MOBILE BANKING SAFETY TIPS

NO MATTER WHAT KIND OF MOBILE BANKING METHOD YOU USE, REDUCE FRAUD AND PROTECT YOUR MONEY BY FOLLOWING A FEW PRECAUTIONS

- Do not give out your mobile account information, password, or user ID.
- Do not leave your mobile device unattended while you are logged into your banking account.
- Do not send privileged account information (account number, password, etc.) in any public or general e-mail system.
- Notify us immediately if you receive an alert about activity that you did not initiate. It is possible that access to your account has been compromised and an immediate response may be necessary.
- If you are unable to access our site, please notify us immediately. This may be an indication that either your account or the Bank's site is subject to criminal activity.
- Lock your phone with a PIN to prevent unsophisticated takeover of your bank account.
- Do not download software from unofficial or unfamiliar sources which can result in downloading viruses of malware.
- Do not allow a vendor to "jail break" your phone (it can eliminate or diminish inherent phone security features).
- Update security applications as soon as the updates are available to reduce your phone's security vulnerabilities.
- Eliminate or uninstall applications that you do not use.
- Load anti-virus software from a legitimate vendor.
- Be careful who you allow to use your phone.
- Be careful in disposal of your phone to ensure that information about you, your contacts or your banking security access is not on the phone.
- Be aware of what your phone can access and what would be at risk if your phone was lost or stolen. If you suspect your mobile device has been lost or stolen, notify us immediately by calling **407-745-4545 or 321-784-8333** so we can disable your mobile banking application.