Client Update
SFC Cybersecurity Review of Internet/Mobile Trading Systems

HONG KONG
Mark Johnson
mdjohnson@debevoise.com

Ralph Sellar
rsellar@debevoise.com

NEW YORK
Jim Pastore
jjpastore@debevoise.com

WASHINGTON, D.C.
Luke Dembosky
ldembosky@debevoise.com

LONDON
Robert Maddox
rmaddox@debevoise.com

On 13 October 2016, the Hong Kong Securities and Futures Commission ("SFC") announced a review of the cybersecurity preparedness, compliance and resilience of brokers' internet/mobile trading systems. A link to the SFC's notice can be found here.

The review follows 16 reported hacking incidents which involved 7 securities brokers and total unauthorized trades in excess of HK$100 million.

The review will comprise three components:

- A questionnaire provided to a mix of small to medium sized securities and futures brokers as well as leveraged foreign exchange traders. The primary objective is to assess the cybersecurity aspects of internet/mobile trading systems.
- Onsite inspections of selected brokers for a deep dive review of their information technology and other related management controls and an assessment of their design and effectiveness in preventing and detecting cyberattacks.
- Benchmarking the SFC regulatory requirements and market practices in Hong Kong against requirements of major financial services regulators and other relevant market practices in Hong Kong or elsewhere.

The findings of this review will be used by the SFC to further develop policy to improve overall cybersecurity resilience in the markets.

Cybersecurity management is a key priority for the SFC's supervision of licensed corporations ("LCs") and the SFC has promulgated a number of Circulars setting out in detail the cybersecurity controls which it expects LCs to implement. In particular, in addition to controls for the detection and prevention of

cyberattacks, the SFC also expects LCs to have a written contingency plan for dealing with cyberattacks when they happen. The SFC has urged LCs to review and enhance their cybersecurity controls in light of the latest incidents. LCs which fail to implement adequate cybersecurity controls risk enforcement action.

The SFC's activities closely mirror steps other regulators worldwide have taken with respect to cybersecurity. The U.S. Securities and Exchange Commission ("SEC") Office of Compliance Inspections and Examinations ("OCIE"), for instance, conducted a similar sweep, resulting in a published report in February 2015. The SEC has since brought three actions against registered investment advisors for cybersecurity lapses. Similarly, the New York Department of Financial Services last month proposed stringent cybersecurity regulations for regulated banks (including foreign banks operating in New York) and insurance companies.

The UK Financial Conduct Authority ("FCA") is also crystallizing its stance on cybersecurity and has publically stated that all UK regulated entities should address cyberscurity threats, irrespective of their size or services offered. In non-binding comments, the FCA has also signaled that firms should have a "security culture" that permeates from the board to every employee, as well as calling for greater information sharing both with the regulator and between financial institutions. While the FCA is yet to issue specific cybersecurity requirements, it is clear that it will use the existing regulatory regime to enforce against firms which fail to implement adequate systems and controls to address cyber risk or report significant incidents when they occur.

* * *

Debevoise & Plimpton has a leading cybersecurity practice. If you would like to discuss any of the issues arising from this notice or how your company's cybersecurity controls can be enhanced, please do not hesitate to contact us.