

Protecting your information and money has always been our priority mission. This section provides you with our privacy policies and shares with you useful information about online security. It also gives you tips on protecting yourself from fraud.

SECURITY POLICY

At OCBC Securities, we are committed to protecting the security and confidentiality of your personal information so as to provide you with a safe and secure online environment. Our website uses commercially proven security hardware and software products. These security products include routers, firewalls, intrusion detection systems and secure operating system to safeguard your interest.

Industry standard Secure Socket Layer (SSL) communication protocol is the de facto cryptographic standard that we use for securing data communication between the browser and our website. Digital certificate technology is used to ensure transaction privacy, message integrity and server-side authentication. This also serves as an assurance that the website runs legitimately under the care of OCBC Securities.

All connections must pass through at least one router and one firewall to gain access to the server. The firewall checks for the appropriate source address and restricts unauthorised access to the appropriate server.

Additional technical security features include Verisign digital certificates, 128-bit encryption, one-way hashing of all user passwords and automatic logoff after a certain period (currently 4 hours).

OCBC Securities' Internet Trading is regularly reviewed and audited by external and internal auditors to ensure that your interest is safeguarded.

Apart from the security measures put in place by OCBC Securities, you play an equally important role in ensuring your online security and account information is not compromised.

You should adopt the following recommended practices in protecting the security of your system:

- Do not share your user ID or password with anyone.
- Do not display your account information in a manner that is visible to others and your PC should never be left unattended. For your protection, OCBC Securities Internet Trading will automatically terminate your session if there is no activity for a period of time.
- Always use the recommended browser. All browsers and application software should be upgraded to support SSL 128-bit encryption.
- Always check that our website address changes from <http://> to <https://> and a security icon, usually in the form of a lock or key, appears when authentication and encryption is expected.

PRIVACY POLICY

At OCBC Securities, we respect every individual's right to privacy. Our relationship with you is our most valuable asset and is the very basis of our name and reputation. Whether you are an OCBC Securities customer, a registered user or a visitor to the public area of our website, we understand the importance you place on the privacy and security of information that personally identifies you or your account information. We refer to and treat this information as "personal information." We extend the following privacy policy to you.

The OCBC Securities Privacy Policy

1. We do not sell personal information to anyone.
2. We will only share personal information with others as stated in this policy, only when we have given you advanced notice or sought for your permission. We reserve the right to disclose or report personal information in limited circumstances, where we believe in good faith that disclosure is required under law, to cooperate with regulators or law enforcement authorities, to perform credit checks, to collect or report debts owed to us, to protect our rights or property, or upon reasonable request by a unit trust in which you have chosen to invest.
3. Whenever we collect personal information from you, we will reference this policy or otherwise explain to you how we intend to use that information. We will use such information in ways that are compatible with the purpose, which we originally requested for it. For example, we will use the information to process your requests and transactions, to provide you with additional information about products and services or to evaluate your financial needs. To do so, we may share personal information with our agents or affiliates. We will limit the collection and use of personal information to what is necessary to administer our business and to deliver superior service to you. This may include advising you about our products or services, those of our affiliates, and other opportunities that we believe may be of interest to you. To serve you better, we may combine the information which you have given to us through our website or other channels.
4. We will protect the confidentiality of all personal information, which you have shared with us. In cases where we share personal information with our agents or affiliates, we will protect that personal information with a strict confidentiality as stated in our agreement. Companies hired by us to provide support services or to act as our agent must conform to our privacy standards.
5. OCBC Securities corporate policies stipulate that any employees with access to confidential customer information is not permitted to use or disclose such information except for business purposes. All employees are required to safeguard such information as specified in their confidentiality agreements with OCBC Securities. There are occasions where we may assist a company that is not affiliated with OCBC Securities, in providing a product or service to you. For example, if you are a unit trust customer, we may share personal information with the unit trust company or its agents or affiliates. In such circumstances, instructions can be found in the marketing materials on how you can request to stop receiving such communications in the future.
6. In all cases, your personal information is protected by a strict confidentiality agreement. We do not allow any non-affiliated company to retain your personal information any longer than it is necessary to provide you with the product, service or information unless you have granted us permission to do so.
7. When you register for OCBC Securities Internet Trading facility, we require you to provide us with your personal particulars. Such information enables us to deliver personalised services and communicate separately with you. We also use aggregated information collected on the use of our services to evaluate our users' preferences, improve our services and facilitate our reporting of Internet usage. Like most websites, we use small bits of data called "Cookies" which is stored

on users' computers to simulate a continuous connection. This "Cookies" enables us to "remember" information about your preferences thereby allowing you to move within our Service without reintroducing yourself. When we collect information from you, it will be held in a secure server and in the strictest confidence. For example, if you submit your email address to OCBC Securities, you will receive the latest information about our Privacy Policy, promotions, products and services. We will use your email address for no other purposes other than for sending to you the requested information.

CUSTOMER SERVICE

If you have any queries, problem, grievance or dispute relating to or arising out of the use of OCBC Securities online trading platform, you can call us at 1800 338 8688 or (65) 63388688. We are available to attend to you from 8.30a.m to 6.00p.m (Mondays to Fridays, excluding Singapore Public Holidays).

We will advise on the immediate steps to be taken by you and/or actions that we will take. Alternatively, you may send us an email to cs@ocbcsec.com and we will try to respond to you within 24 hours provided that we receive your notification during business hours and the following day is not a Saturday, Sunday or public holiday, in which case we will reply on the next business day.

DISPUTE RESOLUTION

We are committed to providing you with quality service. We will promptly attend to any claim or dispute which you may have in respect of or arising out of OCBC Securities Online Trading. Without prejudice in any way to either party's right to take immediate steps to seek urgent relief before a Singapore court or the right to seek legal redress, we will immediately investigate any claim/dispute brought to our attention and will attempt to revert to you within seven (7) working days from the date of receipt of notification. Soon thereafter, we will consult you in good faith with a view to reaching a quick and amicable resolution of the matter, satisfactory to both parties.

UNAVAILABILITY OF ONLINE TRADING PLATFORM

In the event that OCBC Securities online trading platform is unavailable, you are encouraged to perform your transactions via your Trading Representative.

SAFEGUARDING YOUR INTERNET TRADING ACCESS

At OCBC Securities, we have implemented measures to safeguard your account information. However, to ensure that your online security and account information are not compromised, we recommend that you adopt the following OCBC Securities Online Trading security guidelines:

1. Before entering your User ID and PIN, you should always ensure that the website you are visiting belongs to OCBC Securities. This can be verified by the URL displayed in your browser as well as the Bank's name in its digital certificate. This precaution will ensure that you are not revealing your OCBC Securities Online Trading Account Number and PIN to a website other than OCBC Securities.
2. To ensure that you enjoy the highest level of security possible, all browsers and application software should be upgraded to support SSL 128-bit encryption or a higher encryption standard with the most updated security features available.
3. It is important to protect yourself against any forms of online theft of your Access Code/User ID/Username and PIN/Password. Each valid Access Code/User ID/Username and PIN/Password identify you uniquely as one of our valued customers. Only authorised users are allowed to log in to our secured Internet Banking website(s).

Important tips on how you can safeguard and protect your account information.

- (a) Password has to be at least 8 characters and has to be alphanumeric. For added security, your password cannot contain repeated characters.
- (b) Password should not be based on user-id, personal telephone number, birthday or any other personal information.
- (c) Password must be kept confidential and not be divulged to anyone.
- (d) Password must be memorised and not be recorded anywhere.
- (e) Password must be changed regularly.
- (f) The same Password should not be used for different websites, applications or services, particularly when they relate to different entities.
- (g) Please do not select the browser option for storing or retaining user name and password.
- (h) Please check the authenticity of the bank's website by comparing the URL and observing the bank's name in its digital certificate or by observing the indicators provided by an extended validation certificate.
- (i) Please check that the bank's 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.
- (j) Please do not allow anyone to keep, use or tamper with your One-time Password security token.
- (k) Please do not reveal the OTP (One Time Password) generated by the security token to anyone.
- (l) Please do not divulge the serial number of your security token to anyone.
- (m) Please check your account and transactions frequently and report any discrepancy.

4. Please install anti-virus, anti-spyware and firewall software in your personal computers, particularly when you are linked via broadband connections, digital subscriber lines or cable modems.
5. Please update the anti-virus and firewall products with security patches or newer versions on a regular basis.
6. Please remove file and printer sharing in your computers, especially when you have internet access via cable modems, broadband connections or similar set-ups.
7. Make regular backup of critical data.
8. Consider the use of encryption technology to protect highly sensitive data.
9. Log off the online session and turn off the computer when not in use.
10. Do not install software or run programs of unknown origin.
11. Delete junk or chain emails.
12. Do not open email attachments from strangers.
13. Do not disclose personal, financial or credit card information to little known or suspect websites.
14. Do not use a computer or device which cannot be trusted.
15. Do not use public or internet cafe computers to access online banking or perform financial transactions.
16. You are advised not to access Online Trading using 'jailbroken' or 'rooted' mobile devices (ie the phone Operating System has been tampered with) , as it poses potential risk of malicious software infection.
17. You are advised to only download the Mobile Trading application from authorized sources such as Apple App Store and Google Play Store.
18. If you are using the mobile phone SMS token to generate the One-time password for your Online Trading access, you are advised to notify the bank in the event of lost/theft of your mobile device and if you suspect there is unauthorized access to your account.
19. If you notice any unusual/unauthorised transactions, please change your Password and notify us immediately. It is important that you inform us immediately by calling our Customer Service Hotlines at 1-800-338-8688.
20. Your usage of OCBC Securities Online Trading is subject at all times to the Terms and Conditions found on our website (www.iOCBC.com). You should therefore read carefully and adhere to the recommended security practices. OCBC Securities is not responsible for any loss or damage in connection to the use of OCBC Securities Online Trading services unless such loss is attributable to our negligence or wilful default.
21. As a user OCBC Securities Online Trading, you have the right to (1) suspend your Online Trading access immediately should you suspect any unusual activity and/or

unauthorised access, (2) terminate this service, (3) request for a new set of OCBC Online Password and (4) obtain information from the OCBC Securities regarding your online transactions.

UNDERSTANDING YOUR OBLIGATIONS AND RESPONSIBILITIES

Your use of OCBC Securities Internet Trading is governed by the ['Terms and Conditions'](#) found at our web-site. It is important that you clearly understand your obligations and responsibilities before using OCBC Securities' web-site at www.iocbc.com

As a user of OCBC Securities Internet Trading service, you are to:

- comply with the standards and procedures established by OCBC Securities from time to time;
- take all reasonable precautions; and
- observe with extreme care all security measures when accessing your online accounts or carrying out online transactions.

You will note that that under the said terms and conditions, you will remain liable for all instructions made through the use of your User ID and Password, whether or not authorised by you. OCBC Securities will not be liable for acting upon such instructions in good faith nor shall OCBC Securities be obliged to investigate the authenticity of such instructions.

You will also note that OCBC Securities shall not be liable to you in the following circumstances:

- (a) Failure on the part of the customer to adhere to the said terms and conditions
- (b) Failure to follow recommended security measures prescribed in ['Safeguarding your Internet Trading Access'](#), found in our home page
- (c) Failure on the part of OCBC Securities to act on instructions of the Customer as a result of anything beyond OCBC Securities' control. This includes, amongst other things, any machine, equipment, system or software failing to work, failure to act by any third party and any act, omission or delay of any agent or third party.

If any loss or damage results directly from OCBC Securities' security breach, gross negligence, wilful default or fraud then, OCBC Securities will be liable to the Customer, and not to any third party, for the amount of any such loss or damage. However, OCBC Securities will not be liable to the Customer for any loss of business, loss of reputation, loss of opportunity, loss of profits any type of special, consequential or indirect loss whatsoever.

SECURITY TIPS ON EMAIL AND OTHER NEW THREATS

With the Email emerging as an increasingly important communication tool, it is critical to take precautionary measures against cyber frauds.

Be wary of :

- any false e-mail address, logo or graphic designed to mislead you into accepting the validity of any email or website;
- any fake domain name which appears to be an OCBC Securities website or the website of any other financial institution
- any hyperlink to any fake website;
- any embedded form in any email; or
- or any other technique or method designed to mislead you or trick you into providing personal details, such as your Internet Trading user name or password, or any other sensitive information or downloading a virus.

Never access iOCBC Internet Trading from a link in an email.

You should personally enter the domain name of OCBC Securities (currently only www.iocbc.com) into your browser when logging onto the OCBC Securities Internet Trading website. You should not accept links or redirections from websites (other than the websites of the OCBC Bank Group) or media for the purpose of logging onto OCBC Securities Internet Trading website.

Never reveal your password to anyone. OCBC Securities will never request for your password for any reasons.

Be aware of Phishing. Phishing is the term coined by hackers who imitate legitimate companies in emails to entice people to share passwords or credit-card numbers. Before entering your user names or passwords, you should always ensure that the website you are visiting belongs to OCBC Securities. This can be verified by the URL displayed in your browser as well as the name of OCBC Securities in its digital certificate. This precaution will ensure that you are not revealing your OCBC Internet Trading user names or passwords, to a website other than OCBC Securities.

Always check that our website address changes from <http://> to <https://> and a security icon, usually in the form of a lock or key, appears when authentication and encryption is expected.

Double click on the "Padlock" or "Key" and a new window will pop-up. This Certificate will ensure the authenticity of the website.

Ensure the following on the Certificate:

- The Certificate is issued to www.iocbc.com
- The Certificate is issued by Verisign
- The Certificate has a valid date
- You are encouraged to delete junk mail, chain mail or any other unsolicited email. Do not open email attachments from strangers.

If you discover or believe that there are fraudulent e-mails, fake websites or other scams directed at you or any other customer of OCBC Securities, please notify OCBC Securities immediately at 1800 – 338 8688.

SECURITY TIPS ON SPYWARE AND ADWARE

OCBC treats online security with utmost importance and issues this security alert on Spywares and Adwares so that you will be better informed on how to protect yourself when using the Internet.

Recent news on Spywares reported that some companies are promising faster internet access if the user channels his web communication through these companies' servers and/or installs special programs onto their computer. In doing so, these companies are provided with opportunities to monitor your web behavior. Some of these companies are even able to decrypt, thus exposing your online communication including encrypted information containing- confidential details such as user ID's, passwords, account particulars -keyed in even at secured websites!

At OCBC, we are committed to provide the highest level of security to our customers. Hence, we strongly advise that you do not access iOCBC Internet Trading System through such web services or have any such dubious computer software are installed in your computer, which can be malicious.

WHAT IS SPYWARE?

Spyware is software that gathers user information while on the Internet and reports them to third parties. Adware is a form of Spyware used by marketers to track Internet user's surfing habits and interests for the purpose of customizing future advertising material. Adware can monitor information such as the type of sites visited, nature of articles read or the types of pop-ups and banners a user clicks on. This information collected is then used to customize future advertisements targeted to the user, or can be sold to a third party for the same purpose.

Spyware and Adware, not only slows down the system performance of a computer. It also uses memory and system resources that can cause system crashes and instability. Such programs may also have the ability to monitor keystrokes, scan files on your hard drive, change the default home page of your browser, and relay information about your web visits to unauthorised/disreputable third parties who can potentially manipulate the information.

Hence, Spyware and Adware programs are considered as potential forms of identity theft as they has the ability to invade your online privacy by gaining access to your passwords, PINs, credit card details and other personal transaction information.

HOW CAN YOU PROTECT YOURSELF?

There are products available that can help you detect, monitor and remove Spyware from your computer. Many complete computer security software suites now come standard with a feature for Spyware detection and removal.

With the proper precautions, you can help protect your OCBC accounts and personal information from harmful programs:

1. Be wary of banners, ads and pop-ups while surfing the Internet. Refrain from clicking on them no matter how enticing they may appear.
2. Avoid downloading programs and email attachments from unknown sources. Downloads may contain hidden programs that can compromise your computer's security. Also, never download or open email attachments from unknown senders.
3. Keep your computer operating system and Web browser current. If your computer is more than five years old, its operating system (e.g. Windows 98, OS 7 etc.) may not offer the same level of protection as newer systems. System manufacturers such as Microsoft and Apple provide frequent updates to help make your system more secure. You may check out their websites: <http://www.microsoft.com/security> or <http://www.apple.com/support/security/>
4. Install and update your computer with the latest anti-virus software. Commercially available virus protection software helps reduce the risk of contracting computer viruses that can compromise your security. These programs offer the protection against the latest threats – provided you continuously keep the program updated.
5. Install up-to-date anti Spyware program to regularly scan your computer, locate, quarantine and delete any Spyware/ Adware in your computer Review terms and conditions when you install free programs or subscribe to services from the Internet.
6. Recommended Password Management
7. Internet Trading Password must be kept confidential at all times and not be divulged to anyone
 - Change your Internet Trading Password on a regular basis
 - Password should not be based on user-id, personal telephone number, birthday or other personal information
 - Password must be memorized and not be recorded anywhere

The same password should not be used for different websites, applications or services, particularly when they relate to different entities

PROHIBITED TRADING PRACTICES

At OCBC Securities, we always have your interest at heart. While we strive to make our internet trading portal iOCBC as user friendly as possible for you, we would also want to highlight certain trading practices that are prohibited by law under the Securities and Futures Act (“SFA”).

These practices could possibly be deemed as offences under Section 197 of the SFA on false trading and market rigging transaction. The following illustrates the prohibited practices where there is a No change in beneficial ownership of securities.

Example 1: Customer A has one trading account and used the same trading account number to trade

Customer A places an order via the Internet to buy x number of shares in Company XYZ at \$0.50 in the market. Following the first order placed, he later keyed-in another order, via the Internet, to sell shares in Company XYZ at the same price in the market. The sell order was matched (completely or partially) against his own buy order in his trading account in the market. The reverse also applies where customer A’s sell order matches against his subsequent buy order.

Example 2: Customer B has multiple accounts (Cash / SBL / Margin) opened with OSPL and used a different trading account number to trade

Customer B places an order under his cash account, via the Internet, to buy x number of shares in Company XYZ at \$0.50 in the market. Following the first order placed, he keyed-in another order, under his SBL / margin account (i.e. different trading account number), via the Internet, to sell shares in Company XYZ at the same price in the market. The sell order was matched (completely or partially) against his own buy order in his cash accounts in the market. The reverse also applies where customer B’s sell order in his cash account matches against his subsequent buy order in his other accounts.

The above examples have the effect of creating a “wash sale”. A wash sale is a purchase or sale of any securities that does not involve a change in the beneficial ownership of those securities. Section 197 (1) of the SFA prohibits any person from creating or doing anything that is intended or likely to create a false or misleading appearance of active trading in any securities on a securities market, or with respect to the market for, or the price of, such securities. Wash sale could have the effect of creating such false or misleading appearances.

Under Section 197(3) read with section 197(4) of the SFA, a person engaging in wash sales in securities is deemed to have created a false or misleading appearance of active trading in securities on a securities market unless the person establishes that the purpose for which he conducted the wash sale was not, or did not include, the purpose of creating a false or misleading appearance of active trading in securities on a securities market.

Apart from the above, there are some other market conduct offences under the SFA which apply generally to a person as follows:

SFA 198: Securities market manipulation

SFA 199: False or misleading statements, etc.

SFA 200: Fraudulently inducing persons to deal in securities

SFA 201: Employment of manipulative and deceptive devices

SFA 202: Dissemination of information about illegal transactions

SFA 204: PENALTIES

You may refer to [Statutes.Online Database](#) for more information

TRADING RULES, LIMITATIONS, & RISKS OF INTERNET TRADING (FUTURES & FX)

Electronic trading systems is one of the trading avenues we offer to our valued clients. While we strive to make your trading as rewarding as possible, we would also like to take this opportunity to provide you with some information and guidance that are associated with E-trading.

One important aspect to be aware of is certain trading practices that would possibly be deemed as offences under the Securities and Futures Act ("SFA") and Futures Trading Rules. The relevant laws and rules are set out in **Appendix 1** for your reference.

You will appreciate that in order to make best use of the trading system it is necessary to have a good understanding of the various features and functionalities available. The "Price and Quantity setting" feature, for example, protects you from erroneously executing trades through the setting of parameters in the trading system. Do refer to the user guide we have sent to you to help you better understand the system. If you need assistance, feel free to call our Helpdesk.

Electronic trading relies heavily on hardware and connectivity. Having a good understanding of the characteristics, limitations and risks associated with such mode of trading will enable you to better manage certain situations that may arise. You may refer to **Appendix 2** or the section on electronic trading in our agreement.

You may wish to visit the various Exchanges' website to familiarize yourself with the contracts specifications which offer crucial information pertaining to a contract, such as contract size, tick value and last trading day.

Appendix 1**Securities and Futures Act (“SFA”) and Futures Trading Rules****SFA s206 : False trading**

No person shall create, or do anything that is intended or likely to create, a false or misleading appearance of active trading in any futures contract on a futures market or in connection with leveraged foreign exchange trading, or a false or misleading appearance with respect to the market for, or the price of futures contracts on a futures market or foreign exchange in connection with leveraged foreign exchange trading.

SFA s208 : Manipulation of price of futures contract and cornering

No person shall, directly or indirectly —

- (a) manipulate or attempt to manipulate the price of a futures contract that may be dealt in on a futures market, or of any commodity which is the subject of such futures contract; or
- (b) corner, or attempt to corner, any commodity which is the subject of a futures contract.

SFA s209 : Fraudulently inducing persons to trade in futures contracts

(1) No person shall —

(a) by making or publishing any statement, promise or forecast that he knows or ought reasonably to have known to be false, misleading or deceptive;

(b) by any dishonest concealment of material facts;

(c) by the reckless making or publishing of any statement, promise or forecast that is false, misleading or deceptive; or

(d) by recording or storing in, or by means of, any mechanical, electronic or other device information that he knows to be false or misleading in a material particular, induce or attempt to induce another person to trade in a futures contract or engage in leveraged foreign exchange trading.

(2) In any proceedings against a person for a contravention of subsection (1) constituted by recording or storing information as mentioned in subsection (1) (d), it is a defence if it is established that, at the time when the defendant so recorded or stored the information, he had no reasonable grounds for expecting that the information would be available to any other person.

SFA s210 : Employment of fraudulent or deceptive devices, etc. No person shall, directly or indirectly, in connection with any transaction involving trading in a futures contract or leveraged foreign exchange trading —

(a) employ any device, scheme or artifice to defraud;

(b) engage in any act, practice or course of business which operates as a fraud or deception, or is likely to operate as a fraud or deception, upon any person;

(c) make any false statement of a material fact; or

(d) omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading.

SFA s211: Dissemination of information about illegal transactions No person shall circulate, disseminate, or authorise, or be concerned in the circulation or dissemination of, any statement or information to the effect that the price of a class of futures contracts or foreign exchange in connection with leveraged foreign exchange trading will, or is likely to, rise or fall or be maintained because of the market operations of one or more persons which, to his knowledge, are conducted in contravention of section 206, 207, 208, 209 or 210 if —

(a) the person, or a person associated with the person, has conducted such market operations; or

(b) the person, or a person associated with the person, has received, or expects to receive, directly or indirectly, any consideration or benefit for circulating or disseminating, or authorising or being concerned in the circulation or dissemination, the statement or information.

SGX-DT Rule 3.4.1: Market Manipulation A Member, Approved Trader or Registered Representative shall not manipulate or attempt to manipulate the price of a contract or of any underlying, or corner, or attempt to corner, any underlying.

SGX-DT Rule 3.4.2: Churning A Member, Approved Trader or Registered Representative is prohibited from churning or generating commissions through creating excessive transactions in a Customer's Account.

SGX-DT Rule: 3.4.3 False Trading, Bucketing, Fraudulent Inducement to Trade and Employment of Fraudulent Device

A Member, Approved Trader or Registered Representative shall not:

(a) engage in, or knowingly act with any other Person in, any act or practice that will or is likely to create a false or misleading appearance of active trading in any contract or a false or misleading appearance with respect to the price of any contract;

(b) knowingly execute, or hold out as having executed, an order for the purchase or sale of a contract, without having effected a bona fide purchase or sale of the contract in accordance with this Rules;

(c) induce or attempt to induce another person to trade in a contract:

(i) by making or publishing any statement, promise or forecast that it knows or ought reasonably to know to be false, misleading or deceptive;

(ii) by any dishonest concealment of material facts;

(iii) by the reckless making or publishing of any statement, promise or forecast that is false, misleading or deceptive; or

(iv) by recording or storing in any mechanical, electronic or other device information that is knowingly false or materially misleading;

or

(d) directly or indirectly in connection with any trading in a contract:

(i) employ any device, scheme or artifice to defraud;

(ii) engage in any act, practice or course of business which operates as a fraud or deception, or is likely to operate as a fraud or deception upon any Person;

(iii) make any false statement of a material fact; or

(iv) omit to state a material fact necessary in order to make any statements made, in the light of the circumstances under which they were made, not misleading.

In the course of your trading, do be mindful of the said prohibited trading practices as any person who contravenes any of the above provisions shall be guilty of an offence and shall be liable to a fine not exceeding \$250,000 or to imprisonment not exceeding 7 years, or to both.

[Appendix 2](#)

Potential limitations and risks of on-line trading, which includes but not limited to the following:

(a) possibility of delays in order transmission and confirmation of order execution, and what to do in case of such delays;

(b) not being able to withdraw erroneous orders in time due to the speed of electronic trading; and

(c) danger of unauthorised access to a Customer's on-line account and non-compliance of recommended preventive security measures in relation to matters such as the protection of passwords and leaving an on-line screen unattended.

(d) exposed to risks associated with systems including the failure of hardware and software, resulting in orders either not executed according to instructions or not executed at all