POLICY HIGHLIGHTS SHEET

E-payments User Protection Guidelines

PREFACE
This is a policy highlights sheet to seek views from **individuals and micro-enterprises** on MAS' proposals for **E-payments User Protection Guidelines** (the "**Guidelines**").[1] The paper will cover the following: (a) What are the Guidelines MAS is proposing; (b) Why MAS is proposing the Guidelines; (c) What the measures mean for account holders and account users; (d) Expected timeline for the implementation of the Guidelines; and (e) Areas for which MAS is seeking public feedback on.

PART 1: WHAT ARE THE GUIDELINES MAS IS PROPOSING
MAS proposes to issue the Guidelines to set standards on the following areas: (a) When an unauthorised transaction is made, whether the account holder is liable for any amount lost, and if so, how much; (b) What account holders, account users, and financial institutions ("**FIs**") should do to protect e-payment accounts; and (c) How FIs and account holders can resolve unauthorised payment transactions and payments sent to the wrong party. We seek your views on the Guidelines explained in Part 3 below.

PART 2: WHY MAS IS PROPOSING THE GUIDELINES
MAS is proposing the Guidelines to encourage adoption of e-payments by making e-payments solutions simpler and more secure to use. By setting standards on the protection of access to account user funds in e-payment accounts, MAS aims to address the protection for account holders arising from unauthorised or erroneous payment transactions from the protected accounts. Protected accounts are payment accounts that: (a) allow for electronic payment transactions to be made; (b) are operated by a bank, credit card company, finance company or widely accepted stored value facility holder;[2] (c) are held in the name of an individual or micro-enterprise; and

[1] This note is intended to provide an overview of the guidelines which MAS would like to seek feedback from the public on. Readers may wish to read this in conjunction with MAS' consultation paper on the proposed E-payments User Protection Guidelines, accessible here.

[2] The current widely accepted stored value facility holders are EZ-Link Pte Ltd, Network for Electronic Transfers (Singapore) Pte Ltd (NETS), and CapitaLand Voucher Pte Ltd.

(d) can have a balance of more than S$500, or is a credit facility.

An account holder must be an individual or micro-enterprise. A micro-enterprise is any business employing fewer than 10 persons or with an annual turnover of no more than S$1 million.
An account user is any account holder or any person that the account holder has authorised to use the account holder's protected account.

The guidelines are intended to protect e-payment users from higher value losses. Accounts which can hold a limited amount of less than S$500 such as transport stored value cards are not covered in these guidelines. These cards are usually bearer instruments and users of such cards are encouraged to safe-keep such cards as they would with cash.

PART 3: WHAT DOES THIS MEAN FOR ME?

Measures related to unauthorised transactions

Some measures apply to both the account holder and the account user. However, the account holder is responsible for the actions of the account user as the account user's use of the protected account is permitted by the account holder.

What the account holder is liable for in any unauthorised transaction

The Guidelines clarify when, and if so how much, an account holder should pay (i.e. is liable) for losses arising from unauthorised transactions. Unauthorised transactions are payment transactions made from the protected account which the account user did not know of and consent to.

Outcome A: Account holder is not liable for any loss.

Where the account holder did not contribute to the loss, and where he took full care of his protected account, he is not liable for such loss. This includes situations where the FI or merchant has been fraudulent or negligent, or where the account holder shows that the account user did not contribute to the loss.[3]

- This means that you as an account holder are not liable for any loss if it arises from situations you are not responsible for.

Outcome B: Account holder is liable only up to S$100.

The account holder is liable for a loss of not more than S$100 when the account user was not reckless but nevertheless contributed to the loss.

- This means that you as the account holder will be liable for up to S$100 if the loss arises from situations you contributed to. This is provided that you and your account user (if any) were not reckless.

[3] Please see paragraph 4.1 of the consultation paper for further details.

Outcome C: Account holder is liable for actual loss.

The account holder is liable for actual loss when the loss occurred primarily due to r recklessness of the account user. The actual loss will be capped at any applicable transaction limit or daily payment limit that the account holder and FI have agreed to.

- This means that you as the account holder are liable for actual loss if the loss arises from the recklessness of any person you authorised to use your protected account (including yourself).
- Please note that the account holder is liable for all transactions authorised by any account user, including a situation where the account user acted fraudulently to defraud the account holder or responsible FI.

How an FI should protect the account holder

The Guidelines also clarify that the FI that issues or operates any protected account should provide the account holder or account user with all the following:

(a) adequate transaction notifications;
(b) opportunity for account user to confirm payment transactions; and
(c) a free transaction reporting channel.

FI should provide sufficient transaction notifications to allow the account holder to properly monitor his protected account.

- The FI should send the account holder a consolidated list of all the transactions made to or from the protected account, at least once a day.
- The notifications should be sent to the account holder's phone number by SMS or email address.
- The notification should contain detailed information of the transaction including, recipient credentials, transaction amount, time and date, and the merchant's trading name.

How account holders and account users should secure their access codes and protected accounts

Account holders and account users are encouraged to complete and adopt the following tasks and security habits regarding their protected accounts and access codes (i.e. passwords or pass codes).[4]

Account holders should:

(a) Give his or her updated contact information to the FI and monitor notifications from the FI;
(b) Report unauthorised transactions to the FI by the next business day;
(c) Give the FI full information on any unauthorised transaction; and
(d) Make a police report if requested to by the FI.

[4] Please see Part B of the consultation paper for the full set of duties.

Account users should, with reference to the **Annex** to this paper:

(a) Protect access codes; and

(b) Protect access to protected account.

Measures related to mistaken transactions

What to do in the event that a payment is made to the wrong person

We encourage account users to check the recipient's details carefully before executing any payment transaction. However, if a payment is accidentally made to the wrong person, both the payer's FI and the recipient's FI should make reasonable efforts to recover the money paid to the wrong person within the proposed timeline. This includes informing the recipient of the transaction and that wrongful retention of money that does not belong to him or her, is a criminal offence.

PART 4: EXPECTED TIMELINE

MAS plans to develop and publish the Guidelines in the first half of 2018.

We would like to hear from you!

MAS welcomes your feedback, which should be sent by **16 March 2018** to epaymentsconsult@mas.gov.sg.

In particular, we would like to know your views on:

(a) Whether the overall framework will be useful for you as an account holder or account user.

(b) Proposed scope of a "protected account".

(c) Proposed scope of Outcomes A, B and C.

(d) Whether the duties proposed for account holders and account users are reasonable and useful for the purposes of protecting e-payment accounts.

(e) Whether the duties of FIs are useful and what else you think FIs should do.

Annex

Duties of account users to protect access code[5]

An account user should not do any of the following:

(a) Voluntarily disclose any access code to any third party, except as instructed by the responsible FI for any purpose including to initiate or execute any payment transaction involving the protected account;

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

(c) Keep a record of any access code in a way that allows any third party to easily misuse the access code.

If the account user keeps a record of any access code, he should make reasonable efforts to secure the record, including:

(a) Keeping the record in a secure electronic or physical location accessible or known only to the account user; and

(b) Keeping the record in a place where the record is unlikely to be found by a third party.

Duties of account users to secure the protected account[6]

The account user should at the minimum do the following where a device is used to access the protected account:

(a) Update the device's browser[7] to the latest version available;

(b) Patch the device's operating systems[8] with regular security updates;

(c) Install and maintain the latest anti-virus software on the device;

(d) Use strong passwords, such as a mixture of letters, numbers and symbols; and

(e) Enable notification alerts on transactions initiated by or executed using the protected account.

The account user should also where possible follow security instructions or advice provided by the responsible FI to the account holder.

[5] Please see paragraphs 5.4 and 5.5 of the consultation paper

[6] Please see paragraphs 5.6 and 5.7 of the consultation paper

[7] Examples: Chrome, Safari, Internet Explorer, Firefox

[8] Examples: Windows operating system (OS), Macintosh OS, iOS, Android OS