ANNEX I-2

Monetary Authority of Singapore

E-PAYMENTS USER PROTECTION GUIDELINES

[Last updated six months after date of Act commencement]

Issue Date **: 28 September 2018**
Effective Date **: 30 June 2019** [Amended six months after date of Act commencement]

E-PAYMENTS USER PROTECTION GUIDELINES

1 Overview and Application of the guidelines

1.1 The E-Payments User Protection Guidelines (the "**Guidelines**") cover the following areas:

(a) application of the Guidelines;
(b) duties of account holders and account users;
(c) duties of the responsible financial institution;
(d) liability for losses arising from unauthorised transactions; and
(e) specific duties in relation to erroneous transactions.

1.2 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 Guidelines set out duties of users of protected accounts. Where expressly stated, certain parts of these Guidelines do not apply to any responsible FI in respect of any credit card, charge card or debit card[1] it has issued.[2] The Guidelines relating to the resolution of erroneous transactions apply to FIs in relation to any payment account where such an FI is the FI of the recipient of an erroneous transaction. The terms "protected account" and "responsible FI" are defined in these Guidelines.

1.3 The aim of these Guidelines is to establish a common baseline protection offered by responsible FIs on a business as usual basis to individuals or sole proprietors from losses arising from isolated unauthorised transactions or erroneous transactions from the protected accounts of these account holders.

[1] Debit cards in these Guidelines refer to the debit cards that the Code of Practice for Banks – Credit Cards in the Code of Consumer Banking Practice by the Association of Banks in Singapore applies to.

[2] Holders of credit cards, charge cards and debit cards issued in Singapore currently benefit from liability apportionment in the ABS Code of Practice for Banks – Credit Cards, and existing fraud prevention measures in place. As such, the liability apportionment set out in the Guidelines do not apply to transactions on credit cards, charge cards and debit cards issued in Singapore.

1.4 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.

2 Definitions

2.1 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 3.1;

[Deleted on date of Act commencement]

"**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 joint account holder and a supplementary credit card 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;

"**digital payment token"** has the same meaning given by section 2(1) of the Payment Services Act 2019;

[Amended on date of Act commencement]

"**e-money**" has the same meaning given by section 2(1) of the Payment Services Act 2019;

[Amended on date of Act commencement]

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

"**money**" includes currency and e-money but does not include digital payment tokens;

[Amended on date of Act commencement]

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

[Deleted on date of Act commencement]

"**payment account**" has the same meaning given by section 2(1) of the Payment Services Act 2019;

[Amended on date of Act commencement]

"**payment transaction**" means the placing, transfer or withdrawal of money, whether for the purpose of paying for goods or services or for any other purpose, and regardless of whether the intended recipient of the money is entitled to the money, where the placing, transfer or withdrawal of money is initiated through electronic means and where the money is received through electronic means;

[Amended on date of Act commencement]

"**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 sole proprietors;

(b) is capable of having a balance of more than S$500 (or equivalent amount expressed in any other currency) at any one time, or is a credit facility;

(c) is capable of being used for electronic payment transactions; and

(d) where issued by a relevant payment service provider is a payment account that stores specified e-money.

[Amended six months after date of Act commencement]

"**relevant exempt payment service provider"** means any exempt payment service provider under section 13(1)(a) to (d) of the Payment Services Act 2019 that provides account issuance services where each payment account issued stores e-money;

[Amended six months after date of Act commencement]

"**relevant payment service provider"** means any major payment institution as defined in section 2(1) of the Payment Services Act 2019 that has in force a licence that entitles it to carry on a business of providing account issuance services or any relevant exempt payment service provider;

[Amended six months after date of Act commencement]

"responsible FI" in relation to any protected account, means any bank, non-bank credit card issuer, finance company or relevant payment service provider that issued the protected account

[Amended six months after date of Act commencement]

"**sole proprietor**" means any business owned by an individual where the owner is personally liable for debts and losses of the business;

"**specified e-money"** has the same meaning given by section 2(1) of the Payment Services Act 2019;

[Amended six months after date of Act commencement]

"**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) any person who is a party to the payment transaction;

(b) any person's payment account;

[Amended on date of Act commencement]

[Deleted on date of Act commencement]

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

2.2 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.

3 Duties of account holders and account users

Account holder to provide contact information, opt to receive all outgoing transaction notifications and monitor notifications

[Amended on 25 April 2019]

3.1 The account holder of a protected account 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 Section 4. 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 4.4 to any or all the account holders. The duties of the account holders in this Section 3 will apply to all the account holders that the responsible FI has been instructed to send transaction notifications to.

3.2 The account holder should at a minimum provide the following contact information 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.

3.3 It is the account holder's responsibility to enable transaction notification alerts on any device used to receive transaction notifications from the responsible FI, to opt to receive all transaction notifications for all outgoing transactions of (any amount) made from the account holder's protected account, and 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.

[Amended on 25 April 2019]

Account user to protect access codes

3.4 An account user of a protected account 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.

3.5 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; and

(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

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

(a) update the device's browser[3] to the latest version available;

(b) patch the device's operating systems[4] with regular security updates provided by the operating system provider;

(c) install and maintain the latest anti-virus software on the device, where applicable; and

(d) use strong passwords, such as a mixture of letters, numbers and symbols.

3.7 An account holder should inform all account users of the security instructions or advice provided by the responsible FI to the account holder. An account user should where possible follow security instructions or advice provided by the responsible FI to the account holder.

Account holder to report unauthorised transactions

3.8 The account holder of a protected account should report any unauthorised transactions to the responsible FI as soon as practicable after receipt of any transaction notification alert for any unauthorised transaction. Where the account holder is not able to

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

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

report the unauthorised transaction to the responsible FI as soon as he receives any transaction notification alert for any unauthorised transaction, the account holder should if the responsible FI so requests, provide the responsible FI with reasons for the delayed report. This includes time periods or circumstances[5] where it would not be reasonable to expect the account holder to monitor transaction notifications.

The report should be made 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

3.9 The account holder of a protected account should within a reasonable time provide the responsible FI with any of the following information as requested by the responsible FI:

(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

[5] Examples of such time periods and circumstances are late evening to early morning, and work or travel commitments that do not allow the account holder to access his or her phone.

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

Account holder to make police report

3.10 The account holder of a protected account should make a police report if the responsible FI requests such a report to be made to facilitate its claims investigation process.

4 Duties of the responsible FI

4.1 Except for paragraph 4.4, this Section 4 does not apply to any responsible FI in respect of any credit card, charge card or and debit card issued by the responsible FI.

Responsible FI to clearly inform account holder of user protection duties

4.2 A responsible FI should inform every account holder of a protected account of the user protection duties.

4.3 For the purpose of paragraph 4.2 user protection duties comprise:

(a) duties of the account holder and account user as set out in Section 3; and
(b) duties of the responsible FI as set out in Section 4, excluding this paragraph.

Responsible FI to provide outgoing transaction notifications

4.4 Subject to paragraph 4.5, a responsible FI should provide transaction notifications that fulfil the following criteria to each account holder of a protected account that the responsible FI has been instructed to send transaction notifications to in accordance with paragraph 3.1, in respect of all outgoing transactions (of any amount) made from the account holder's protected account.

(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 every account contact selected by the account holder to receive such notifications.
(b) The transaction notification should be sent on a real time basis for each transaction or on a batched basis at least once every 24 hours to consolidate every outgoing transaction made in the past 24 hours. The responsible FI may but is not expected to send both real time notifications and daily batched notifications to the account holder.
(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, but the responsible FI may omit any confidential information provided that the information provided to the account holder still allows the account holder to

identify the transaction as being an authorised transaction (as referred to in paragraph 5.3) or unauthorised transaction.

- 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.

[Amended on 25 April 2019]

Compliance with account holder preference

4.5 Notwithstanding paragraph 4.4, a responsible FI can elect to comply with an account holder's transaction notification preferences. While the responsible FI should make available to account holders the option to receive transaction notifications for all outgoing transactions (of any amount) made from the account holder's protected account, if the account holder instructs or has instructed the responsible FI otherwise, the responsible FI may provide notifications for outgoing transactions in accordance with the account holder's instructions. For example, the responsible FI may provide outgoing transaction notifications to the account holder only for amounts higher than $0.01 or only for certain types of outgoing transactions, as instructed by the account holder.[6]

[Amended on 25 April 2019]

[6] For example, if the account holder chooses not to receive pre-authorised, first person, or recurring transaction notifications, while the responsible FI should make the option to receive these notifications available to the account holder, the responsible FI may comply with the account holder's instructions and not notify the account holder of such transactions.

4.6 A responsible FI should explain the Guidelines clearly to each account holder (whether a new or existing customer of the responsible FI) and should highlight the duties of the account holder in paragraph 3.3, explain how the liability framework in Section 5 of the Guidelines will be affected by the account holder's transaction notification preferences and how any relevant claim by an account holder (as defined in paragraph 4.12) will be resolved. The responsible FI should act fairly and responsibly to the account holder at all times.

[Amended on 25 April 2019]

Incoming transaction notifications

4.7 A responsible FI is encouraged to provide transaction notifications that fulfil the criteria set out in paragraph 4.4(a) to (d) for payments to the account holder's protected account ("incoming transaction notifications") as a matter of good practice, as incoming transaction notifications provide e-payment users with a fuller view of their e-payments.

[Amended on 25 April 2019]

Responsible FI to provide recipient credential information

4.8 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.

4.9 The onscreen opportunity should contain the following information:

(a) information that allows the account user to identify the protected account to be debited;
(b) the intended transaction amount;
(c) 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

(d) a warning to ask the account user to check the information before executing the payment transaction.

Responsible FI to provide reporting channel

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

4.11 The reporting channel should have all the following characteristics.

(a) 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.
(b) Any person who makes a report through the reporting channel should receive a written acknowledgement of his report through SMS or email.
(c) 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.
(d) 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.

Responsible FI to assess claims and complete claims investigation

4.12 A responsible FI should assess any claim made by any account holder in relation to any unauthorised transaction covered in Section 5 ("**relevant claim**") for the purposes of assessing the account holder's liability in accordance with Section 5. Where the responsible FI has assessed that the relevant claim does not fall within Section 5, the responsible FI should resolve such a claim in a fair and reasonable manner. The responsible FI should communicate the claim resolution process and assessment to the account holder in a timely and transparent manner.

4.13 The responsible FI may require that any account holder furnish a police report in respect of unauthorised transaction claim, before the responsible FI begins the claims resolution process. 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.

4.14 The responsible FI should complete an investigation of any relevant claim within 21 business days for straightforward cases or 45 business days for complex cases. Complex cases may include cases where any party to the unauthorised transaction is resident overseas or where the responsible FI has not received sufficient information from the account holder to complete the investigation. The responsible FI should within these periods give each account holder that the responsible FI has been instructed to send transaction notifications to in accordance with paragraph 3.1 a written or oral report of the investigation outcome and its assessment of the account holder's liability in accordance with Section 5. The responsible FI should seek acknowledgement (which need not be an agreement) from that account holder of the investigation report.

4.15 Where the account holder does not agree with the responsible FI's assessment of liability, or where the responsible FI's has assessed that the claim falls outside of Section 5, the account holder and the responsible FI may proceed to commence other forms of dispute resolution, including mediation at FIDReC where the responsible FI is a FIDReC member.

Responsible FI to credit protected account

4.16 The responsible FI should credit the account holder's protected account with the total loss arising from any unauthorised transaction as soon as the responsible FI has completed its investigation and assessed that the account holder is not liable for any loss arising from the unauthorised transaction. The responsible FI should disclose this arrangement to the account holder at the time the account holder reports the unauthorised transaction to the responsible FI, and inform the account holder of the timeline for completing its investigation in accordance with paragraph 4.14.

[Amended on 25 April 2019]

5 Liability for losses arising from unauthorised transactions

5.1 Section 5 does not apply to any responsible FI in respect of any credit card, charge card or debit card issued by the responsible FI.

Account holder is liable for actual loss

5.2 The account holder of a protected account is liable for actual loss arising from an unauthorised transaction where any account user's recklessness was the primary cause of the

loss. Recklessness would include the situation where any account user deliberately did not comply with Section 3. 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.

5.3 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 of a protected account 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.

Account holder is not liable for any loss

Loss resulting from any action or omission by the responsible FI

5.4 The account holder of a protected account is not liable for any loss arising from an unauthorised transaction if the loss arises from any action or omission by the responsible FI and does not arise from any failure by any account user to comply with any duty in Section 3.

5.5 Any action or omission by the responsible FI includes the following:

(a) fraud or negligence by the responsible FI, its employee, its agent or any outsourcing service provider contracted by the responsible FI to provide the responsible FI's services through the protected account;

(b) non-compliance by the responsible FI or its employee with any requirement imposed by the Authority on the responsible FI in respect of its provision of any financial service;

(c) non-compliance by the responsible FI with any duty set out in Section 4.

Loss resulting from any action or omission of any independent third party

5.6 The account holder of a protected account is not liable for any loss arising from an unauthorised transaction that does not exceed $1,000, if the loss arises from any action or omission by any third party not referred to in paragraph 5.5 and does not arise from any failure by any account user to comply with any duty in Section 3.

Agreement to reduce account holder's liability

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

5.8 The responsible FI may offer to reduce the account holder's liability specified in this Section 5 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.

Application of this section to joint accounts

5.9 Where the protected account is a joint account, the liability for losses set out in this Section 5 apply jointly to each account holder in a joint account.

6 Specific duties in relation to erroneous transactions

FIs to make reasonable efforts to recover sums sent in error by the account user

6.1 Where an account holder has informed his responsible FI in accordance with this Section 6 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 FI has informed the wrongful recipient's FI of the erroneous transaction, the FIs of both the account holder and of the wrong recipient should make reasonable efforts to recover the sum sent in error. For the purposes of this Section 6, "FI" in relation to any payment account means any bank, non-bank credit card issuer, finance company or relevant payment service provider that issued the payment account.

[Amended six months after date of Act commencement]

6.2 For the purposes of paragraph 6.1, reasonable efforts means the following:

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

- within two business days of receiving the necessary information from the account holder under this Section, the FI should inform the recipient FI of the erroneous transaction;
- within seven business days of informing the recipient FI, the 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 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 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 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.

6.3 The timeline specified above assumes that the case is straightforward. FIs are to use their best efforts to respond within the timelines specified above. The FIs may take longer to convey instructions in complex cases such as where any party to the transaction is resident overseas or where the FIs have not received sufficient information from the account holder to convey instructions within the specified timeline. For avoidance of doubt, the FIs are not expected to resolve each erroneous transaction claim but to facilitate effective communication between the account holder and the recipient with the aim to improve the account holder's chances of recovering the payment amount sent through the erroneous transaction.

Account holder to provide information on erroneous transaction

6.4 For the purposes of assisting the FI to recover sums sent in error, the account holder of a protected account 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 3.9 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.