Mobile Best Practice Guidelines

- Generations Bank will **never** call, email, or text you requesting your personal information. If you are contacted, please **do not provide any personal information**, and contact your local branch immediately.
- It is **highly** recommended that for security purposes, customer do not jailbreak their smartphones. Jailbreaking or "self-hacking" 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 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 credible sources.
- If your device is lost or stolen, contact us **as soon as you're sure** that the device has been compromised. Remote wipe instructions are also available for both Android and iOS through the bank's website.
- 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.