Online Banking Safety, Awareness and Protection

Occurrences of account takeover, fraud, and identity theft have increased significantly over recent years. Cybercriminals are using sophisticated methods (malware, spyware, phishing, keylogging, man-in-the-browser) to obtain access to accounts and create fraudulent transactions out of these accounts. Phishing and malware attacks have more than doubled in the last 12 months resulting in potential losses exceeding $1 billion and they are occurring locally. As a user of online banking services such as wire transfers and ACH origination (which allow funds to be transferred out of accounts to third parties) we want you to be aware of these possibilities and offer you the greatest protection of your assets and identity. While we constantly strive to ensure the security and confidentiality of your information on our networks and services offered, we cannot ensure the protection on your computers in accessing this information, which is where many of these attacks originate.

At **FCB**, we offer you several features and controls that can help you manage your accounts, protect your funds, maintain confidentiality of your information/identity and mitigate the risks of fraud. We encourage you to utilize them:

General and Sign-on Controls:

- **We will never email**, call or otherwise ask you for your user name, password, or other online banking credentials on an unsolicited basis. You should never provide this information to others as these "phishing" attempts are frequently used to try to gain fraudulent access. Online account sites you deal with should already know this information.
- **We may send you periodic messages within** your online banking session to notify you of service upgrades or availability, security awareness material, or the availability of other FCB services or products.
- **Do not include complete account or card numbers**, balances, social security numbers, passwords, or PIN's in an e-mail to FCB unless responding to an encrypted e-mail originated by FCB.
- **Do NOT open suspicious e-mail attachments.** Historically e-mail attachments are one of the most popular ways to spread malware. If you don't know what it is, delete it immediately rather than open it. Also, do not download files or install software from unknown sources, which increases the risk of malicious attacks.
- Always "**register" your computer as Private** when accessing online banking and **DO NOT use public or unsecured sites** (i.e. the library or an Internet café) when accessing online banking sites. Registering your computer as private will also not require challenge questions on every login.
- **Create a difficult password**, of at least eight (8) characters composed of a combination of upper/lowercase letters, numbers, and special characters and do not include the username to avoid easily guessed passwords. You are encouraged to periodically change your password (i.e. every 90 days).
- **Safeguard your username and password** and do not: post next to your computer; make it easily accessible to anyone; or be negligent in providing to someone. Avoid using an automatic login feature that saves usernames and passwords for the site.
- **Always verify your login image and passphrase** to ensure they match what you have selected. If they do not match, do not continue the login as fraudsters may be attempting to capture your login information and reroute you to another fictitious site.
- **Upon login, check the date and time of your last login** to verify it was in fact you logging in and not a possible hacker. Also, verify the last failed login date/time to determine if someone may be trying to hack into the account. If you find that the last login was not authentic, please call FCB immediately. Example follows:

  Welcome FCB TEST, the last time you signed on was 4/11/2012 at 1:24 PM Eastern Standard Time. Your last failed sign on was 4/10/2012 at 3:59 PM Eastern Standard

- **Be sure to Sign-off session when completed**. Do not just close the page, "X" out, or go to another site leaving session open.
- **Monitor and review your account activity frequently** to ensure no fraudulent activity has occurred and if so, report it immediately to FCB. Also, ensure that monthly statements are promptly reviewed and reconciled, as losses could accumulate quickly if fraudulent transactions go undetected.
- **Consider separation of duties** when processing higher risk transactions such as wires or ACH. These controls would allow one employee to originate the request and then another to approve or release the transaction. No one employee could process the entire transaction helping to reduce the risk of fraudulent activity both internally and externally.
- **Contact the Bank immediately to remove any terminated employees** or others that no longer need online banking access to reduce risk exposure.

Business/Personal Computer Controls:

- **Use a software firewall.** If you are using Windows XP or Vista, enable the Windows Firewall. If you have a Mac and are running OS X 10.2 or above, enable the built-in firewall.
- **Protect your computer with well-known anti-virus/spyware software.** Update the virus definitions and scan your computer regularly. Most anti-virus software will provide tools to automate and schedule these tasks so that they take place when you are not using your computer.
- **Avoid fake anti-malware**. Some anti-malware vendors that promise to rid your computer of malware, actually install malware instead, often holding your computer hostage until you pay them. Don't buy anti-malware software advertized in pop-up ads. Reputable software is not sold this way.
- K**eep Your Operating System Up-To-Date.** Many viruses rely on systems without current patches or security to spread. Configure your computer to update the operating system automatically if possible with current service packs, etc. Be sure that your antivirus and antispyware software is configured to update automatically as well.
- **Step-up authentication** of Out-of-Band authentication and/or Out-of-Wallet questions may be required for device ID's that are not recognized, utilizing one-time security codes to help deter hackers and account takeovers.
- Consideration of using a **stand-alone, dedicated computer** for only financial transactions with no web browsing, e-mail, or social media allowed.
- Perform your own **internal fraud risk assessments** and evaluate your online controls periodically to minimize risk.

Alerts:

- **Utilize built-in e-mail/text alert features** to monitor account access and activity as these are very effective tools in mitigating fraud risks.
- **Pay close attention to alerts/messages** for possible fraudulent access and do not ignore. If you know you did not access your account or conduct a transaction, notify FCB immediately at 301-620-1400.
- **Alerts can be setup to show**:

* Access by the user for every login	* Password change	* Email address change
* Failed sign-on attempts	* Username change	* Account Balance < $xxx
* Account Balance > $xxx	* Account Transfer Completed	* Account Transfer Failed
* Debit/Credit Transactions	* Daily/Weekly Transfer Summary	* Wire Transfer Completed
* Wire Transfer Failed	* Wire Transfer Changed	* ACH Batch Changed/Added
* ACH Batch Failed	* New Bill Payment Payee	* Summary of Bill Pymts. Made

Transaction Limits:

- **Can be placed on Wire Transfers** at multiple levels – per transaction, daily, weekly, or monthly
- **Can be placed on ACH Batches** at multiple levels – per transaction, daily, weekly, or monthly
- **Can be placed on Funds Transfers** at multiple levels – per transaction, daily, weekly, or monthly

Online Banking Activity Review:

- In addition to reviewing transaction activity on your accounts on a regular basis, also **review your Transfer Activity, ACH Activity, and Wire Transfer Activity history** to verify that the most recent transfer activity is legitimate and authentic.
- **Sign-up for eStatements** to eliminate the mailing of your account numbers, checks and activity that could be susceptible to theft and fraud; and receive your statement much quicker for review, while saving paper.

FCB Marble Security:

- Provides online banking users with a **secured and private** "tunnel" browser connection running inside a virtual machine protecting the user from malware and host applications. Provides an **encrypted keyboard and a read-only** mode that stops malware, keyloggers, man-in-the-middle attacks, and site altering to offer you the ultimate protection and peace of mind when performing online banking, sensitive financial/personal transactions, or just web browsing.

Please see your Business Online Banking Agreement, Online Banking Agreement, Bill Pay Agreement, and "Important Information about Deposit Accounts" booklet for a description of your responsibilities and the extent of the Bank's liability regarding unauthorized transactions using Online Banking services.

At **FCB**, we are committed to protecting your information, however it is critical that **you** also be aware of the risks present, implement various controls to minimize the risks, and actively monitor your accounts for any potential fraud. If you ever feel your online profile, accounts, or identity have been compromised or you receive an unsolicited request for any information, please **contact us immediately at 301-620-1400**.

We appreciate your business and want to work closely with you to protect what is yours!!