Online Security

We use industry standard security technology and practices to ensure your account and online transaction are safe and secure. We do this in the following ways:

■ Online User ID and Log-in Password

Online access to your account is only possible once you have authenticated yourself by using the correct user ID and log-in password. Pleases remember and do not share them with anyone. We suggest following the guidelines below.

1. Change your log-in password immediately once you received your password letter.

2. Do not use a log-in password that is easy to remember or guess, e.g. birthday or phone number.

3. Change your log-in password periodically so as to protect your online security.

4. Safeguard your user ID and log-in password. Do not disclose User ID and log-in password to others nor record them anywhere visible to avoid theft.

5. To protect your accounts, your access will be locked after 5 unsuccessful attempts. You may have it unlocked by contacting Customer Service.

■ 128-bit Secure Sockets Layer (SSL) Technology

Secure Sockets Layer (SSL) technology is used within your Internet banking session to encrypt your personal information so that no one else can read it. We use SSL encryption, which is accepted as the industry standard.

■ Additional Security Mechanism for Transactions

To add an extra level of security, a digital signature (through an I-Key containing digital certificate) and one-time password (OTP) generated by Token if checker is requested are used when performing online transactions. Please plug-in I-Key every time while making a transaction. Your transaction will be initialed successfully only after inputting correct I-Key password. If checker is needed, checker needs to approve the transaction by inputting the correct OTP generated by Token. Please follow the *"Online User ID and Password"* guidelines for I-Key password and Token password. Please pull out I-Key from your computer and keep it in the secure place after the online transaction is done. Safeguard your I-Key and Token. If I-Key or Token is lost or stolen, please promptly contact our Customer Service.

*****Please remember your I-Key password and Token Password and if you input wrong I-Key password or Token Password for 4 consecutive times, your I-Key or Token will be locked and you need to contact our Customer Service for further help.***

■ Timeouts

Internet banking online session will automatically log you off or timeout if your computer remains inactive for a period of time. You need to login again to resume your session. Please remember to log out every time and close your browser when you finished using online banking.

■ The Online Security Tips

We understand your concerns about online security. Enjoy the benefits of Internet banking service by following the guidelines below:

1. *During the Internet banking logon process, the bank's will **NOT** ask customers to enter any numbers displayed on the web to the security device to obtain security code*
2. *Customers should continue to take precautionary measures to keep their computer safe to guard against Trojan Horse attack, including:*
3. *Install personal firewall and anti-virus software in their personal computers and keep them up-to-date*
4. *Be very cautious about opening attachments in e-mails from unfamiliar sources, and avoid visiting or downloading software from suspicious websites*
5. *Never access the Internet banking accounts through hyperlinks embedded in emails, Internet search engines, suspicious pop-up windows or any other doubtful channels. Customers should connect to a bank website through typing the authentic website address in the address bar of the browser or by bookmarking the genuine website and using that for subsequent access. If customers find the website of the bank suspicious, they should not enter any information (including user ID, password and OTP) to the website and should report to the bank immediately.*
6. *If any unusual screens pop up and/or the computer responds unusually slow, customers are advised to log out from the Internet banking and scan the computer with the most updated version of virus protection software*
7. *Don't disclose any personal information including logon password or OTP to any person through any means such as e-mail, over the phone or in person*
8. *Review the transaction records regularly and report to the bank immediately if identify any suspicious transactions in the bank accounts*
9. *Follow the Internet banking logon instructions and security tips published by the banks when conducting Internet banking transactions*

☎Customer Service

Taiwan: 0800-017-888 **/ Hong Kong:** (852)2916-1816 **/ China:** (86) 21-2080-5888
New York: (212) 457-8903 **/ Vietnam:** (84) 28-3910-1888 ext.6301~6304
New Delhi: (91) 11-43688888 **/ Japan:**(81) 3-3288-9888 **/ Singapore:**(65) 6351-4888