Security Best Practices on CitiDirect BE^{SM}

At Citi, security for our clients is our utmost concern. As hackers and others, such as organized criminals, continue to try to get unauthorized access to funds, we would like to highlight some best practices to help make sure you are secure.

Social engineering attack

Citi has received business intelligence reports advising that there have been a few incidents of organized criminals calling bank clients and falsely advising them that they are the bank's representatives.

Typically, when this happens, the client receives an unsolicited call from "Bank Technical Support." The client is then asked for technical information about how the system works, how transactions are input and who authorizes them. The criminals often ask if the user can take them through the transaction by sharing their screens. They could even ask users to share passwords, token / authentication device information or other credentials.

Please note that Citi will never call you on an unsolicited basis and ask you for PINs, passwords or any other such security information.

The goal of these criminals is to understand the banking system and then try to create a fraudulent transaction.

If you receive any suspicious calls (such as unsolicited or unexpected contact asking for information), please contact your Security Manager and Citi Client Service person immediately.

CitiDirect BE^{SM} Best Practices

In order to maintain the best level of security, please ensure that you regularly review your controls.

- CitiDirect BE^{SM} supports up to nine levels of approval. It is strongly recommended that your organization set one or more levels of approval
- Ensure that high risk or high value transactions go through more stringent approval flows
- Leverage the CitiDirect BE^{SM} pre-format functionality to ensure you are only paying known or pre-approved beneficiaries
- For payments to be made by your organization, please ensure that your organization implements a robust process to prevent fraudulent attempts to change the beneficiary bank account details. Such attempts, if successful, would result in your money ending up in the wrong hands.

For assistance with implementing the above best practices please utilize the *client academy* training or contact your client service representative

Never share your SafeWord Card

SafeWord Cards should never be shared. Sharing a Safeword card increases the risk of fraud. Because you have agreed to keep your SafeWord card secret, any transaction that utilizes that card will be attributable to you. CitiDirect's key security mechanism is to distinguish between the person inputting a transaction and the authorizer of the transaction. If SafeWord cards are shared, it becomes easier for one person to both input and authorize a transaction.

You can use CitiDirect BE^{SM} mobile to approve payments and monitor your intraday balances when roaming. Alerts also can be set on large value transactions or when balance limits are reached.

Keep your PIN secret

Similarly, it is very important to keep your PIN secret. Your PIN is your first line of defense against someone using your SafeWord card to input or authorize a transaction in your name. Treat your PIN the same as you would your own Banking card PIN and do not store the PIN in a visible location such as the sleeve of the card. Do note that the PIN on your Safeword card can be changed and Citi recommends that users change PINs periodically. Please review the below instructions:

Change your SafeWord PIN as follows (you can cancel the following procedure at any time by pressing Clr):

1. Press ON to turn your SafeWord card on.
2. At the Enter Pin prompt, type your existing PIN.
3. The host? prompt is displayed. Since you are not entering a Challenge, ignore this prompt and continue with the next step.
4. Press Pin to indicate that you want to change your PIN.

   Note: Please ensure that you remember the new PIN that you enter in Step 5 below as this PIN will be known only to you. If you forget your new PIN, Citibank cannot reset it. You must contact Citibank to have a new SafeWord card issued to you.
5. At the new Pin prompt, type your new PIN on the keypad. You can change the digits in your PIN but not the length. It must be four digits long. After you type the last digit, your new PIN is stored in the SafeWord card.

   Note: The display area on your card may contain the following alpha-numerics:
   - 0 is zero not O as in Oscar
   - 8 is eight not B as in Bravo
   - 5 is five not S as in Sierra
   - A is A as in Alpha not R as in Romeo
   - l is one not I as in India
6. At the AGAIN prompt, retype your new PIN.
7. At the SUCCESS prompt, you may turn OFF your SafeWord card. You have successfully changed your PIN.

IMPORTANT: Citi will not on an unsolicited basis request users to provide their electronic banking credentials such as PINs, passwords or any other such security information.

Delete former employees

Ensure that when employees leave or transfer to other roles they are deleted from the system and that their Safeword card is deleted. It is important that cards are not reassigned to new users. Also note that users can be scheduled automatically to expire on a future date to ensure cards are not used inappropriately.

Entitlement reviews

Perform regular user and entitlement reviews on the system to ensure access is appropriate and current.

Ensure the CitiDirect User has received both the Safeword Card and PIN prior to enabling* on the system.

Users that are “out of office” for extended periods should be disabled* until returning to the office (e.g. vacations, extended leave, etc.)

**How is this done? Under the user’s profile check the box titled “enable” to enable user; uncheck the enable box to disable the user — make sure you save your changes (also refer to the Security Manager Guide for more information).*

Other tips

Intraday reporting can be used to monitor transaction initiation during your business day, AFRD (Automated File and Reports Delivery) can be used to automate the generation and delivery of these reports.

PC Best Practices

- **Beware of Malware —** Malware can be downloaded under various circumstances, such as when visiting a malicious or vulnerable website, viewing an email message or by clicking on a deceptive pop-up window. Malware is malicious software installed on your computer which has a harmful intent that can, among other things, capture your login passwords and other personal data. Examples of malware include software such as spyware, adware and viruses. One way to help protect you from Malware is to exercise caution before installing programs on your computer or opening email attachments. Here are some precautions that are important to take:
  - Only install applications and software from well-known companies you trust
  - Make sure your computer is cleansed from viruses/spyware and has up-to-date anti-virus and anti-spyware software installed
  - Keep your operating system and browser up-to-date with the latest security updates and patches
- **Install anti-virus, anti-spyware and malware detection software —** one way to defend against computer attacks is to utilize preventative software. You will need to update the software regularly to guard against new risks so set the software to update automatically.
- **Use a pop-up blocker —** set your browser preferences to block pop–ups—aside from being annoying, these pop-ups can contain inappropriate content or have malicious intentions
- **Log Out -** Make sure users log out and exit browser or close browser window when finished using CitiDirect

- **Update -** Keep browser and Java plug-in updated to the latest version
- **Protect -** Ensure devices (PCs, Desktops, Laptops, etc.) used to access CitiDirect are password protected

Additionally, you may need to engage your IT department to assist with the PC best practices and perform related risk assessment along with controls evaluation periodically.

Please contact your Citi Representative immediately if you notice suspicious account activity or experience information security-related events.