Monetary Authority of Singapore

SECURITIES AND FUTURES ACT (CAP. 289)

FREQUENTLY ASKED QUESTIONS (FAQs) ON TWO-FACTOR AUTHENTICATION FOR ONLINE TRADING PLATFORMS

Disclaimer: The FAQs are meant to provide guidance to the industry on MAS' policy and administration of the SFA regime. They do not constitute legal advice. MAS expects industry participants to retain their independent legal counsel to advise them on how their business operations should be conducted in order to satisfy the legal/regulatory requirements and to advise them on all applicable laws of Singapore.

Issued on 14 December 2016

Two-Factor Authentication (2FA)

Q1. What is 2FA and why is it important?

Two-factor authentication for system login can be based on any two of the factors, i.e. What you know (e.g. PIN), What you have (e.g. One-Time-Password (OTP) token) and Who you are (e.g. Biometrics). A common form of 2FA involves the user entering his password as the first factor, together with a OTP generated by either a hardware token or delivered to the user via Short Message Service (SMS), to log in to an online system.

The primary objective of two-factor authentication is to secure the customer authentication process and to protect online customer accounts against unauthorised access. When implemented properly, 2FA offers much greater protection against hacking than single-factor password authentication, and helps to safeguard online user accounts from unauthorised access even when the passwords have been compromised.

Q2. Is the implementation of 2FA for online trading platforms mandatory for all Financial Institutions (FIs)?

Given the prevalence of cyber threats and incidents, MAS expects FIs to adhere closely to the MAS Technology Risk Management Guidelines to secure their online financial services. FIs which offer trading of capital markets products using online trading platforms and still using only single-factor password authentication for login to such platforms should enhance their controls with a stronger authentication mechanism.

In this regard, all FIs which are licensed or exempted under Section 99 of the Securities and Futures Act (Cap. 289) ("SFA") to deal in securities, trade in futures contracts and/or conduct leveraged foreign exchange trading should make available 2FA for the online trading accounts of all customers, other than institutional investors[1].

Q3. What if customers choose not to adopt 2FA?

FIs should highlight the security risks of single-factor authentication to all customers and encourage their adoption of 2FA given the associated risks of not doing so. Where a customer chooses not to opt for 2FA, the FI should document the customer's choice and obtain the customer's acknowledgement of the attendant risks.

---

[1] As defined in section 4A of the SFA.

Q4. Aside from 2FA, what other security measures should be put in place by brokers to detect or deter unauthorized trading?

2FA is only one of the many security controls that can be implemented for online financial systems. In addition to implementing 2FA, FIs are expected to strengthen internal controls to further mitigate the risk of unauthorised trades. In particular, brokers should:

(i) provide prompt notification to customers (e.g. via SMS, email or push notification) on the execution of trades, as well as changes to customer and account-related information;

(ii) implement stringent password policies (e.g. on password length and complexity); and

(iii) step up their efforts to raise customers' awareness of the risks associated with online trading, so that customers are able to make informed choices on whether to adopt 2FA.

Q5. Is there a timeline for FIs to implement 2FA for their online trading services?

FIs that have yet to offer 2FA for online trading in securities should do so by 21 September 2017, while FIs that have yet to implement 2FA for online trading in other product classes (i.e. futures and leveraged foreign exchange) should do so by 21 March 2018.