2FA Risk Awareness Statement

1. What is 2FA?

2FA (also known as two-factor authentication) is the verification of a user's online identity using two distinct factors.

The current practice used by financial institutions in Singapore is to require clients to go through a 2-factor authentication process – (1) a Personal Identification Number (PIN), which is issued by the financial institution and (2) a One-Time Password (OTP), which is generated by a hardware token device or software token application, or sent via a Short Message Service (SMS) to the client. This is also the same practice adopted by Schwab. When a Schwab client who has elected to participate in 2FA wishes to access an online service by Schwab, the client is required to enter the PIN and the OTP for authentication.

2. What is the purpose of 2FA?

The key objectives of 2FA are to protect the client's online trading account and information from unauthorized access, and enhance the overall security of online trading systems.

Schwab take's a proactive role in protecting our clients. We have risk mitigating measures in place to protect your online trading account and information from unauthorized access. Please contact Schwab for more details.

3. Is 2FA compulsory for trading through Schwab?

2FA is not compulsory for trading through Schwab. Nonetheless, clients are strongly encouraged to use 2FA on their online trading accounts. Clients that elect to use 2FA for login will be required to provide both PIN and OTP to access the online trading services. Clients should exercise due care to safeguard their PIN and OTP, and not disclose them to other parties.

For users of hardware tokens, any loss or theft of the token shall be reported to Schwab or OTP provider immediately. The lost/stolen token will be disabled and the user will not be able to access his online trading account until such time when he completes the de-registration process and a new token is received. There may be a fee for the token. Please contact Schwab for more details.

4. What if I choose not to use 2FA for trading through Schwab?

In general, single-factor password authentication is more susceptible to password-based attacks and malware that could result in the compromise and hijacking of online trading accounts by unauthorized parties. This could in turn lead to unauthorized disclosure of your personal and trading information that may be available on the online trading account, or the carrying out of fraudulent trades through your online trading account. Choosing not to use 2FA for the online trading account would increase your exposure to these risks.

5. How can I protect myself if I choose not to use 2FA for online trading through Schwab?

You should observe the following practices to secure the confidentiality and integrity of your password and PIN (for funds transfer), security tokens, personal details and other confidential data as far as possible. These will help to prevent unauthorised transactions and fraudulent use of your accounts and make sure that no one else would be able to observe or steal your access credentials or other security information to impersonate them or obtain unauthorised access to your online accounts:

You should:

(a) Take the following precautions as regards your PIN and password (“credentials”);

- Credentials should be at least 8 characters of alphanumeric mix;
- Credentials should not be based on guessable information such as user-id, personal telephone number, birthday or other personal information;
- Credentials should be kept confidential and not be divulged to anyone;
- Credentials should be memorised and not be recorded anywhere;
- Credentials should be changed regularly or when there is any suspicion that it has been compromised or impaired; and
- The same PIN should not be used for different websites, applications or services, particularly when they related to different entities,

(b) Not select the browser option for storing or retaining user name and password

(c) Check the authenticity of our website by comparing the URL and our name in its digital certificate or by observing the indicators provided by an extended validation certificate;

(d) Check that the website address changes from ‘http://’ to ‘https://’ and a security icon that looks like a lock or key appears when authentication and encryption is expected;

(e) Check your account information, balance and transactions frequently and report any discrepancy;

(f) Install anti-virus, anti-spyware and firewall software in your personal computers and mobile devices;

(g) Update operation system, virus and firewall products with security patches or newer versions on a regular basis;

(h) Remove file and printer sharing in computers, especially when they are connected to the internet;

(i) Make regular backup of critical data;

(j) Consider the use of encryption technology to protect highly sensitive or confidential information;

(k) Log off each and every online session;

(l) Clear browser cache after each and every online session;

(m) Not install software or run programs of unknown origin;

(n) Delete junk or chain emails;

(o) Not open email attachments from strangers;

(p) Not disclose personal, financial or credit card information to little-known or suspect websites;

(q) Not use a computer or a device which cannot be trusted; and

(r) Not use public or internet café computers to access online services or perform financial transactions.

(1017-ZHC8) REG98874SG-00