Best Practices for Mobile Banking Security

User education is a universal security principle and industry best practice.

Security is a relationship among many parties to help protect your mobile device when accessing mobile banking and treasury applications. Many of these recommendations parallel the best practices you should employ when accessing the internet from a personal computer. The current fraud landscape is innovative, requiring ongoing diligence. Fraudsters continue to deploy and find methods to compromise information in a fast-paced and ever-changing online environment. Heightened risks of internet and mobile fraud requires users to be diligent in protecting mobile devices.

**Passwords**

- Keep your password information safe and use strong passwords for all applications on the mobile device.
- Strong passwords consist of 8 or more digits, with a combination of numbers and letters.

**Manage system settings, downloads and device software**

- Only download applications from reputable sites/stores after reviewing feedback from other users and closely review application permission requests.
- Install mobile security software and regularly update security patches to help detect viruses.
- Keep the operating system and software up-to-date by installing updates when available.
- Don't access banking or shopping applications using private credentials while connected through public Wi-Fi connections.
- Don't leave your Wi-Fi in ad hoc mode.
- Disable discoverable mode after enabling Bluetooth® devices, if your Smartphone does not automatically default to off after adding a device.
- Setup a personal firewall to protect your device from unauthorized electronic access. The firewall can be set on different levels, allowing varying degrees of limited access.
- Validate that your credentials don’t appear in the URL when interacting with a web site.

**Physical device security**

- Don’t leave your mobile device unattended in public places.
- Use the lock function on the mobile device and frequently change the lock password.
- Delete any confidential information from the device prior to any third party servicing.
- Don’t store financial information in your mobile device.
- Use tokens when initiating or approving transactions to help protect against fraud.
  - Discontinue using the mobile banking application if the mobile device is stolen.
  - Report it stolen to the bank and receive new credentials
- Don’t modify the mobile device to:
  - Give yourself more control
  - Enable features that void warranties
  - Change the root file systems
  - Allow modifications to install third-party software or hardware components