

## **Important Advisory on E-Payment User Protection Guidelines**

The Monetary Authority of Singapore (“MAS”) issued the E-Payments User Protection Guidelines (“Guidelines”) to set out the duties of responsible financial institutions and consumers in relation to unauthorised and erroneous payment transactions in relation to protected accounts (EZ-Link Wallet with Mastercard), and provides guidance on the liability for losses arising from unauthorised transactions.

The Guidelines establish a common baseline protection that Financial Institutions including SimplyGo will provide to customers from losses arising from unauthorised or erroneous e-payment transactions from their protected accounts.

SimplyGo will provide you with transaction notifications and a reporting channel, so that you may be alerted of unauthorised transactions and report them should they happen. SimplyGo will investigate all claims of unauthorised transactions with the aim of achieving a fair and reasonable resolution.

### **Your Role and Responsibility**

We are also required under the Guidelines to draw to your attention your role and responsibility under the Guidelines. Please note that you are required to take reasonable steps to:

- ensure that your phone is protected with a secure password or other security mechanism and not to disclose it to any other person;
- ensure that your contact details with SimplyGo are kept up to date; and
- ensure that access to the SimplyGo App is kept safe and secure.

We recommend that for your protection to enable transaction notification alerts on your device used to receive transaction notifications from us, to opt to receive all transaction notifications for all outgoing transactions of (any amount) made from your account, and to monitor the transaction notifications sent to the account contact.

Your responsibilities include: -

- practise good security hygiene by changing your login password and payment pin periodically and do not share these details or your One Time Password with anyone
- do not download and install applications from third-party websites outside official sources (“sideload apps”), in particular unverified applications which request device permissions that are unrelated to their intended functionalities
- monitor transaction notifications and report unauthorised transactions to SimplyGo as soon as possible

- provide information on unauthorised transactions as requested by us to support investigations
- close SimplyGo App every time you are not using the App or have finished using it
- only download SimplyGo app from the official app stores (Google Play Store / Apple Play Store)
- check carefully the e-payment instruction and details of the recipient before executing or confirming any e-payment transaction
- patch the device's operating systems with regular security updates provided by the operating system provider

#### SimplyGo's role and responsibilities

- We will provide you with transaction notification that fulfils MAS' criteria to enable you to determine if any transaction is authorised by you;
- We will provide you with reporting channel for the purposes of reporting unauthorised or erroneous transactions;
- We will assess any claim made by you in relation to any unauthorised transaction covered in Section 5 of the Guidelines in a fair and reasonable manner;

Please note that the above is only a summary of the E-Payment User Protection Guidelines and customers are advised to access the complete and updated version of the Guidelines at <https://www.mas.gov.sg/regulation/guidelines/e-payments-user-protection-guidelines>