervises.

Moreover, both the SFC and the HKMA have stated that they will incorporate the Guidelines into their supervisory processes, concluding that compliance with the Guidelines will be viewed as relevant to assessing whether a supervised institution is "fit and proper" to remain licensed to conduct regulated activities in Hong Kong. The HKMA intends to incorporate the Guidelines into its Supervisory Policy Manual in due

[3] The Guidelines apply to persons which are engaged in internet trading and are licensed by, or registered with, the SFC for: Type 1 regulated activity (dealing in securities); Type 2 regulated activity (dealing in futures contracts); Type 3 regulated activity (leveraged foreign exchange trading); and/or Type 9 regulated activity (asset management) to the extent they distribute funds under their management through their internet-based trading facilities.

[4] See Hong Kong Monetary Authority, Security Controls Related To Internet Banking Services (May 26, 2016), http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20160526e1.pdf.

course. As a result, implementation of the Guidelines is effectively mandatory for entities supervised by the SFC and HKMA, given the potential impact of a breach on their licensed status in Hong Kong.

III. The International Perspective

The SFC and HKMA join an increasing number of authorities around the world issuing guidance with respect to cybersecurity issues. A recent report by the Financial Stability Board regarding cybersecurity regulation in the financial services sector concluded that there is a growing emphasis on cybersecurity regulation, but that most jurisdictions draw upon a small body of previously developed practice and that there was a lack of uniformity in the approach to cybersecurity across jurisdictions.[5]

In the U.S., for example, the Securities and Exchange Commission has published guidance on cybersecurity issues, although that guidance is not mandatory.[6] In New York, the Department of Financial Services implemented cybersecurity regulations that took effect August 28, 2017 and imposed extensive requirements, similar in some respects to those reflected in the Guidelines, and notable in their requirement that regulated firms appoint a Chief Information Security Officer. Our August 21, 2017 alert memorandum provides additional information about the New York DFS requirements. In the U.K., the Financial Conduct Authority has published high-level guidance emphasizing the importance of cybersecurity, while imposing a requirement only that supervised firms report cybersecurity breaches pursuant to their general obligation of transparency with regulators.[7] The European Union's General Data Protection Regulation, which comes into force in May 2018, imposes additional obligations on firms operating in the E.U., as described in our May 3, 2017 alert memorandum.

While the SFC's Guidelines do not directly mirror the requirements set out in other jurisdictions, they provide baseline requirements that are unlikely to conflict with either firms' existing cybersecurity initiatives or with regulatory requirements in other jurisdictions.

Cleary Gottlieb provides continuing coverage of developments in cybersecurity issues in our Cybersecurity and Privacy Watch blog at www.clearycyberwatch.com.

…

CLEARY GOTTLIEB

[5] See Financial Stability Board, Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices (October 13, 2017), http://www.fsb.org/wp-content/uploads/P131017-2.pdf.

[6] See, e.g., Securities and Exchange Commission, IM Guidance Update (April 2015), https://www.sec.gov/investment/im-guidance-2015-02.pdf.

[7] See Financial Conduct Authority, Cyber resilience, https://www.fca.org.uk/firms/cyber-resilience.

Appendix A

The following is a summary of the requirements under the October 27, 2017 Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading published by the Hong Kong Securities and Futures Commission:

1. **Protection of Clients' Internet Trading Accounts**. To ensure the protection of clients' internet trading accounts the Guidelines require licensed or registered persons to implement six controls:

   - Two-factor authentication for login to clients' internet trading accounts.[1]

   - Effective monitoring and surveillance mechanisms to detect unauthorized access to clients' internet trading accounts. While the Guidelines do not specify a particular monitoring or surveillance regime, but leave to each institution the obligation to ensure that its system is effective, the SFC's FAQ notes that an internet broker could, for example, monitor (i) logging into multiple client accounts from the same IP address; and (ii) change of IP address for accessing the same client account from one country to another country in a short period of time.

   - Prompt notification to clients after certain activities have taken place in their internet trading accounts. Note that the channel used for such notification should differ from the one used for system login. These activities include: (i) system login; (ii) password reset; (iii) trade execution;[2] (iv) fund transfers to third party accounts unless the accounts have been registered with the licensed or registered persons prior to the transfer; and (v) changes to client account-related information. The Guidelines do not define the requirement that notification be "prompt."

   - Strong encryption algorithms to: (i) encrypt sensitive information such as client login credentials and trade data during transmission between internal networks and client devices; and (ii) protect client login passwords stored in its internet trading system.

   - 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. Ideally, a client login password should be randomly generated by the system; in a situation in which it is not, the licensed or registered person should implement security controls that adequately compensates for this failure such as compulsory change of password upon the first login after account activation.

   - Stringent password policies and session timeout controls in its internet trading system, which include: (i) minimum password length; (ii) periodic reminders for those clients who have not

[1] Two-factor authentication refers to an authentication mechanism which utilizes any two of the following factors: what a client knows, what a client has, and who a client is.

[2] Clients may choose to opt out from "trade execution" notifications only. In the event they choose to do so, adequate risk disclosures should be provided by the licensed or registered person to the client and an acknowledgment should be executed by the client confirming the client understands the risk involved in doing so.

changed their passwords for a long period; (iii) minimum password complexity (i.e. alphanumeric) and history; (iv) appropriate controls on invalid login attempts; and (v) session timeout after a period of inactivity.

2. **Infrastructure Security Management**. Along with controls for protecting access to clients' trading accounts, the Guidelines provide ten measures for ensuring infrastructure security. Licensed or registered persons should:

   a. Deploy a secure network infrastructure through proper network segmentation, i.e., a demilitarized zone with multi-tiered firewalls.

   b. Establish policies and procedures to ensure that system access is granted to users on a need-to-have basis. In addition, reviews should be conducted, on at least a yearly basis, to ensure that user access to critical systems and databases is restricted to persons on a need-to-have basis.

   c. Grant remote access to internal networks on a need-to-have basis and implement security controls over such access.

   d. Monitor and evaluate security patches or hotfixes released by software providers on a timely basis and, subject to an evaluation of the impact, conduct testing as soon as practicable and implement the security patches or hotfixes within one month following the completion of testing.

   e. Implement and update anti-virus and anti-malware solutions on a timely basis.

   f. Implement security controls to prevent unauthorized installation of hardware and software.

   g. Establish physical security policies and procedures to protect critical system components and to prevent unauthorized physical access to the facilities hosting the internet trading system as well as the critical system components.

   h. Back up business records, client and transaction databases, servers and supporting documentation in an off-line medium on at least a daily basis.

   i. Make all reasonable efforts to cover possible cyber-attack scenarios such as distributed denial-of-service (DDoS) attacks[3] and total loss of business records and client data resulting from cyber-attacks (e.g. ransomware) in the contingency plan and crisis management procedures.

   j. In the event 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

[3] In a DDoS attack, multiple compromised computer systems attack a server, website or other network resource, and cause a denial of service for its users.

service-level agreement with the service provider which specifies the terms of service and the responsibilities of the provider.

3. **Cybersecurity Management and Supervision**. The Guidelines outline the key roles and responsibilities that the responsible officer(s) or executive officer(s) in charge of the overall management and supervision of the internet trading system should define as part of a licensed or registered person's cybersecurity risk management framework. 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). The responsibilities include: (i) reviewing and approving cybersecurity risk management policies and procedures; (ii) reviewing and approving the budget and spending on resources for cybersecurity risk management; (iii) arranging to conduct a self-assessment of the overall cybersecurity risk management framework on a regular basis; (iv) reviewing significant issues escalated from cybersecurity incident reporting; (v) reviewing major findings identified from internal and external audits and cybersecurity reviews; (vi) monitoring and assessing the latest cybersecurity threats and attacks; (vii) reviewing and approving the contingency plan, which covers cybersecurity scenarios and corresponding contingency strategies, developed for the internet trading system; and (viii) where applicable, reviewing and approving the service level agreement and contract with a third-party service provider relating to internet trading.

   Licensed or registered persons should also establish written policies and procedures specifying the manner in which a suspected or actual cybersecurity incident should be escalated and reported internally and externally. In addition, licensed or registered persons should provide adequate cybersecurity awareness training to all internal system users on, at least, a yearly basis, and should tailor the content of the training program to the type and level of cybersecurity risks it faces. Also, licensed or registered persons should take reasonable steps to alert clients to 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.