Recommended best practices to keep your mobile devices secure:

- Use the lock function on the device with a password or Personal Identification Number (PIN). While most mobile devices now contain password / PIN lock options, they are not always on by default. Also, if your device has an auto-lock timer (to place it into locked mode after a period of time) use it. Activating this security measure can help you avoid problems, in case of loss or theft of your mobile device. Frequently, change the lock password or PIN.

- Using and protecting your user name(s) and password(s) and deactivating a compromised mobile phone number or device, in order to protect the confidentiality of this information.

- Update the mobile banking app, from time to time, with the most recent mobile banking app. As we update security features and add new features, you'll want to be sure you have the most current version.

- Limit loss by always keeping your device physically secured or in a secure location. If your device is lost or stolen, please review your account activity and contact us immediately regarding any suspicious transactions.

- Take appropriate precautions when using public Wireless Local Areas Networks for use of the Services.

- Exercise due diligence with unexpected messages or notifications. Do not click on suspicious links sent via unsolicited text message, email, or suspicious push notification.