

First Commercial Bank

Internet Banking Disclosure

Important! Please read the following message before using Internet Banking System.

While Internet Banking can bring you more convenience in terms of faster and easier access to your bank account(s), there are inherent risks that you need to be aware of. Due to the open nature of the Internet, web-based systems such as Internet Banking are inherently subject to risks such as those related to virus attacks, hacking, unauthorized access and fraudulent transactions.



While FCB has put in place the necessary security practices and measures to safeguard against these risks, in order to ensure the safety of Internet Banking transactions, you, as the end-user, also need to take necessary procedures to safeguard your account information.

To ensure your online banking sessions are secure, FCB recommends that you follow these simple security tips.

✓ Make sure the login address and certification.

1. Do using our service from following linkage:

- The First Bank portal site: <http://www.firstbank.com.tw>
- The e-banking main page: <https://ebank.firstbank.com.tw>

2. All data transmit between your computer and the FCB internet banking system was secure by SSL(Secure Sockets Layer)-128 bit encryption. As a result, when you visit our e-banking site, there will be a yellow lock (like  or ) shows by browser. Please click it and check the certification information:

- Issue to: ebank.firstbank.com.tw
- Issuer: TWCA Secure CA
- Please verify the period of validity.

✓ Protecting Your Account

1. Check your account and transaction history details regularly.
2. Under no circumstances will FCB ever send you an email asking for your personal information.
You should NOT respond to such email or reveal your Password to anyone.
3. If there is any other people/group inform you that your personal information disclose and need to check it with you, please call FCB in advance to confirm it.
4. Do not use shared/public PCs for Internet Banking.
5. Please logoff the Internet Banking System after you have completed the use of the service to avoid your account being misused.

✓ Protecting Your Password

1. Please choose your Password as follow:
 - Make your Password has a certain level of complexity. The length must longer than eight digits, and mixed with char and number.

- Do not choose a Password that is easily guessed, like your telephone number, NRIC number, date of birth, User ID, or other associated data.
 - Never use the same Password for other financial or non-financial services.
 - Avoid using sequential numbers or the same number more than twice.
2. Avoid storing Customer ID, User ID and Password.
 3. Do not reveal your Password to anyone or share your Password with others.
 4. Memorize your Password. Do not write down your Password or store it in computer hard-disk, diskette, mobile phone or other insecure means.
 5. Do not use your Password when someone else can see you keying it in.
 6. Change your Password regularly by using the "Change Password" service.
 7. Change your Password immediately if you suspect it has been exposed to others or the moment you suspect any unauthorized access.

✓ **Protecting Your Computer**

1. Protect your PC from viruses and malicious programs.
2. Install the antivirus software and updated it with the latest virus definition.
3. Do not open email attachments from strangers or install software or run programs of an unknown origin.

✓ **Relative Link**

The user rights and interests, and the information about internet bank crime and terrorism could be found as follow link:

United States:

1. The Better Business Bureau's website on Data Security Made Simpler:
<http://www.bbb.org/data-security;>
2. The Small Business Administration's (SBA) website on Protecting and Securing Customer Information:
<http://community.sba.gov/community/blogs/community-blogs/business-law-advisor/how-small-businesses-can-protect-and-secure-customer-information;>
3. The Federal Trade Commission's (FTC) interactive business guide for protecting data:
<http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html;>
4. The National Institute of Standards and Technology's (NIST) Fundamentals of Information Security for Small Businesses:
<http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf;>
5. The jointly issued "Fraud Advisory for Businesses: Corporate Account Takeover" from the U.S. Secret Service, FBI, IC3, and FS-ISAC available on the IC3 website (<http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf>) or the FS-ISAC website (<http://www.fsisac.com/files/public/db/p265.pdf>); and
6. NACHA – The Electronic Payments Association's website has numerous articles regarding Corporate Account Takeover for both financial institutions and customers:
[http://www.nacha.org/c/Corporate_Account_Takeover_Resource_Center.cfm.](http://www.nacha.org/c/Corporate_Account_Takeover_Resource_Center.cfm)

Taiwan:

1. Financial Supervisory Commission, Executive Yuan (<http://www.banking.gov.tw/>)
2. The Bankers Association of The Republic of China(<http://www.ba.org.tw/>)

✓ **The Internet Service Hour:**

The clients who apply for internet bank could use the Inquiry function. If you need to using the transfer function, please fill out the “New York E-Banking Services Application”, providing the Authorization account, and deliver to FCB New York branch. The service time is as follow:

1. e-Banking Inquiry

- ✓ 24 hours (Service will not available during the system maintenance period)

2.Account Transfer Service

- ✓ During the business day 00:00 am— 07:30 pm. (transfer initiated after 3 pm EST must be set as a reserved transaction effective within the business day in 10 calendar days)

3.Scheduled Funds Transfer Service

- ✓ 24 hours (Service will not available during the system maintenance period)

✓ **Contact Us**

If you have any question, please contact us in the business hours.The contact information is as below.

Telephone : 1-212-599-6868

Fax : 1-212-599-6133

Email : fcby@firstbankny.com

Address : 750 3rd Avenue, 34 Fl., New York, NY 10017