2FA Risk Awareness Statement

1. What is 2FA?

Two-Factor Authentication (2FA) is a trusted technology that allows financial institutions to verify your online identity using two distinct factors:

1. Your Personal Identification Number (PIN); and

2. A One-Time Password (OTP), which is generated by a hardware token device, sent via a Short Message Service (SMS) or generated by Google Authenticator (mobile app).

If you elect to use 2FA authentication with your OANDA account, you will then need to enter the OTP after your PIN when you log into your account.

2. What is the purpose of 2FA?

The key objectives of 2FA are to protect your online trading account and information from unauthorised access, and to enhance the overall security of our online trading platform.

3. Is 2FA compulsory for trading through OANDA Asia Pacific?

2FA is not compulsory when trading with OANDA Asia Pacific, however you are strongly encouraged to use 2FA when logging into your OANDA account. If you elect to use 2FA for login, you will be required to provide both your PIN and OTP to access our online trading services. You should also exercise due care to safeguard your PIN and OTP, and not disclose them to other parties.

4. What if I choose not to use 2FA for trading through OANDA Asia Pacific?

In general, single-factor password authentication is more susceptible to password-based attacks and malware that could result in the compromise and hijacking of your online trading accounts by unauthorised parties. This could also result in the unauthorised disclosure of any personal and trading information that is available in your OANDA account, or unlawful activity and fraudulent trades from your online trading account. By choosing not to use 2FA, you could increase your exposure to these risks.

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

You should observe the following practices to help secure the confidentiality and integrity of your password and PIN, personal details and other confidential data as far as possible. These will help mitigate the risk of unauthorised transactions and fraudulent use of your accounts and reduce the chance of unlawful parties observing or stealing your access credentials or other security information with a view to obtaining unauthorised access to your online accounts:

(a) Take the following precautions with 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, telephone number, birthday or other personal information;
- Credentials should be kept confidential and not be divulged to anyone;
- Credentials should be changed regularly or when there is any suspicion that your online identity 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) Do not select the browser option for storing or retaining username 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 on computers, especially when they are connected to the Internet;

(i) Regularly back up 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)Do not install software or run programs of unknown origin;

(n) Delete junk or chain emails;

(o) Do not open email attachments from strangers;

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

(q) Do not use a computer or device that cannot be trusted; and

(r) Do not use public or Internet café computers to access online services or perform financial transactions.