Remote Deposit Capture Services

Security Best Practices

- Keep the original items for 30 days and store them under lock and key, after 30 days destroy the original items. Ensure that only authorized personnel have access to the stored original items.
- Stamp or mark the front of each item as “Scanned” or “Processed” to indicate the check has been scanned and deposited.
- Do not store customers’ account information, photocopies, or private information in your general files which are accessible to non-authorized personnel. Perform a routine audit for potential security breaches to customers’ information.
- Set up dual control for user permissions. We recommend that you require a second user to verify and approve transactions prior to them being sent to the bank.
- Install a security software suite that includes anti-virus, anti-spyware, malware and adware detection, from a reputable vendor. Keep the software up-to-date through an automatic update feature and configure it to perform recurring, automated complete system scans on a routine basis.
- Install a firewall on your computer to block unauthorized access; this is particularly important if you use a broadband connection, such as DSL or a cable modem.
- Avoid phishing attacks that attempt to fraudulently acquire passwords and user IDs by masquerading as a trustworthy person or business in an electronic communication. Never click on a URL within an email, enter the URL yourself or from your saved favorites.
- Protect user IDs & passwords by establishing a unique user ID and a strong password using a combination of numbers and upper and lower case letters.
- Never leave your PC unattended while you are logged into the site. Set the computer to automatically lock after a set period of inactivity.
- Clean the scanner equipment regularly with the proper cleaning products.

For more information,
please visit our website at **www.FirstAmBank.com**
or call us at **847-427-5000**.