LIGHTHOUSE BANK

Mobile Banking Fraud Prevention Best Practices

The security of your information and money is a top priority for us. As the use of Smart Phones and wireless devices continues to grow, we feel it is important to provide you information on additional ways to keep your information safe and prevent potential fraud. The information below is an example of "best practices" for securing your mobile devices.

Best Practices and Protection

With mobile banking, your banking and financial transactions are at your fingertips. Here are some precautions for safe and secure mobile banking.

- Set up a PIN/password to access the menu on your mobile device.
- Delete junk messages and chain messages regularly.
- Do not open any URL in messages that you are not sure about.
- Remember SMS/Text will never ask for sensitive information
- If you have to share your mobile device with anyone else or send it in for repair/maintenance.
  - Clear the browsing history.
  - Clear cache and temporary files stored in the memory as they may contain your account numbers and other sensitive information.
- Set the screen timeout to five minutes or less
- Avoid using auto-complete features that remember names or passwords
- Protect your passwords and never reveal them to anyone
- Do not store personal information or user names and passwords in your mobile device

Manage Your Applications Wisely

- Download apps only from trustworthy sources – Like iTunes® or Google Play™
- Don't install a new app until it has established a good reputation
- Keep applications updated. Remove applications you no longer use

What To Do If Your Device Is Lost or Stolen

- Notify your cellular provider to 'suspend/deactivate' your device until it is located.
- Login to online banking, click on mobile banking, deactivate your mobile device and consider changing your password.

- Notify us to ensure your device is disabled even if your cellular provider has deactivated your device (applications/web may still be accessed via Wi-Fi connections), or your device has been located by calling 1-831-600-4000 Monday – Thursday from 9:00 am to 5:00 pm or Friday from 9:00 am to 6:00 pm.
- If enabled, remotely wipe the data from your device

Additional Precautions and Protection

- Make passwords unique- truly safe passwords don't incorporate names, phone numbers, addresses, known dates.
- Never leave your mobile device unattended- while using Bank's mobile app or any other mobile activity.
- Install an anti-malware application – there are several available, like Lookout™, Sophos™, etc.
- Be careful of any mobile device bought second-hand from places like eBay™ or Craigslist – they can contain pre-installed malicious software
- Know where your device is and don't loan it to anyone
- Just like your computer, do not click on links in emails or texts that you are not familiar with
- Be aware of your surroundings when in public to help prevent theft
- Auto-wipe your device if PIN/password is entered incorrectly after 10 attempts
- Do not use public Wi-Fi/WLAN to conduce wireless banking