Secure usage guidelines for OneCard mobile application

Updated on 19 March 2025

This document sets forth the general secure usage guidelines that apply to the access and use of mobile application 'OneCard' ("**App**") operated and managed by FPL Technologies Private Limited and may include its affiliates ("**Company**").

Do's

- Download the App from a secure store (Google Play Store, IOS Store).
- Regularly check your credit card statements to ensure that all transactions are legitimate.
- While exchanging, selling, lending or giving your phone for repairs, please make sure that the App is uninstalled and temporary files, browsing history and cache cleared.
- If you receive any suspicious e-mails and you unknowingly provided personal information or financial information, report it to help@getonecard.app
- Always report phishing. If you have responded to one of these suspicious e-mails, report it to help@getonecard.app
- Enter your App PIN / password only in the space provided for. Change your App PIN / password at least once every 90 (ninety) days.
- You can also enable fingerprint authentication for logging into your mobile device.
- Use multi-factor authentication, since this adds an extra layer of security beyond passwords.
- Ensure to close the App when you are done using App.
- Regularly update your App in your mobile device, and your mobile device's software whenever a new update is available.
- You can set limits for online transactions, POS payments, contactless/tap to pay, BharatQR transactions from the 'My Controls' section in the App. It is advisable to set a lower limit for the mentioned transaction types. You can update the limit as and when required through App.
- You can also activate or deactivate any of online transactions, POS payments, contactless/tap to pay, BharatQR transactions from the 'My Controls' section in the App.

Don't's

- Your App PIN / passwords should not be the same as other applications.
- Do not share your App PIN / password as this is a security risk.
- Avoid downloading applications which can take remote access or which can record your App screens.
- Do not save passwords on your mobile device.
- Avoid using unsecured Wi-Fi networks while accessing App.
- Do not share any of your confidential information vis-à-vis App through suspicious emails, websites, social media networks, text messages or phone calls.
- The Company neither asks any user or customer to install any other application nor asks the user or customer to do screen sharing. The Company never sends email / SMS or makes phone calls for getting customer information like card number or CVV. Please report immediately by emailing to help@getonecard.app if you receive any e-mail purported to be originated by the Company.