Mobile Best Practices Guidelines

- Bank of Brodhead will **never** call, email, or text you requesting your personal information. If you are contacted, please **do not provide any personal information**, and contact us immediately at 608-897-2121.
- It is **highly** recommended that for security purposes, customers do not jailbreak or root their smartphones. Jailbreaking or rooting can potentially make your device vulnerable to malicious software and applications. This is largely due to the increased access to "unapproved" applications, which could be subject to or contain malicious software.
- It is **highly** recommended that you enable a passcode or similar lock screen mechanism on your device. This will help deter unauthorized access to your mobile device.
- It is **highly** recommended that you close out of the application once you have completed your session.
- Please only download applications from reputable sources.
- If your device is lost or stolen, contact us as soon as you are sure that the device has been compromised. Locator/Remote wipe applications and services are available for both Android and iPhone models. Links to each service are provided on the bank's website. While we can remotely wipe the data from your mobile banking application, it is **highly** recommended that you employ a locator/remote wipe solution for your phone.
- It is also recommended that Bluetooth be disabled for the duration of your mobile banking session. While this issue has generally been addressed by device developers, there is still a possibility of what is called Bluesnarfing, or information theft through the use of Bluetooth connectivity.