Best Practices and Recommendations for use of Mobile Banking/IMPS/UPI

- Reduce the risk of downloading potentially harmful apps by limiting your download sources to official app stores, such as your device’s manufacturer or operating system app store.
- Prior to downloading / installing apps on android devices (even from Google Play Store):
    - ➢ Always review the app details, number of downloads, user reviews, comments and "ADDITIONAL INFORMATION" section.
    - ➢ Verify app permissions and grant only those permissions which have relevant context for the app's purpose.
    - ➢ Do not check "Un-trusted Sources" checkbox to install side loaded apps.

- Install Android updates and patches as and when available from Android device vendors.
- Do not browse un-trusted websites or follow un-trusted links and exercise caution while clicking on the link provided in any unsolicited emails and SMSs.
- Install and maintain updated anti-virus and antispyware software.
- Look for suspicious numbers that don't look like real mobile phone numbers. Scammers often mask their identity by using email-to-text services to avoid revealing their actual phone number. Genuine SMS messages received from banks usually contain sender id (consisting of bank’s short name) instead of a phone number in sender information field.
- Do extensive research before clicking on link provided in the message. There are many websites that allow anyone to run search based on a phone number and see any relatable information about whether or not a number is legit.
- Only click on URLs that clearly indicate the website domain. When in doubt, users can search for the organisation's website directly using search engines to ensure that the websites they visited are legitimate.
- Consider using Safe Browsing tools, filtering tools (antivirus and content-based filtering) in your antivirus, firewall, and filtering services.
- Exercise caution towards shortened URLs, such as those involving bit.ly and tinyurl. Users are advised to hover their cursors over the shortened URLs (if possible) to see the full website domain which they are visiting or use a URL checker that will allow the user to enter a short URL and view the full URL. Users can also use the shortening service preview feature to see a preview of the full URL.
- Look out for valid encryption certificates by checking for the green lock in the browser's address bar, before providing any sensitive information such as personal particulars or account login details.
- Customer should report any unusual activity in their account immediately to the respective bank with the relevant details for taking further appropriate actions.