Important Information on the E-Payments User Protection Guidelines

(For Individuals)

The Monetary Authority of Singapore ("MAS") issued the E-Payments User Protection Guidelines ("Guidelines") with the objective of standardising protection offered by responsible financial institutions to individuals from losses arising from unauthorised transactions or erroneous transactions. Any term used in this notice shall have the same meaning as defined in the Guidelines, unless expressly defined otherwise.

In accordance with the Guidelines, CIMB Bank Berhad, Singapore Branch ("CIMB Bank") is issuing this notice to account holders and account users of protected accounts about:

a. their duties as set out in Section 3 of the Guidelines (Part A of this notice); and

b. CIMB Bank's duties as set out in Section 4 (excluding paragraph 4.3) of the Guidelines (Part B of this notice).

Please note that this notice is only a summary of the Guidelines and you should visit the MAS website to access the complete and updated version of the Guidelines and/or refer to our Terms and Conditions Governing Electronic Banking Services available on our website.

Part A: Duties of account holders and account users

1. Provide contact information, opt to receive all outgoing transaction notifications and monitor notifications

   Please ensure that the contact information which you have provided to us is up-to-date. If you wish to change/provide your mobile phone number or email address, you may do so via Clicks Internet Banking or email/mail to us the Personal Particulars Update Form.

   For security reasons, each mobile number and email address can only be used by one customer for receiving such notifications. It is your responsibility to enable transaction notification alerts on the device you use to receive such notifications from us and to monitor all transaction notifications sent by CIMB Bank.

2. Protect access codes and protect access to protected account

   1. Protect yourself and your computer/mobile devices

      At CIMB Bank, we are committed to protect your online security and peace of mind. We use multiple layers of security to ensure that your Online Banking sessions are protected by a high level of security. However, you also play an important role in safeguarding your computer/mobile devices and your online information. Below are some recommendations on how to stay safe online below.

   2. Install anti-virus and anti-malware software

      Protect your devices from virus and malware by installing anti-virus and anti-malware software. To maximise your protection, update them regularly to ensure you always have the latest virus definition.

   3. Avoid rooting or jailbreaking your mobile devices

It is not advisable to install or access CIMB Clicks Mobile App on a rooted or jailbroken mobile device as it poses potential risks to viruses and malicious software, making it vulnerable to fraudulent attacks. You are advised to download your Mobile Banking application only from authorized sources such as Apple App Store or Google Play Store.

4. Install a personal firewall

   Firewall software and/or hardware helps provide a protective shield between your computer/mobile device and the Internet. This barrier can help prevent unauthorised people gaining access to your computer/mobile device, reading information from it or placing viruses on it while you are connected to the Internet.

5. Install anti-spyware software

   Spyware is a general term for hidden programs on your computer/mobile devices that track what you are doing on your computer/mobile devices. Spyware is often bundled together with file sharing, email virus checking or browser accelerator programs, and it is installed on your computer/mobile devices without your knowledge to intercept information about you and your computer/mobile devices. The type of information gathered can include personal Internet usage, and in some instances, confidential data such as passwords. You can download and run a specialist program designed to help identify and remove threats from spyware. Like an anti-virus program, it also needs to be regularly updated in order to recognise the latest threats.

6. Keep your browser and operating system up-to-date

   From time to time security weaknesses or bugs are found in browsers and operating systems. Usually 'Service Packs' are issued by the software company to make sure these are fixed as quickly as possible. You should make regular checks on your software vendor's website and apply any new security patches as soon as possible to ensure you have the most updated security features available.

7. Avoid running programs or opening email attachments from any source you do not know or trust

   You should avoid installing software or running programmes of unknown origin and avoid opening email attachments from any source you do not know or trust. We also recommend that you scan all email attachments for viruses and delete junk and chain emails on a regular basis. Also, never call a number appearing on an email you suspect is fraudulent. A phony telephone number may be used in the email.

   Important note: The bank will never ask you to disclose, change or update your personal banking information via emails, phone or SMS. You could be coaxed into entering a bogus website that may look fraudulently identical to the bank's site. If you have received any unauthorized request, please call us immediately at +65 6333 7777 or email to AtYourService@cimb.com

3. Please ensure that you check the transaction details and recipient credentials carefully before confirming any payment transaction.

   In addition, please do not:

   a. Voluntarily disclose your access code (e.g. OTP, Internet Banking Login ID and Password, etc.) to any third party.

b. Disclose the access code in a recognisable way on any payment account, authentication device, or any container for the payment account

c. Keep a record of any access code in a way that allows easy access by third party to misuse the code. Instead, CIMB Bank recommends for our account holders to keep such records in a secure electronic or physical location accessible or known only to the account holders.

4. Report unauthorised transactions

In the event that you detect an erroneous and/or unauthorised transaction, immediately report to CIMB Bank after receipt of any transaction notification alert for any unauthorised transaction via one of the following channels:

a. Customer Service Hotline – +65 6333 7777

b. Customer Service Email – AtYourService@cimb.com

c. One of the following branches:

Raffles Place Branch
50 Raffles Place #01-02
Singapore Land Tower
Singapore 048623

Orchard Branch (Across the street from Paragon)
270 Orchard Road #03-02
Singapore 238857

5. Provide information on unauthorised transactions

You are responsible for reporting any unauthorised or erroneous transaction to CIMB Bank as soon as possible after receiving notification of the transaction. In the event that you are unable to report to CIMB Bank as soon as you receive the notification, you may be required to provide CIMB Bank with reasons for the delay.

In the report to CIMB Bank, you are required to provide the following information:

a. The protected account that is affected

b. The account holder's identification information

c. The type of authentication device, access code and device that is used to perform the payment transaction

d. The name or identity of any account user for the protected account that was used

e. Details on whether or not the protected account's authentication device or access code was lost, stolen and misused and if so, the

f. Date and time of loss or misuse

g. Date and time that the loss or misuse was reported to us; and

h. Date and time and method that the loss or misuse was reported to the police

i. If access code is applicable to the protected account:

j. How the account holder / user recorded the access code; and

k. Whether the account holder / user had disclosed the access code to anyone.

l. Any other information about the unauthorised transaction that is known to the account holder and/or CIMB Bank may require.

m. Make a police report

You should make a police report if CIMB Bank requests such a report to be made to facilitate our claims investigation process.

Part B: Duties of CIMB Bank

1. When a transaction notification is sent to you, we will:

   a. Send the transaction notification to the main account holder's contact, subject to our Terms and Conditions Governing E-Alerts

   b. Ensure that transaction notifications will be sent to you on a real-time basis or on a batched basis of at least once every 24 hours to consolidate notifiable transaction made in the past 24 hours. Do note that we are not required to send both real time and batched notifications

   c. Send transaction notifications to you either by SMS or email

   d. Ensure that transaction notifications contain the following information:

      i. Information that allows you to identify the protected account such as the account number;

      ii. Information that allows you to identify the recipient whether by name or by other credentials such as the recipient's account number;

      iii. Information that allows us to later identify you, the protected account, and the recipient account;

      iv. Transaction amount;

      v. Transaction time and date;

      vi. Transaction type;

2. We will resolve all claims made by you in relation to an unauthorised transaction in a fair and reasonable manner. In the event that the a claim made by you falls under this notice, we will complete an investigation within 21 business days for straightforward cases or 45 business days for complex cases, provided that you have submitted any claim in accordance with your obligations as per this notice.

3. Please note that any investigation will only commence upon submission of police report for unauthorised transaction. Submission of police report after 5pm of a business day would only commence investigation on next business day. Submission of police report over the weekend will only commence investigation on the next business day.

For more information on the E-Payments User Protection Guidelines by the Monetary Authority of Singapore, please visit www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulations-Guidance-and-Licensing/Payment-and-Settlement-Systems/PSOA-Guidelines/Epayments-User-Protection-Guidelines.pdf.