IMPORTANT NOTICE ON THE E-PAYMENTS USER PROTECTION GUIDELINES

(FOR SOLE PROPRIETORS)

1. Part A – Introduction

1.1. 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 and sole proprietors from losses arising from unauthorised transactions or erroneous transactions.

1.2. Any term used in this notice shall have the same meaning as defined in the Guidelines, unless expressly defined otherwise.

1.3. 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 CIMB Bank Terms and Conditions Governing Electronic Banking Services (available at https://www.cimbbank.com.sg/content/dam/cimbsingapore/business/support/terms-and-conditions/tnc-electronic-banking-service-20150101.pdf).

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

(a) their duties set out in section 3 of the Guidelines (Part B of this notice); and

(b) CIMB's duties set out in section 4 (excluding paragraph 4.3) of the Guidelines (Part C of this notice).

2. Part B – Duties of Customers

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

(a) It is the Customers' responsibility to enable transaction notifications on any device used to access BizChannel@CIMB and receive transaction notifications from CIMB.

(b) Customers should opt to receive transaction notifications for all outgoing transactions of (any amount) made from protected accounts, and to monitor the transaction notifications sent to the Customers. This will include Customers monitoring all transaction e-alerts such as SMS, email from CIMB, and checking the transaction details etc.

(c) Customers should update contact particulars if they are existing subscribers of transaction e-alerts or sign-up for this service by using the relevant forms available at:

(i) https://www.cimbbank.com.sg/content/dam/cimbsingapore/business/support/forms/daily-banking/form-e-alerts-service-update-20181025.pdf (for update of particulars); or

(ii) https://www.cimbbank.com.sg/content/dam/cimbsingapore/business/support/forms/daily-banking/form-corp-e-alerts-service-app-20180427.pdf (for new application).

2.2. Protect access codes and protect access to protected account

(a) Customers should protect the access codes they use to authenticate any payment transaction and to protect access to their protected account by ensuring that they use strong passwords and keeping the relevant security software updated.

(b) Without limitation to the generality of the foregoing, Customers should consider adopting the recommendations below:

(i) Install anti-virus and anti-malware software: Customers should protect their devices from virus and malware by installing anti-virus and anti-malware software. To maximise the protection, update the anti-virus and anti-malware software regularly to ensure that the latest virus definition is being used for such software.

(ii) Install a personal firewall: Firewall software and/or hardware helps provide a protective shield between your computer and the Internet. This barrier can help unauthorised people gaining access to your computer, reading information from it or placing viruses on it while you are connected to the Internet.

(iii) Install anti-spyware software: Spyware is a general term for hidden programs on your computer that track what you are doing on your computer. Spyware is often bundled together with file sharing, email virus checking or browser accelerator programs, and it is installed on your computer without your knowledge to intercept information about you and your computer. 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.

(iv) 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.

(v) Avoid running programs or opening email attachments from any source you don't know or trust: You should avoid installing software or running programmes of unknown origin and avoid 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.

2.3. Report unauthorised transactions and provide information on unauthorised transaction

(a) In the event that a Customer detects an erroneous and/or unauthorised transaction, immediately report to CIMB during office hours from Monday to Friday (9am to 6pm) via:

(i) BizChannel@CIMB Hotline at (65) 6438 7888; and/or

(ii) Client Service Email at sg.bizchannelsupport@cimb.com.

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

(c) In the report to CIMB, you are required to provide the following information:

(i) The protected account that is affected;

(ii) The account holder identification information;

(iii) The type of authentication device, access code and device that is used to perform the payment transaction;

(iv) The name or identity of any account user for the protected account that was used;

(v) Details on whether or not the protected account's authentication device or access code was lost, stolen and misused and if so, the following details:

(A) Date and time of loss or misuse;

(B) Date and time that the loss or misuse was reported to CIMB; and

(C) Date and time and method that the loss or misuse was reported to the police.[1]

(vi) If access code is applicable to the protected account:

(A) How the account holder / user recorded the access code; and

(B) Whether the account holder / user had disclosed the access code to anyone.

(vii) Any other information about the unauthorised transaction that CIMB may require.

3. **Part C – Duties of CIMB**

3.1. Transaction Notification

(a) CIMB provides a transaction alert service to Customers via SMS and/or email, which Customers will need to opt-in to receive. The said transaction alert will be sent to Customers when both incoming and outgoing transaction(s) are performed on the designated account(s) nominated by Customers in the setup form[2] and such alert will contain the following information:

(i) details to allow Customers to identify the protected account such as the account number;

(ii) transaction amount;

(iii) transaction time and date;

(iv) transaction type; and

(v) transaction reference number.

(b) Customers are able to define the transaction threshold amounts to receive the transaction notifications. For the avoidance of doubt, the existing thresholds selected by Customers prior to the date of this notice will continue to apply, unless Customers notify CIMB otherwise in writing.

3.2. Providing details of online transactions to Customers

Where transactions are made by way of internet banking, any mobile phone application or device arranged for payment transactions, CIMB will provide an onscreen opportunity for the

[1] *In addition to informing us of an unauthorised transaction, you should also make a police report for the unauthorised transaction in order to facilitate the investigation process. Please note that the timeline to complete the investigation process, as stated in the Guidelines, will only start once a valid police report is made.*

[2] *Customers will need to provide instructions to CIMB in relation to receiving transaction notifications using the relevant form specified in paragraph 2.1(c) of this notice.*

person who is making the transaction to confirm the payment transaction and recipient credentials before any authorised payment transaction is executed.

3.3. Investigation and claims process

(a) CIMB will facilitate communication between Customers and the payment recipients with the objective of recovering the payment for erroneous transactions.

(b) Depending on the complexity of the case, CIMB will typically need up to 45 business days to complete our investigation provided that Customers have submitted their claims in accordance with the requirements which CIMB will impose from time to time.

Information correct as of 30 June 2019

Notice issued by CIMB Bank Berhad Singapore Branch (Company No: 13491-P), a licensed financial institution incorporated in Malaysia and registered in Singapore as a foreign company (UEN: S99FC5759D)