CONSULTATION PAPER

P004 - 2018

February 2018

Proposed E-payments User Protection Guidelines

Monetary Authority of Singapore

Contents

1 Preface

1.1 In 2016, MAS embarked on a review of the regulatory framework governing payment services in Singapore with a view to modernising and streamlining the existing frameworks to encourage the wider adoption of electronic payments ("**e-payments**") in Singapore. Arising from this review, MAS consulted twice on the proposed activity-based Payment Services Bill (the "**Bill**") in August 2016 and November 2017[1].

1.2 As part of the payment services regulatory review, one key recommendation to encourage the use of e-payments was to enhance consumer or account user protection[2]. MAS has proposed measures to protect funds belonging to account users and merchants in the Bill. However, a comprehensive framework will also need to provide protection for account users from losses arising from unauthorised or mistaken payment transactions.

1.3 To reduce these risks of unauthorised or mistaken payment transactions to users, MAS proposes to issue a set of guidelines to standardise the protection given to users arising from these two risks. The proposed guidelines will cover the following key areas:

(a) Liability caps to clarify the amounts that the account user and the financial institution is liable for in any unauthorised payment transaction;
(b) Notification duties of account users and financial institutions for all payment transactions; and
(c) Resolution processes for both unauthorised payment transactions and mistaken payment transactions.

1.4 These guidelines will apply to banks and non-bank credit card issuers under the Banking Act (Cap. 19) ("**BA**"), finance companies under the Finance Companies Act ("**FCA**") and widely accepted stored value facility ("**WA SVF**") holders under the Payment Systems (Oversight) Act (Cap. 222A) ("**PS(O)A**"). When the Payment Services Bill commences, MAS

[1] Please see page 35 of the November 2017 consultation paper where MAS announced that a separate consultation paper will be published to seek feedback on proposed guidelines to set standards on the protection of access to funds in payment accounts.

[2] Please see page 21 of the Singapore Payments Roadmap report which may be accessed at this link: http://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Press%20Releases/Singapore%20Payments%20Roadmap%20Report%20%20August%202016.pdf.

also intends to make the guidelines applicable to payment services licensees that issue payment accounts.

1.5 Parts 2 to 8 of this consultation paper set out the proposed Guidelines, explanations of policy intent and corresponding consultation questions. The explanations aim to guide the reader, and will not form part of the final Guidelines. Both the explanations and consultation questions are marked out clearly in box text.

1.6 The **Annex** sets out a list of questions asked in this paper. A Policy Highlights Sheet which summarises the key proposals for consideration and feedback by consumers is available together with this consultation paper on the consultation paper section of the MAS website.

1.7 MAS invites comments from:

a) Financial institutions – Banks, non-bank credit card issuers, finance companies, and holders of WA SVFs;

b) Businesses – Retail businesses, billing organisations (e.g. telecommunication and utility companies, town councils, and strata management corporations); and

c) Other interested parties – Members of the public, consumer associations, government agencies, law firms, trade associations, non-profit organisations, charities and other parties who may be impacted by or interested in the proposed review.

Please note that all submissions received will be published and attributed to the respective respondents unless they specifically request MAS not to do so. As such, if respondents would like (i) their whole submission or part of it, or (ii) their identity, or both, to be kept confidential, please clearly state so in the submission to MAS. In addition, MAS reserves the right not to publish any submission received where MAS considers it not in the public interest to do so, such as where the submission appears to be libellous or offensive.

1.8 Please submit written comments by 16 March 2018 to –

E-payments User Protection Guidelines
FinTech and Innovation Group
Monetary Authority of Singapore
10 Shenton Way, MAS Building
Singapore 079117
Fax: (65) 62203973
Email: epaymentsconsult@mas.gov.sg

1.9 Electronic submission is encouraged. We would appreciate that you use this suggested format for your submission to ease our collation efforts.[3]

[3] If you are providing a PDF version of your response, we would be grateful if you could also send a Word copy of your response for our collation.

2 Application of the Guidelines

2.1 These Guidelines set out the expectations of the Monetary Authority of Singapore (the "**Authority**") of any responsible financial institution ("**FI**") that issues or operates a protected account. The terms "protected account" and "responsible FI" are defined in these Guidelines.

2.2 The aim of these Guidelines is to standardise the protection offered to individuals or micro-enterprises from losses arising from unauthorised or mistaken payment transactions from the protected accounts of these account holders.

2.3 These Guidelines provide general guidance, and are not intended to be comprehensive nor replace or override any legislative provisions. They should be read in conjunction with the provisions of the relevant legislation, the subsidiary legislation made under the relevant legislation, as well as written directions, notices, codes and other guidelines that MAS may issue from time to time pursuant to the relevant legislation and subsidiary legislation.

Explanation for Question 1

We propose to issue these Guidelines with a view to encourage the wider adoption by the public of e-payments in Singapore, by enhancing account user protection in respect of access to the user's funds in any protected account. To balance the interests of account users and costs to the responsible FI, the scope of these Guidelines is intended to:

(a) clarify the responsibilities and liabilities of responsible FIs and account users for unauthorised payment transactions and mistaken payment transactions;
(b) protect account users that are individuals or micro-enterprises as they generally are less able to negotiate terms of agreement with FIs, as compared to large corporations; and
(c) protect payment accounts that are credit facilities or have a load capacity of greater than S$500 where a large amount of account user funds may be lost in an unauthorised or mistaken payment transaction.

Payment transactions arising from scams are more suitably addressed through other means such as police investigations and specialised guidelines as those are more

generally intended to deceive and cheat, with an authorised and intended payment being incidental to consummating the scam, rather than to exploit any vulnerability or having the effect of damaging confidence in e-payments. MAS will together with other public agencies and industry associations continue to monitor trends in payment transaction scams and assess the need to issue guidance where suitable.

Question 1. **Scope of application.** MAS seeks comments on the scope of payment transactions, protected accounts, account users, and responsible FIs selected for protection under these Guidelines, and whether other types of payment transactions, payment accounts, users of payment services, and FIs should also be within the ambit of these Guidelines. MAS also seeks views on whether this set of Guidelines achieves the intended effect of increasing consumer confidence in the use of e-payments and encouraging the wider adoption by the public of e-payments in Singapore.

3 Definitions

3.1 For the purposes of these Guidelines:

"**access code**" means a password, code or any other arrangement that the account user must keep secret, that may be required to authenticate any payment transaction or account user, and may include any of the following:

(a) personal identification number, password or code;
(b) internet banking authentication code;
(c) telephone banking authentication code;
(d) code generated by an authentication device;
(e) code sent by the responsible FI by phone text message such as SMS,

but does not include a number printed on a payment account (e.g. a security number printed on a credit card or debit card).

"**account agreement**" means the terms and conditions that the responsible FI and account holder have agreed to that governs the use of a payment account issued by the responsible FI to the account holder;

"**account contact**" means the contact information that the account holder provided the responsible FI under paragraph 5.1;

"**approved holder"** has the same meaning as in section 2(1) of the Payment Systems (Oversight) Act (Cap. 222A);

"**account user**" means—
(a) any account holder; or
(b) any person who is authorised in a manner in accordance with the account agreement, by the responsible FI and any account holder of a protected account to initiate, execute or both initiate and execute payment transactions using the protected account;

"**authentication device**" means any device that is issued by the responsible FI to the account user for the purposes of authenticating any payment transaction initiated from a payment account, including a device that is used to generate, receive or input any access code;

"**account holder**" means any person in whose name a payment account has been opened or to whom a payment account has been issued, and includes a supplementary credit card holder and a joint account holder;

"**bank"** has the same meaning as in section 2(1) of the Banking Act (Cap. 19);

"**currency**" means currency notes and coins which are legal tender in Singapore or a country or territory other than Singapore;

"**e-money**" means any electronically stored monetary value that is denominated in any currency that—

(a) has been paid in advance for the purpose of making payment transactions through the use of a payment account;

(b) is accepted by a person other than the person that issues the e-money; and

(c) represents a claim on the person that issues the e-money;

but does not include any deposit accepted in Singapore, from any person in Singapore, by a person in the course of carrying on (whether in Singapore or elsewhere) a deposit-taking business;

"**finance company**" has the same meaning as in section 2 of the Finance Companies Act (Cap. 108);

"**micro-enterprise**" means any business employing fewer than 10 persons or with annual turnover of no more than S$1 million;

"**money**" includes currency and e-money but does not include virtual currency;

"**non-bank credit card issuer**" means a person who is granted a licence under section 57B of the Banking Act (Cap. 19);

"**payee**" means a person who is the intended recipient of money which has been the subject of a payment transaction;

"**payer**" means a person who holds a payment account and initiates, or consents to the initiation of, a payment order from that payment account;

"**payment account**" means—

(a) any account held in the name of, or any account with a unique identifier of, one or more persons; or
(b) any personalised device or personalised facility,
which is used by any person for the initiation, execution, or both of payment transactions and includes a bank account, debit card, credit card and charge card;

"**payment transaction**" means an act, initiated by the payer or payee, of placing, transferring or withdrawing money, irrespective of any underlying obligations between the payer or payee and includes—
(a) the placing, transferring or withdrawing of money for the purposes of making payment for goods or services; and
(b) the placing, transferring or withdrawing of money for any other purpose;

"**protected account**" means any payment account that—
(a) is held in the name of one or more persons, all of whom are either individuals or micro-enterprises;
(b) is capable of having a balance of more than S$500 at any one time, or is a credit facility; and
(c) is capable of being used for electronic payment transactions;

"**responsible FI**" in relation to any protected account, means
any bank, non-bank credit card issuer, finance company or approved holder that issued the protected account;

"**unique identifier**" means a combination of letters, numbers or symbols specified by the responsible FI to the account holder and is to be provided by the account user in relation to a payment transaction in order to identify unambiguously one or both of—

(a) the other person who is a party to the payment transaction;
(b) the other person's payment account;

"**virtual currency**" means any digital representation of value that—
(a) is expressed as a unit;
(b) is not denominated in any currency;
(c) is a medium of exchange accepted by the public or a section of the public, as payment for goods or services or the discharge of a debt; and
(d) can be transferred, stored or traded electronically;

"**unauthorised transaction**" in relation to any protected account, means any payment transaction initiated by any person without the knowledge and consent of an account user of the protected account.

3.2 The expressions used in these Guidelines shall, except where expressly defined in these Guidelines, have the same meanings as in the applicable Acts in which the expressions are referred to or used.

Question 2. Definitions. MAS seeks comments on the proposed definitions to be used in these Guidelines, in particular, whether they are sufficiently clear and suitable. If you propose a different definition for the same term that is from another legislation or paper, please cite the full title of the legislation or paper and the specific provision in that legislation or paper where the term is defined. Please also let us have your views on whether these guidelines should also cover accounts that are not protected accounts but are linked to protected accounts[4], and if so, in what way.

4 Part A: Liability for losses arising from unauthorised transactions

Account holder is not liable for any loss

4.1 The account holder is **not liable** for any loss arising from an unauthorised transaction if the loss arises from any of the following situations:

(a) Fraud or negligence by the responsible FI, its employee, its agent or any third party engaged by the responsible FI;

(b) Fraud or negligence by a merchant from whom any account user purchases or has previously purchased goods or services, or that merchant's employee or agent;

(c) A device including an authentication device, access code, unique identifier, application or system that is not valid, including one that is compromised, forged, faulty, expired or terminated, but not by reason of any account user's action;

[4] For example, some transport stored value cards allow automatic top ups from bank accounts linked to the stored value card.

(d) A payment transaction requiring the use of an authentication device, access code or unique identifier, that is initiated or executed before any account user received the authentication device, access code or unique identifier;

(e) A payment transaction that was initiated or executed after the responsible FI was informed by any account holder that there has been a breach or loss of the protected account or any authentication device or access code for that protected account;

(f) Any account holder shows that the account user has not contributed to the loss, and where the account holder shows that the account user complied with Part B, that fact shall be one factor the account holder may rely on in assisting the account holder to show that the account user has not contributed to the loss; or

(g) The responsible FI did not comply with any duty set out in Part C and such non-compliance caused the loss.

4.2 In respect of situation (d), the account user is presumed not to have received the authentication device, access code or unique identifier unless the responsible FI has an acknowledgement of receipt[5] from the account user, which does not include proof of delivery.

Explanation for Question 3

The intent of this measure is to standardise the situations where account holders will not be liable for losses arising from unauthorised transactions. We understand that many FIs currently provide for these arrangements in their terms and conditions of payment accounts, including those that are aligned with payment card scheme rules and the Association of Banks in Singapore's Code of Consumer Banking Practice ("**ABS Code**"). However the terms and conditions of payment accounts vary from FI to FI, among different products, and not all FIs subscribe to the ABS Code. By standardising the "no liability" situations, account users will have the assurance that they will not be

[5] For example:
(a) Card activation using SMS from a cardholder's registered mobile number with the card issuer
(b) Hardware token activation via online banking

liable for losses in the specified situations where the affected payment account is provided by FI providers of mainstream payment accounts. This improved clarity should give account users more confidence to use e-payments knowing that they are protected from unlimited liability where the loss arises from situations they are not responsible for.

Question 3. Where the account holder is not liable for any loss. MAS seeks comments on the scope of the "no liability" situations, and whether there are more situations that the Guidelines should cater for under the "no liability" category.

Account holder is liable for a maximum of S$100

4.3 Where the responsible FI is unable to show under paragraph 4.5 that any account user's recklessness was the primary cause of the loss arising from any unauthorised transaction, the account holder of that protected account is liable for an amount **no more than S$100**, unless paragraph 4.1 applies. The situations where the account holder is liable for an amount no more than S$100 may include the following where an account user's negligence contributed to the loss:

(a) misplacement of the protected account or authentication device or access code for that protected account; and

(b) where any account holder reported the unauthorised transaction to the responsible FI outside of the timeline set out in paragraph 5.8 but within a period acceptable to the responsible FI for this limited liability.

4.4 The responsible FI may require that any account holder furnish a police report in respect of any of the situations in paragraph 4.3(a) and (b) if the account holder is making a report of unauthorised transactions to the responsible FI for the third or subsequent time in any calendar year, before the responsible FI begins the claims resolution process under paragraphs 6.8 and 6.9. Upon enquiry by an account holder, the responsible FI will be expected to provide the account holder with relevant information that the responsible FI has of all the unauthorised transactions which were initiated or executed from a protected account, including transaction dates, transaction timestamps and parties to the transaction.

Explanation for Question 4

The concept of limiting the liability of the account user to a certain amount is common in many developed jurisdictions, including Australia and the United Kingdom. The ABS Code also specifies a limitation of card user's liability to S$100 where certain conditions are met. We observed that the liability cap of S$100 appears to be generally acceptable to both account users and financial institutions, and serves the purpose of containing moral hazard.

Question 4. Where the account holder's liability is capped. MAS seeks comments on the scope of the "limited liability" situations, and whether there are more situations that the Guidelines should cater for under this category. MAS also seeks views on whether the S$100 liability cap is appropriate.

Account holder is liable for actual loss

4.5 The account holder is liable for actual loss arising from an unauthorised transaction where the responsible FI shows that any account user's recklessness was the primary cause of the loss. Recklessness would include the situation where any account holder or account user deliberately did not comply with Part B. The account user is expected to provide the responsible FI with information the responsible FI reasonably requires to determine whether any account user was reckless. The actual loss that the account holder is liable for in this paragraph is capped at any applicable transaction limit or daily payment limit that the account holder and responsible FI have agreed to.

4.6 For the avoidance of doubt, where any account user knew of and consented to a transaction ("authorised transaction"), such a transaction is not an unauthorised transaction, notwithstanding that the account holder may not have consented to the transaction. This would also include the situation where any account user acts fraudulently to defraud any account holder or the responsible FI. The account holder is liable for all authorised transactions up to any applicable transaction limit or daily payment limit that the account holder and responsible FI have agreed to.

Explanation for Question 5

Where the account user has perpetuated or is the primary cause of the unauthorised transaction, the account holder should be liable for the actual loss arising from such unauthorised transactions as it would not be reasonable to ask the responsible FI to bear such losses. We also want to encourage account users to exercise due diligence in using payment accounts and not be reckless or unreasonably careless in protecting such accounts. However, the actual loss should be limited by any applicable transaction limit or daily payment limit as the account holder should be able to rely on the safety net agreed with the responsible FI.

Question 5. Where the account holder is liable for actual loss. MAS seeks comments on the scope of the "actual loss" situations, and whether there are more situations that the Guidelines should cater for under the "actual loss" category, given the intent that these Guidelines should encourage the use of e-payments.

Agreement to reduce account holder's liability

4.7 Where the account agreement specifies a lower amount for the account holder's liability in the same situations described in this Part, the responsible FI should fulfil its obligation to all account holders under the account agreement.

4.8 Where any payment account scheme rules applicable to the protected account specifies a lower amount for the account holder's liability in the same situations described in this Part, the responsible FI should fulfil its obligation to the account holder under the scheme rules.

4.9 The responsible FI may offer to reduce the liability caps specified in this Part on a case by case basis, where the responsible FI deems it to be appropriate to offer such a lower amount to the account holder.

Question 6. Liability for losses arising from unauthorised transactions. MAS seeks comments on the overall scope of this Part of the Guidelines and whether there are other significant factors that MAS should consider for this Part. MAS also

seeks comments on whether it would be appropriate for the responsible FI and account holder to go through a dispute resolution process agreed between the responsible FI and the account holder in the unlikely event that paragraphs 4.1, 4.3 and 4.5 do not apply.

Application of this Part to Joint Accounts

4.10 Where the protected account is a joint account, the liability for losses set out in this Part A apply jointly to each account holder in a joint account.

5 Part B: Duties of account holders and account users

Account holder to provide contact information and monitor notifications

5.1 The account holder should provide the responsible FI with contact details as required by the responsible FI in order for the responsible FI to send the account holder transaction notifications in accordance with Part C. Where the protected account is a joint account, the account holders should jointly give instructions to the responsible FI on whether the responsible FI should send transaction notifications under paragraph 6.3 to any or all the account holders. The duties of the account holders in this Part B will apply to all the account holders that the responsible FI has been instructed to send transaction notifications to.

5.2 The account holder should at a minimum provide the following contact information (see definition of "account contact"), which must be complete and accurate, to the responsible FI:

(a) Where the account holder has opted to receive transaction notifications by SMS, his Singapore mobile phone number; or
(b) Where the account holder has opted to receive notification by email, his email address.

5.3 It is the account holder's responsibility to monitor the transaction notifications sent to the account contact. The responsible FI may assume that the account holder will monitor such transaction notifications without further reminders or repeat notifications.

Account user to protect access codes

5.4 A 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.

5.5 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;
(b) Keeping the record in a place where the record is unlikely to be found by a third party.

Account user to protect access to protected account

5.6 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[6] to the latest version available;
(b) Patch the device's operating systems[7] 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.

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

Account holder to report unauthorised transactions

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

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

5.8 The account holder should report any unauthorised transactions to the responsible FI by the **next business day** from receipt of any transaction notification for any unauthorised transactions, or as soon as practicable if the responsible FI agrees, in any of the following ways:

(a) By reporting the unauthorised transaction in any communications channel for such purpose as set out in the account agreement;
(b) By reporting the unauthorised transaction to the responsible FI in any other way and where the responsible FI acknowledges receipt of such a report.

Account holder to provide information on unauthorised transaction

5.9 The account holder should provide the responsible FI with all the following information, as requested by the responsible FI, within **five business days** from receipt of any transaction notification for any unauthorised transaction:

(a) the protected account affected;
(b) the account holder's identification information;
(c) the type of authentication device, access code and device used to perform the payment transaction;
(d) the name or identity of any account user for the protected account;
(e) whether a protected account, authentication device, or access code was lost, stolen or misused and if so:
- the date and time of the loss or misuse,
- the date and time that the loss or misuse, was reported to the responsible FI, and
- the date, time and method that the loss or misuse, was reported to the police;

(f) where any access code is applicable to the protected account,
- how the account holder or any account user recorded the access code, and
- whether the account holder or any account user had disclosed the access code to anyone; and

(g) any other information about the unauthorised transaction that is known to the account holder.

Account holder to make police report

5.10 With reference to paragraph 4.4, the account user should make a police report if the responsible FI requests such a report to be made in accordance with paragraph 4.4.

Explanation for Question 7

To benefit from the liability caps in Part A, the account holder and any account user of the affected protected account should act in a responsible manner and assist the responsible FI in any claim investigation. We propose that account holders have a set of reporting duties for two main purposes. The first is to encourage good e-payment usage habits such as monitoring payment transaction notifications closely. The second is to enable the account holder to provide the responsible FI with all the information the responsible FI needs to process any claims and further any investigation necessary.

Question 7. Reporting duties of the account holder. MAS seeks comments on the proposed reporting duties of the account holder. In particular, we are interested to know if the reporting duties are sufficient from the point of view of the responsible FI, or if any duty is too onerous for the account holder to take on. We seek views on the respective deadlines proposed in this Part and if your view is that the deadline should be different, please explain in detail with data to support such arguments if possible. We are also interested to hear from you on whether the account holder should report by the next calendar day instead of the next business day, and whether your operations are ready to support receipt of reports every calendar day. If the next business day is a preferable deadline, please let us have your preferred definition of "business day".

Explanation for Question 8

While MAS expects all FIs to apply the technology risk management guidelines, any account user of a protected account should use and secure the protected account in a responsible manner. To educate account users on good security hygiene and habits, we have set out basic dos and don'ts of keeping the access code and protected account safe.

Question 8. Duty to protect access codes and protected accounts. MAS seeks comments on the proposed duties of the account user to protect access codes

and protected accounts. We seek views on whether any duty is too onerous for the account user, or if there are any other duties that the account user should be encouraged to take on. We also seek views on the respective deadlines proposed in this Part.

6 Part C: Duties of the responsible financial institution

Responsible FI to clearly inform account holder of user protection duties

6.1 A responsible FI should inform every account holder of a protected account of the user protection duties by:

(a) Setting out the user protection duties in the account agreement; or
(b) Obtaining the account holder's written acknowledgement of the user protection duties.

6.2 For the purpose of paragraph 6.1 user protection duties comprise:

(a) Duties of the account holder and account user as set out in Part B
(b) Duties of the responsible FI as set out in Part C, excluding this paragraph.

Responsible FI to provide transaction notifications

6.3 A responsible FI should provide transaction notifications that fulfil the following criteria to each account holder that the responsible FI has been instructed to send transaction notifications to in accordance with paragraph 5.1, in respect of all transactions made to or from the account holder's protected account ("**notifiable transaction**"):

(a) The transaction notification should be sent to the account holder's account contact. If the account holder has provided more than one account contact to the responsible FI, the transaction notification should be sent to the account contact selected by the account holder to receive such notifications.
(b) The transaction notification should be sent at least once every 24 hours during which any notifiable transaction is made. In at least one of the transaction notifications for any given day, the responsible FI must consolidate every notifiable transaction made in the past 24 hours.
(c) The transaction notification should be conveyed to the account holder by way of SMS or email. An in-app notification must be accompanied by an SMS or email notification that meets the deadline in sub-paragraph (b).
(d) The transaction notification should contain the following information:
    - Information that allows the account holder to identify the protected account such as the protected account number;

- Information that allows the account holder to identify the recipient whether by name or by other credentials such as the recipient's account number;
- Information that allows the responsible FI to later identify the account holder, the protected account, and the recipient account such as each account number or name of the account holder;
- Transaction amount;
- Transaction time and date;
- Transaction type;
- If the transaction is for goods and services provided by a business, the trading name of the merchant and where possible, the merchant's reference number for the transaction.

Responsible FI to provide recipient credential information

6.4 Where transactions are made by way of internet banking, any mobile phone application or device arranged for by a responsible FI for payment transactions, including a payment kiosk, a responsible FI should provide an onscreen opportunity for any account user of a protected account to confirm the payment transaction and recipient credentials before the responsible FI executes any authorised payment transaction.

6.5 The onscreen opportunity should contain the following information:

- Information that allows the account user to identify the protected account to be debited;
- The intended transaction amount;
- Credentials of the intended recipient that is sufficient for the account user to identify the recipient, which at the minimum should be the recipient's phone number, identification number, account number or name as registered for the purpose of receiving such payments; and
- A warning to ask the account user to check the information before executing the payment transaction.

Responsible FI to provide reporting channel

6.6 The responsible FI should provide account holders with a reporting channel for the purposes of reporting unauthorised or erroneous payment transactions.

6.7 The reporting channel should have all the following characteristics:

- The reporting channel may be a manned phone line, phone number to receive text messages, online portal to receive text messages, or a monitored email address;
- Any person who makes a report through the reporting channel should receive a written acknowledgement of his report through SMS or email;
- The responsible FI should not charge a fee to any person who makes a report through the reporting channel for the report or any service to facilitate the report; and
- The reporting channel should be available at any time every calendar day, unless it is a manned phone line, in which case that reporting channel should be available during business hours every business day.

Explanation for Question 9

To enable the account holder to monitor all payment transactions made to and from his protected account and report unauthorised or mistaken payment transactions to the responsible FI in a timely way, we propose that responsible FIs provide the account holder with adequate transaction notifications and at least one convenient and free of charge reporting channel. The account holder will be encouraged to take better care of his protected account if the transaction notifications are easy to read and access, and the reporting channel is user friendly. To this end, MAS has proposed guidelines to facilitate the standards on transaction notifications and reporting channels.

To minimise the risks of the account user making an erroneous payment transaction (i.e. paying to the wrong party), we have proposed that responsible FIs provide an onscreen opportunity for the account user to check recipient details before executing (or confirming) the payment transaction.

Question 9. Information and facilities provided by the responsible FI. MAS seeks comments on the proposed transaction notifications, recipient credential information, and reporting channel to be provided by the responsible FI.

Please let us have your views on:

(a) Whether the proposed information in the transaction notification is appropriate for the purpose of allowing the account holder to monitor payment transactions;

(b) Whether the proposed onscreen information is suitable to minimize account user's erroneous transactions;
(c) Whether the proposed characteristics of the reporting channel are suitable in general, and are suitable for your product line; and
(d) Whether the deadlines proposed are appropriate.

Responsible FI to complete claims investigation

6.8 The responsible FI should complete an investigation of any claim made by an account holder in relation to any unauthorised transaction to or from any protected account, within **21 business days** or in exceptional circumstances **45 business days**, of the account holder's report of the transaction to the responsible FI under paragraph 5.8.

6.9 The responsible FI should within the respective periods set out at paragraph 6.8 above give each account holder that the responsible FI has been instructed to send transaction notifications to in accordance with paragraph 5.1 a written or oral report of the investigation outcome and the responsible FI should obtain an acknowledgement (which need not be an agreement) from that account holder.

Responsible FI to credit protected account

6.10 The responsible FI should credit the account holder's protected account with the total loss arising from any unauthorised transaction, regardless of whether the investigation of any claim is still underway, except where the responsible FI has good reasons to believe that the account holder (or in the case of a joint account, any account holder) is primarily responsible for the loss arising from the unauthorised transaction, and has communicated its reasons to the account holder. This includes the situation where within that calendar year, the account holder has made at least two previous reports of unauthorised transactions.

Explanation for Question 10

We encourage responsible FIs to complete claims investigations within the proposed deadlines to give certainty to the account holder on the status and outcome of the claims under investigation. Where the amount lost is large, in particular, the account holder may be distressed by long investigation periods and having to bear the loss of

funds in the meantime. However, we are also mindful that this expectation may put some cost pressures on the responsible FI and it is our intent to maintain a competitive business environment in the payments space, while balancing the needs of account users. MAS views the two components of clarity of claims investigation and crediting the protected account to be important, and the standards proposed are broadly similar to that in other developed jurisdictions.

Question 10. Claims investigation and outcomes. MAS seeks comments on the proposed claims investigation process and proposal to credit the protected account while the claims investigation is ongoing. MAS seeks views on whether the deadlines proposed are appropriate and whether the exclusions from the expectation that the protected account should be credited are adequate. Please also let us know if a list of exceptional circumstances for an extended investigation should be set out in the Guidelines.

7 Part D: Specific Duties in relation to erroneous transactions

Responsible FI to make reasonable efforts to recover sums sent in error

7.1 Where an account holder has informed his responsible FI in accordance with this Part that he or an account user has initiated a payment transaction from a protected account such that money has been placed with or transferred to the wrong recipient ("**erroneous transaction**"), and the account holder's responsible FI has informed the wrongful recipient's responsible FI of the erroneous transaction, the responsible FI of both the account holder and of the wrong recipient should make reasonable efforts to recover the sum sent in error.

7.2 For the purposes of paragraph 7.1, reasonable efforts means the following:

(a) Where the responsible FI is the FI of the account holder:

- Within **two business days** of receiving the necessary information from the account holder under this Part, the responsible FI should inform the recipient FI of the erroneous transaction;
- Within **seven business days** of informing the recipient FI, the responsible FI should ask the recipient FI for the recipient's response and provide the account holder with any new relevant information to allow the account holder to assess if he should make a police report about the erroneous transaction.

(b) Where the responsible FI is the FI of the wrong recipient:

- Within **two business days** of receiving the necessary information from the account holder's FI about any erroneous transaction, the responsible FI should:

i. Inform the recipient of the erroneous transaction and all necessary information that would allow the recipient to determine if the transaction was indeed erroneous;
ii. Ask the recipient for instructions on whether to send the sum sent in error back to the account holder; and
iii. Inform the recipient that his retention or use of sums transferred to him erroneously where he has had notice of the erroneous transaction is an offence under the Penal Code.

- Within **five business days** of receiving the necessary information from the account holder's FI about any erroneous transaction, the responsible FI should

i. ask the recipient for instructions whether to send the sum sent in error back to the account holder; and

ii. inform the account holder's FI about the recipient's response, including nil responses.

Account holder to provide information on erroneous transaction

7.3 For the purposes of assisting the responsible FI to recover sums sent in error, the account holder should provide the responsible FI with any of the following information as requested by the responsible FI:

(a) all the information set out in paragraph 5.9 except limbs (e), (f) and (g);
(b) the recipient's unique identifier, including account number, identification number, name or other credentials entered by the account user; and
(c) the date, time, amount and purpose of the erroneous transaction insofar as such information is known to the account user.

Explanation for Question 11

E-payments have evolved to allow account users to pay to the recipient's identification card number or phone number. Account users are encouraged to check the recipient's credentials carefully before executing any payment transaction.

However, we are mindful that account users may not in every situation know the recipient of the erroneous transaction and may not be able to contact the recipient to inform or persuade him to return the funds received in error. This is a process that the responsible FIs are able to assist in.

At the same time, we want to encourage careful behaviour by account users, and avoid unduly burdening responsible FIs with the expectation that they need to take on police-type investigation duties to recover funds sent in error. Further, we have considered that putting the expectation on responsible FIs to conduct such investigations may not be appropriate as certain account users may abuse this service to seek return of funds that the recipient is indeed entitled to.

We clarify that if the responsible FI does not receive the necessary information from the account holder, the responsible FI is not expected to commence the error resolution process. Also, where the responsible FI is both the sending FI and recipient FI, the same timelines set out in this Part apply.

Question 11. Specific duties in relation to erroneous transactions. MAS seeks comments on the proposed duties of

- the responsible FI of the account holder,
- the responsible FI of the recipient, and
- the account holder

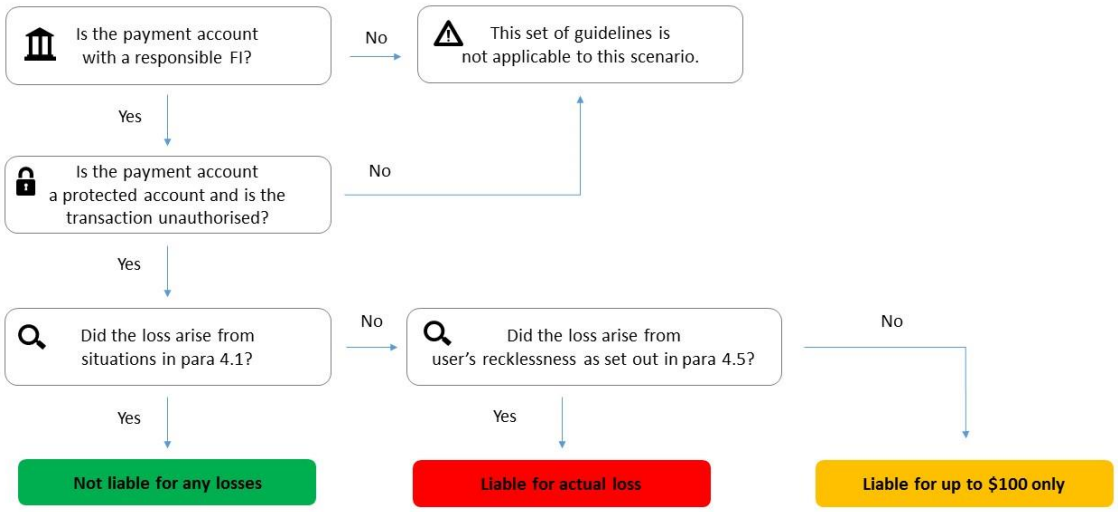
in relation to erroneous transactions. We also seek views on whether the proposed approach that responsible FIs use reasonable efforts to assist the account holder to recover sums paid to the wrong recipient is appropriate.

8 Decision trees

Decision tree for unauthorised transactions

8.1 **Illustration 1** shows a decision tree for unauthorised transactions to guide account users, account holders and responsible FIs on the expectations set out in these guidelines.

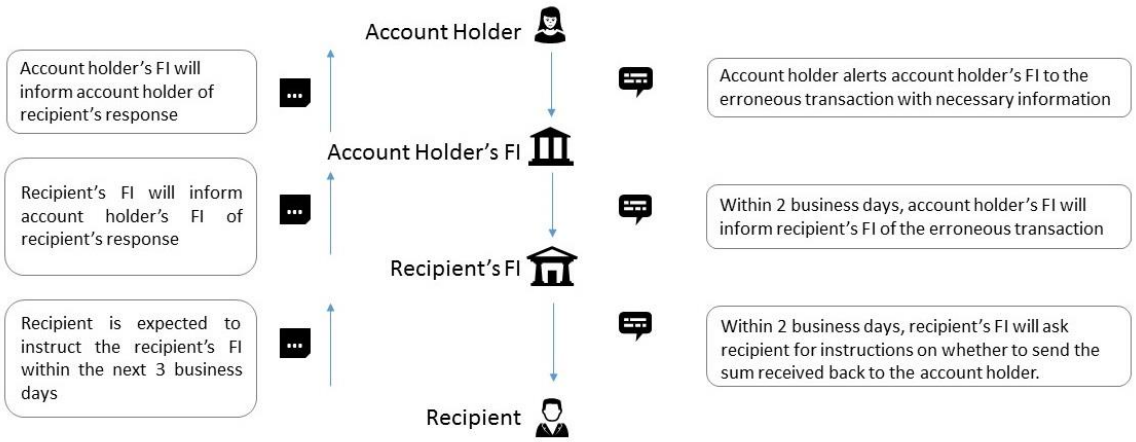
Illustration 1



Decision tree for erroneous transactions

8.2 **Illustration 2** shows a decision tree for erroneous transactions to guide account users, account holders and responsible FIs on the expectations set out in these guidelines.

Illustration 2



Explanation for Question 12

We understand that responsible FIs may wish to tap into an insurance fund to support the refunds to account holders for losses arising from unauthorised transactions that MAS expects the responsible FIs to provide. We propose to facilitate this initiative by first seeking views from the insurance industry on possible solutions that insurers may be able to offer.

Question 12. General questions regarding these Guidelines. MAS seeks comments on any aspect of the proposed Guidelines that have not been covered in earlier questions. We also seek input from the insurance industry on solutions that insurers may have to offer in respect of the unauthorised transaction claims. Where possible, please share with us relevant data such as cost to the responsible FIs and timeframe for implementation of the proposed solution.

Annex

ANNEX: LIST OF QUESTIONS

Monetary Authority of Singapore