Review of Internet Trading Cybersecurity

The Securities and Futures Commission ("**SFC**") had issued a report and a circular on 23 September 2020 to elaborate the regulatory expectations set out in the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading that came into effect in July 2018. This explanatory note summarizes the fact-findings and guidance on specific system security controls which internet brokers should employ for mobile trading applications as provided in the above.

Two-Factor Authentication ("2FA") for systems logins

Deficiencies	Measures Proposed by SFC
• Clients were allowed to deactivate 2FA for system logins. • Delivery of One-Time Password (the "OTP") by email is not an effective second authentication factor. • There were problems with binding clients' devices such as technical security loopholes or allowing clients to bind an excessive number of devices.	• Not to allow clients to deactivate 2FA for system logins. • Not to deliver the OTP by email. • Regularly perform technical assessments to identify security loopholes. • Not to allow clients to bind or register an excessive number of devices to their internet trading account, and internet brokers should implement controls over concurrent logins.

Monitoring and surveillance mechanisms to detect unauthorized access

Deficiencies	Measures Proposed by SFC
• Some internet brokers only reviewed client transactions manually. • Monitoring and surveillance only performed on an ad hoc, weekly or monthly basis. • Design flaws in automated internet protocol ("IP") address monitoring tools.	• Internet brokers should consider the scale of their internet trading operations and implement a monitoring and surveillance mechanism which is appropriate and commensurate with their business needs. • Internet brokers should perform monitoring and surveillance at least daily. • Internet brokers should conduct sufficient technical and user testing before implementing an automated IP address monitoring tool.

Data encryption

Deficiency	Measure proposed by the SFC
Some firms failed to adequately encrypt and protect client login credentials, passwords and trading data as they were using encryption algorithms which did not meet international security standards.	Internet brokers should review international security standards on an ongoing basis, check the status of their data encryption algorithms and upgrade them as appropriate.

Session timeout

Deficiencies	Measures proposed by the SFC
• Session timeout could be disabled by clients. • The idle timeout period could be as long as 24 hours.	• Not to allow clients to disable session timeout. • Internet brokers should limit the idle timeout period (e.g. within 30 minutes) subject to prior assessments and ongoing monitoring. • Internet brokers should perform sufficient testing to ensure session timeout controls are configured and functioning properly.

Security Controls for remote connections

Deficiency	Measure proposed by the SFC
Some vendors were granted remote access at all times which increased cybersecurity risks.	Internet brokers should avoid granting permanent remote access to external parties.

Cybersecurity management and supervision

Deficiency	Measure proposed by the SFC
A large number of firms did not sufficiently cover baseline requirements in their IT audits or self-assessments.	Internet brokers should review their compliance with the baseline requirements in their IT audit or cybersecurity assessments at least annually.

Mobile Trading Applications

Deficiencies	Measures proposed by the SFC
• Unable to detect and block compromised devices from logging into the internet brokers' internet trading systems. • Not adequately protecting their source codes which could allow hackers to by-pass built-in security controls. • Unused code libraries or modules in the mobile trading applications result in an increased risk of hackers installing malware. • Some allowed storage of clients' sensitive information in the mobile devices and such information was not removed from system process memory after logoff. This increased risk that information is accessed by hackers. • Client's biometric data stored in the client's mobile device was allowed to be amended without proper validation and did not disable biometric authentication after repeated failed attempts.	• Internet brokers should detect and block compromised devices from logging into their internet trading systems. • Source codes should be obfuscated to better protect internet brokers from manipulation. • Unused code libraries or modules should be purged from their source codes. • Clients' sensitive information should be removed from their internet trading applications installed on clients' mobile devices once the clients exit the applications or log off their internet trading accounts. • Internet brokers should tighten security controls for biometric authentication, for example:- o Any changes to clients' biometric data should be subject to validation checks; and o Limiting the number of failed authentication attempts.

Given the technical nature of this subject matter, internet brokers should seek professional assistance from their vendors and other consultants as needed.

Should you have any question, please contact our Mr Lawrence Yeung on (852) 2854 3070 or by email at lawrence.yeung@ycylawyers.com.hk.

This explanatory note is not, and should not be regarded as, legal advice. Should you have any enquiries, please seek specific advice from legal advisers.

24 February 2021