Guideline: REs shall incorporate secure, safe, and responsible usage guidelines and training materials for end users within the digital payment applications. They shall also make it mandatory (i.e. not providing any option to circumvent/ avoid the material) for the consumer to go through secure usage guidelines (even in the consumer's preferred

language) while obtaining and recording confirmation during the on-boarding procedure in the first instance and first use after each update of the digital payment application or after major updates to secure and safe usage guidelines.

Indicative Guidelines:

- The Customer shall, at its own risk and consequences, access and use the application services by following the safe and secure guidelines prescribed by the Bank from time to time, including the use of user credentials or OTPs or any other suitable means of authentication as decided by the Bank.
- The Customer and the Users shall keep all OTPs and passwords confidential and well protected and should not reveal the same to any unauthorized person or other third party. Bank shall in no manner be held responsible, if the customer incurs any loss as a result of the user credentials being disclosed by the Customer or User to any unauthorized person or other third parties.
- Bank shall adopt appropriate security measures as in when available in the industry from time to time. However, the Customer acknowledges that the technology used including the internet, usage of public and shared facilities is susceptible to a number of risks, such as hacking, fraudulent transactions, data breach , any or all of which could affect the application services. Bank will not be responsible for any loss, delays or failures caused to or incurred by the Customer/User in the processing of Instructions on account of such risks.
- The Customer shall refrain from performing transactions in the application via shared computer or through unprotected public network (e.g., open Wi-Fi) as it could be leveraged to compromise the user's account.
- In case of web application, customers should log off from the application or close the browser when the application is not in use.
- The Customer shall be vigilant with respect to phishing*, vishing** and smishing*** attacks
  * A technique for attempting to acquire sensitive data, such as bank account numbers, internet banking passwords, other critical credentials/information through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.
  ** A technique for attempting to acquire sensitive data, such as bank account numbers, internet banking passwords, other critical credentials/information through a fraudulent solicitation over a voice call, in which the perpetrator masquerades as a legitimate business or reputable person.
  *** A technique for attempting to acquire sensitive data, such as bank account numbers, internet banking passwords, other critical credentials/information through a fraudulent solicitation through SMS, in which the perpetrator masquerades as a legitimate business or reputable person.
- The Customer shall note that Bank employee/staff will not request the customer to share the transaction OTP with the Bank employee/staff.
- The Customer shall ensure the application is up to date and update or re-download (if required) the application only via authorised channel/play store.
- The Customer must refrain from downloading application APK files from the internet.