Treasury and Trade Solutions

# Security Best Practices on CitiDirect BE℠

At Citi, client security is very important. As individuals with malicious intent continue to try to gain unauthorized access to information, we would like to highlight some best practices recommended for your use, to help make sure you are secure.

In order to maintain the best level of security, it is imperative that you regularly review your controls:

- CitiDirect BE℠ 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 transactions or high-value transactions go through more stringent approval processes
- Leverage the CitiDirect BE pre-format functionality to ensure you are only paying known or pre-approved beneficiaries
- Monitor high-risk account activity such as attempts to change the beneficiary bank account details. Such fraudulent attempts, if successful, can result in a loss of your funds.

For assistance with implementing the above best practices, please utilize the Client Academy training module or contact your Citi Client Service representative.

## Beware of Social Engineering Attacks

Social engineering involves criminals gaining unauthorized access to your information and/or accounts through manipulation or deception. The goal of social engineering is to allow an unauthorized user to commit fraud, industrial espionage or identity theft, or simply to break into a network in order to disrupt systems and applications.

Rather than hacking into systems, social engineers attempt to obtain information by deception. They prey on qualities of human nature, such as the desire to be helpful, the tendency to trust people, and the fear of getting into trouble. Social engineers utilize a number of very different methods, so it is important that you, are aware of them.

Citi has received business intelligence reports advising that there have been a few incidents where social engineers pose as bank employees, customer service representatives or payments systems representatives. **Please note that Citi will never call you on an unsolicited basis and ask you for your electronic banking credentials including personal identification numbers (PINs), passwords or any other such security information.** If you receive any suspicious calls (unsolicited or unexpected in nature where the caller is requesting information), please contact your Security Manager and Citi Client Service person immediately.

### Leverage CitiDirect BE℠ Mobile

You can use CitiDirect BE℠ 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.

### 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 for your use only, any transaction that utilizes that card will be attributable to you. The CitiDirect BE 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.

### Keep your PIN Confidential

Similarly, it is very important to keep your PIN confidential. 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.

### 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 similarly deleted. It is important that cards are not reassigned to new users. Also note that users can be scheduled to automatically expire on a future date to ensure cards are not used inappropriately.

### Review Entitlements

Perform regular user and entitlement reviews on the system to ensure access is current and in line with job description, and segregation of duties is in place. It is strongly recommended that user ID management, transaction initiation, authorization and control activities should not be performed by the same person. 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 (e.g. vacations, extended leave, etc.) should be disabled until they return to the office.

### Other Tips

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

### Personal Computer Best Practices

- Only install applications and software from well-known companies you trust
- 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 intent.
- Log Out – make sure you log out and exit your browser or close the browser window when finished using CitiDirect BE.
- Update – keep browser and Java plug-in updated to the latest version.
- Password protect – Ensure devices (personal computers (PCs), desktops, laptops, etc.) used to access CitiDirect BE 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, experience information security-related events, or have any questions regarding security at Citi.




1150901 GTS26303 11/13