Here is a list of things that you can do to significantly reduce the risk of fraud and identity theft while using our mobile banking services.

- Password protect your mobile device and lock it when not in use
  - Don't reveal password information to anyone or keep it stored on your phone; and
  - Don't let your phone automatically log you in or save your login information.
- Never disclose personal information about your accounts via text or email.
  - We will never ask you to disclose your password or account number via text or email.
  - Text messages and emails are not transmitted in a secure environment.
- Review your accounts on a regular basis to help detect any unauthorized activity.
- Only download applications from reliable sources such as the Apple Store, Android Marketplace or Blackberry App World.
- Make sure you are using a secure internet browser and connection while connected to mobile banking.
- Use text alerts to notify you when your account balance drops below a certain threshold.
- If available, install mobile anti-virus and anti-Spyware software on your mobile phone.
- If your phone was lost or stolen**,** immediately disable your lost or stolen phone within online banking, under OPTIONS.
  - Call your mobile service provider to disconnect your phone service.
  - Change your online banking password.
- If you change your Mobile number, immediately log into online banking and disable your old number.
- Log Out of Mobile Banking when you are finished.

Sharon Savings Bank has provided you these best practices to help assist you safeguard your confidential and financial information. Please be certain to implement these practices to mitigate your risk of loss. Sharon Savings Bank will not be responsible for losses related to security weaknesses within your personal online banking access devices.