



Monetary Authority of Singapore

E-PAYMENTS USER PROTECTION GUIDELINES

[Amendments to take effect on 16 December 2024¹]

¹ This version of the E-Payments User Protection Guidelines indicates the amendments which will take effect on 16 December 2024. It has been published in advance to facilitate implementation by the industry.

Issue Date : 28 September 2018
Effective Date : 16 December 2024 [Amended on 24 October 2024]

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;
- (e) specific duties in relation to erroneous transactions;
- (f) dispute resolution process for handling any disputed investigation; and
- (g) charges relating to transactions under dispute.

[Amended on 24 October 2024]

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 card² it has issued.³ 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.

² 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.

³ 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.

1.3 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 unauthorised transactions, or erroneous transactions from the protected accounts of these account holders.

[Amended on 24 October 2024]

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.

1.5 The revised Guidelines take effect from 16 December 2024. A longer implementation timeline will be provided for amendments to paragraphs 4.21, 6.4, 6.5, and Section 8 of these Guidelines, which will take effect on 16 June 2025.

[Amended on 24 October 2024]

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 Short Message Services (**“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).

[Amended on 24 October 2024]

“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 28 January 2020]

“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 28 January 2020]

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

[Amended on 28 January 2020]

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

“high-risk activities” include, but are not limited to—

- (a) adding of payees to the account holder’s payment profile;
- (b) increasing the transaction limits for outgoing payment transactions from the payment account;
- (c) disabling transaction notifications that the responsible FI will send upon completion of a payment transaction; and
- (d) change in the account holder’s contact information including mobile number, email address and mailing address.

[Amended on 24 October 2024]

“money” includes currency and e-money but does not include digital payment tokens;

[Amended on 28 January 2020]

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

[Deleted on 28 January 2020]

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

[Amended on 28 January 2020]

“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 28 January 2020]

“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\$1,000 (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 on 5 September 2020]

[Amended on 24 October 2024]

“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 on 5 September 2020]

“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 on 5 September 2020]

“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 on 5 September 2020]

“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 on 5 September 2020]

“transaction notification threshold” means—

- (a) the threshold for transaction alerts set by the account holder; or
- (b) if the account holder did not set any threshold for transaction alerts, the default industry-baseline transaction notification threshold.

[Amended on 24 October 2024]

“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;

[Deleted on 28 January 2020]

“unauthorised transaction”⁴ 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. This includes “seemingly authorised transactions” as defined in the Guidelines to the Shared Responsibility Framework.

[Amended on 24 October 2024]

⁴ The following are examples of payment transactions that do not fall within the scope of unauthorised transactions:

- (a) The account user knew of and intended to make the payment transaction, notwithstanding that the transaction could have arisen as a result of falling victim to a scam (e.g., e-commerce, government-official impersonation, job, investment or love scams);
- (b) The transaction was performed by a person as a result of the account holder sharing access and usage of their devices with the person, or storing the person’s biometrics identities on their devices. The account holder is deemed to have consented to the use of his account by this person.

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 information as required by the responsible FI in order for the responsible FI to send the account holder notification alerts for transactions, activation of digital security token and the conduct of high-risk activities 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 paragraphs 4.10 and 4.11 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.

[Amended on 24 October 2024]

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 notification alerts by SMS, his Singapore mobile phone number; or
- (b) where the account holder has opted to receive notification by email, his email address.

[Amended on 24 October 2024]

3.3 It is the account holder's responsibility to enable notification alerts on any device used to receive notification alerts from the responsible FI, to opt to receive notification alerts via SMS, email or in-app/push notification for all outgoing payment transactions (of any amount that is above the transaction notification threshold), activation of digital security token and the conduct of high-risk activities made from the account holder's protected account, and to monitor the notification alerts sent to the account contact. The responsible FI may assume that the account holder will monitor such notification alerts without further reminders or repeat notifications.

[Amended on 25 April 2019]

[Amended on 24 October 2024]

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, including the staff of any responsible FI;
 - (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.

[Amended on 24 October 2024]

- 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 secure 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) download the responsible FI's mobile application(s) only from official sources⁵;
 - (b) update the device's browser⁶ to the latest version available;
 - (c) patch the device's operating systems⁷ with regular security updates provided by the operating system provider;
 - (d) install and maintain the latest anti-virus software on the device, where applicable⁸;

⁵ Examples: Apple App Store, Google Play Store

⁶ Examples: Chrome, Safari, Internet Explorer, Firefox

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

⁸ Examples: periodic updates, patches, version releases initiated by the antivirus software providers from time to time

- (e) use strong passwords, such as a mixture of letters, numbers and symbols or strong authentication methods made available by the device provider such as facial recognition or fingerprint authentication methods;
- (f) not root or jailbreak the devices used; and
- (g) not download and install applications from third-party websites outside official sources (“**sideload apps**”), in particular unverified applications which request device permissions that are unrelated to their intended functionalities.

[Amended on 24 October 2024]

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 user to read content sent with access codes before completing payment transactions or high-risk activities

3.8 An account user of a protected account should read the content of the messages containing the access codes⁹ and verify that the stated recipient or activity is intended prior to completing transactions or high-risk activities.

[Amended on 24 October 2024]

Account user to refer to official sources to obtain website addresses and phone numbers

3.9 An account user of a protected account should refer to official sources, e.g., the MAS Financial Institutions Directory (“**FID**”)¹⁰, and the responsible FI’s mobile application or the back of cards, e.g. credit card, debit card or charge card (“**official sources**”) to obtain the website addresses and phone numbers (“**contact details**”) of the responsible FI.

[Amended on 24 October 2024]

⁹ Examples include one-time passwords sent via SMS or equivalent push notifications via the official mobile application of the responsible FI

¹⁰ Website link: <https://eservices.mas.gov.sg/fid>

3.10 To contact the responsible FI, an account user should use the contact details that were obtained from official sources.

[Amended on 24 October 2024]

3.11 An account user should not click on links or scan Quick Response codes ("**QR codes**") purportedly sent by the responsible FI unless he is expecting to receive information on products and services via these links or QR codes from the responsible FI. The contents of these links or QR codes should not directly result in the account holder providing any access code or performing a payment transaction or high-risk activity.¹¹

[Amended on 24 October 2024]

Account user to understand the risks and implications of performing high-risk activities

3.12 An account user of a protected account should read the risk warning messages sent by the responsible FI before proceeding to confirm the performance of high-risk activities.

[Amended on 24 October 2024]

3.13 If an account user does not understand the risks and implications of performing high-risk activities, he should access the responsible FI's website for more information on these activities or contact the responsible FI prior to performing these activities. When the account user proceeds to perform the high-risk activities, he is deemed to have understood the risks and implications as presented by the responsible FI.

[Amended on 24 October 2024]

Account holder to report unauthorised activities on his protected account

3.14 The account holder of a protected account should report any unauthorised activity to the responsible FI as soon as practicable, and no later than 30 calendar days after receipt

¹¹ Such links are only to provide information and could be part of regulatory requirements, such as Terms and Conditions, product description, steps to execute a transaction and fact sheet for investment products.

of any notification alert for any unauthorised activity, e.g., transactions, high-risk activities, and the activation of a digital security token, that has not been initiated by the account holder or with the account holder's consent.

[Amended on 24 October 2024]

3.15 Where the account holder is not able to report the unauthorised activity to the responsible FI as soon as he receives any notification alert for any unauthorised activity or within the time period set out in paragraph 3.14, the account holder should, if the responsible FI so requests, provide the responsible FI with reasons for the delayed report.

[Amended on 24 October 2024]

3.16 The report should be made in any of the following ways:

- (a) by reporting the unauthorised transaction to the responsible FI 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.

[Amended on 24 October 2024]

Account holder to activate self-service feature ("kill switch") provided by the responsible FI promptly to block further mobile and online access to the protected account

3.17 The account holder of a protected account should activate the kill switch provided by the responsible FI to block further mobile and online access to the protected account as set out in paragraph 4.14, as soon as practicable, after he is notified of any unauthorised transactions and has reason to believe that the account has been compromised, or if he is unable to contact the responsible FI.

[Amended on 24 October 2024]

Account holder to provide information on unauthorised transaction

3.18 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(s) affected, including the account holder's affected accounts with other FIs if any;
- (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 relevant information about the unauthorised transaction that is known to the account holder, such as:
 - a description of the scam incident, including details of the communications with the suspected scammer(s);
 - details of the remote software downloaded (if any) as instructed by the scammer(s);
 - whether the account holder has received any OTPs and/or transaction notifications sent by the responsible FI, and where applicable/possible a confirmation from telecommunication operators to verify the receipt status only if the account holder is able to obtain it; and
 - suspected compromised applications (if any) in the account user's device.

[Amended on 24 October 2024]

Account holder to make police report

3.19 The account holder of a protected account should make a police report as soon as practicable if the responsible FI requests such a report to be made to facilitate its claims investigation process, or if the account holder suspects that he is a victim of scam or fraud.

[Amended on 24 October 2024]

3.20 The account holder should cooperate with the Police and provide evidence¹², as far as practicable. The account holder should also furnish the police report to the responsible FI within 3 calendar days of the responsible FI's request to do so, in order to facilitate the responsible FI's claims investigation process as set out in paragraph 4.22.

[Amended on 24 October 2024]

¹² For example, consumer can furnish his mobile device to the Police for forensics investigation.

4 Duties of the responsible FI

4.1 Section 4 does not apply to any responsible FI in respect of any credit card, charge card or debit card issued by the responsible FI, except for paragraphs 4.2 to 4.6, 4.10 to 4.12, and 4.14 to 4.16.

[Amended on 24 October 2024]

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, including providing such information on its website or mobile application, and in the Terms and Conditions provided to an account holder for any new protected account issued.

[Amended on 24 October 2024]

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.

[Amended on 24 October 2024]

Responsible FI to not send clickable links or QR codes via email or SMS, or phone numbers via SMS to account user

4.4 The responsible FI should not send clickable links or QR codes via email or SMS to an account user of a retail protected account unless:

- (a) it is a link or QR code that only contains information for the account user and does not lead to a (i) website where the account user provides his access codes or performs any payment transaction or (ii) platform where the account user is able to download and install apps; and
- (b) the account user is expecting to receive the email or SMS from the responsible FI.

[Amended on 24 October 2024]

4.5 A responsible FI should not send phone numbers via an SMS to an account holder of a protected account unless the account holder is expecting to receive the SMS from the responsible FI.

[Amended on 24 October 2024]

4.6 A responsible FI should ensure its website address is listed on MAS' FID, and that its contact details reflected on MAS' FID and other official sources are up to date.

[Amended on 24 October 2024]

Responsible FI to impose a cooling off period when performing high-risk activities

4.7 A responsible FI should impose a cooling off period of at least 12 hours¹³ where high-risk activities cannot be performed ("**cooling off period**"), when a digital security token is activated on a device, or when there is a login to a protected account issued by a relevant payment service provider on a new device.

[Amended on 24 October 2024]

Responsible FI to inform account user of the risks and implications of performing high-risk activities

4.8 A responsible FI should inform the account user of a protected account of the risks and implications of performing high-risk activities and obtain additional customer confirmation, at the point before the account holders perform the high-risk activities.

[Amended on 24 October 2024]

Responsible FI to provide notification alerts on a real time basis, for activation of digital security token and conduct of high-risk activities

¹³ If the activation of the security token is via a non-straight through process (e.g. mailing of registration code), the duration of the non-straight through process counts towards fulfilling the cooling off period.

4.9 The responsible FI should provide notification alerts on a real-time basis, that fulfil the following criteria, to the account holder of a protected account, when his digital security token is activated and any high-risk activities are performed:

- (a) The notification alert should be sent to the account holder's existing account contact with the responsible FI. If the account holder has provided more than one account contact to the responsible FI, the notification should be sent to every account contact selected by the account holder to receive such notifications.
- (b) The notification alert should be conveyed to the account holder by way of SMS, email or in-app/push notification.
- (c) The notification alert should contain details relevant to the digital security token provisioning and activation or high-risk activity, such as information on the payee added, new transaction limits or a change in contact details.
- (d) The notification alert should contain a reminder for the account holder to contact the responsible FI if the digital security token provisioning and activation or high-risk activity was not performed by the account holder.

[Amended on 24 October 2024]

Responsible FI to provide outgoing transaction notification alerts on a real-time basis

4.10 Subject to paragraph 4.11, a responsible FI should provide transaction notification alerts that fulfil the following criteria to each account holder of a protected account that the responsible FI has been instructed to send transaction notification alerts to in accordance with paragraph 3.1, in respect of all outgoing payment transactions (in accordance with the transaction notification threshold) made from the account holder's protected account.

- (a) The transaction notification alert 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 alert should be sent to every account contact selected by the account holder to receive such notifications.
- (b) The transaction notification alert should be sent on a real time basis for each transaction.
- (c) The transaction notification alert should be conveyed to the account holder by way of SMS, email or in-app/push notification.
- (d) The transaction notification alert 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 (including currency);
- 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]

[Amended on 24 October 2024]

Compliance with account holder's preference

4.11 Notwithstanding paragraph 4.10, a responsible FI can elect to comply with an account holder's transaction notification alert preferences. While the responsible FI should make available to account holders the option to receive transaction notification alerts for all outgoing payment 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 should provide notification alerts for outgoing transactions in accordance with the account holder's instructions. For example, the responsible FI may provide outgoing transaction notification alerts to the account holder for amounts higher than \$0.01 or only for certain types of outgoing transactions, as instructed by the account holder.¹⁴

¹⁴ 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.

[Amended on 25 April 2019]
[Amended on 24 October 2024]

4.12 A responsible FI should make available on its website or mobile application information on how an account holder can adjust the transaction notification settings. The responsible FI should explain how the liability of the account holder under Section 5 of the Guidelines may be affected by the account holder's transaction notification preferences and how any relevant claim by an account holder (as defined in paragraph 4.22) will be resolved. The responsible FI should act fairly and responsibly to the account holder at all times.

[Amended on 25 April 2019]
[Amended on 24 October 2024]

Incoming transaction notification alerts

4.13 A responsible FI is encouraged to provide transaction notification alerts that fulfil the criteria set out in paragraph 4.10(a) to (d) for payments to the account holder's protected account ("incoming transaction notifications") as a matter of good practice, as incoming transaction notification alerts provide e-payment users with a fuller view of their e-payments.

[Amended on 25 April 2019]
[Amended on 24 October 2024]

Responsible FI to provide a self-service feature ("**kill switch**") for account holder to promptly block further access to protected account

4.14 A responsible FI should provide a kill switch for an account holder to promptly block further mobile and online access to his protected account¹⁵. This includes disallowing mobile and online payment transfers to third parties who are not authorised billers¹⁶. The kill switch should be made available in a prominent manner via the mobile application of the responsible FI, the automated teller machines ("**ATMs**") of the responsible FI, or the reporting channel provided by the responsible FI under paragraph 4.19 to report unauthorised transactions.

¹⁵ Existing mobile and online banking session(s) are to be terminated as well.

¹⁶ Examples of payment transfers to authorised billers include pre-authorised transfers such as GIRO payments to billing organisations.

[Amended on 24 October 2024]

4.15 A responsible FI should educate every account holder of a protected account how to activate this feature, and highlight the duties of the account holder in paragraph 3.17 on when they should activate this feature.

[Amended on 24 October 2024]

Responsible FI to provide information to allow identification of payment recipient

4.16 A responsible FI should provide the following information accompanying the access codes¹⁷ in the same message sent to the account user to allow the account user of a protected account to identify payment recipient:

- (a) information that allows the account user to identify the protected account such as the protected account number;
- (b) information that allows the account user to identify the recipient whether by name or by other credentials;
- (c) the intended transaction amount (including currency); and
- (d) a warning to remind the account user not to reveal the access code to anyone.

[Amended on 24 October 2024]

Responsible FI to provide recipient credential information

4.17 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.

4.18 The onscreen opportunity should contain the following information:

- (a) information that allows the account user to identify the protected account to be debited;

¹⁷ Examples include one-time passwords (OTP) sent via SMS or equivalent push notifications via the official mobile application of the responsible FI

- (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

4.19 The responsible FI should provide account holders of protected accounts with a reporting channel that is available at all times for the purposes of reporting unauthorised or erroneous transactions, and blocking further access via mobile and online channels to his protected account.

[Amended on 24 October 2024]

4.20 The reporting channel should have all the following characteristics:

- (a) The reporting channel¹⁸ may be a manned phone line, phone number to which text messages can be sent, online portal to which text messages can be sent, a monitored email address, mobile application of the responsible FI, or the ATMs of the responsible FI.
- (b) Any person who makes a report through the reporting channel should receive a written acknowledgement of his report through SMS, email, or in-app notification.
- (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.

[Amended on 24 October 2024]

¹⁸ Account holders may also choose to report unauthorised or erroneous transactions in person at the operating premises of the responsible FI where practicable, subject to their operating hours.

Responsible FI to implement real-time detection and blocking of suspected unauthorised transactions

4.21 A responsible FI should have in place capabilities to detect and block suspected unauthorised transactions at all times. A responsible FI should also have capabilities to inquire into the authenticity of the suspected unauthorised transactions before allowing such transactions to be executed. A responsible FI should review the effectiveness of its detection parameters for suspected unauthorised transactions on an annual basis, or as and when there are material triggers.

[Amended on 24 October 2024]

Responsible FI to assess claims and complete claims investigation

4.22 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. It should have a proper governance structure and investigation process, involving representatives who are independent from business units who are to carry out the above assessment.

[Amended on 24 October 2024]

4.23 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.

[Amended on 24 October 2024]

4.24 The responsible FI may require that any account holder furnish a police report in respect of an unauthorised transaction claim, before the responsible FI begins the claims resolution process. In doing so, the responsible FI should, upon request by the account holder, provide information on the procedure to file a police report.

[Amended on 24 October 2024]

4.25 The responsible FI may request any account holder to provide information set out in paragraph 3.18. 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.

[Amended on 24 October 2024]

4.26 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.

4.27 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 the Financial Industry Disputes Resolution Centre Ltd ("FIDReC") where the responsible FI is a FIDReC member.

Responsible FI to credit protected account

4.28 The responsible FI should credit the account holder's protected account with the total loss arising from any unauthorised transaction¹⁹ 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 4.26.

[Amended on 25 April 2019]

[Amended on 24 October 2024]

¹⁹ For the avoidance of doubt, losses arising from unauthorised transactions exclude any loss of business or profit, special, punitive, indirect or consequential loss and any other losses.

Scheduled system downtime

4.29 Where relevant, paragraphs 4.2, 4.7, 4.9, 4.10, 4.13, 4.14, 4.19 and 4.21 shall apply during a scheduled system downtime. The responsible FI is to ensure continued delivery of key services and alternatives, where applicable. The responsible FI should also ensure that scheduled system downtime is not performed during periods where high volume of transactions are expected.

[Amended on 24 October 2024]

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 recklessness²⁰ 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.

[Amended on 24 October 2024]

5.3 For the avoidance of doubt, where any account user knew of and consented to a transaction ("**authorised transaction** ²¹"), 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

²⁰ Examples of conduct that constitute recklessness and could lead to losses from unauthorised transactions include:

- a) storing access code in a manner that can be easily accessed by any third party;
- b) knowingly sharing or surrendering access codes to non-account users, resulting in completed transactions;
- c) ignoring notifications, alerts or warnings from the responsible FI;
- d) following instructions of third parties to open new bank or card accounts without a reasonable basis;
- e) retaining sideloaded apps which are unverified or request device permissions that are unrelated to their intended functionalities; and
- f) selecting a numeric or alphabetical access code that is easily recognisable, such as one which represents their birth date, or part of their name, if the responsible FI has:
 - specifically instructed the account holder not to do so, and
 - warned the account holder of the consequences of doing so.

²¹ Please refer to footnote 4 for examples of authorised transactions.

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.

[Amended on 24 October 2024]

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 the first \$1,000 of loss arising from an unauthorised transaction, 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.

[Amended on 24 October 2024]

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

6.1 Section 6 applies where an account holder or his account user initiates a payment transaction that is not a credit card, charge card or debit card transaction from a protected account, such that money has been placed with or transferred to a wrong recipient (“erroneous transaction”).

[Amended on 24 October 2024]

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

Where the account holder or account user has initiated an erroneous transaction and requests to recover the funds

6.2 Where an account holder has informed his responsible FI in accordance with this Section 6 that he or an account user has initiated an erroneous transaction, and the account holder’s FI has informed the wrong 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 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 on 5 September 2020]

[Amended on 24 October 2024]

6.3 For the purposes of paragraph 6.2, 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 wrong recipient’s FI of the erroneous transaction;
 - within seven business days of informing the recipient’s FI, the FI should ask the wrong recipient’s FI for the recipient’s response (if not already provided) and provide the account holder with an update to allow the account holder to assess if he should make a police report about the erroneous transaction;
 - in the event that the account holder is unable to recover the erroneously transferred funds despite the FI expending all reasonable efforts to do so, and the FI assessed that the case to be closed as a result, the FI should

inform the sender of the decision and advise the sender on the next steps, which may include filing a police report.

(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.

[Amended on 24 October 2024]

Where the wrong recipient has noticed an erroneous transaction and requests to return the sum sent in error

6.4 Where a recipient has informed his responsible FI in accordance with Section 6 that he has received an erroneous transaction and wishes to return the sum sent in error, the recipient's FI should make reasonable efforts to assist the recipient in doing so. Where confirmation is required from the account holder (who had made the erroneous transaction) through the account holder's FI, before the recipient's FI can return the sum sent in error, the FI of the account holder should also make reasonable efforts to facilitate the return of such sum.

[Amended on 24 October 2024]

6.5 For the purposes of paragraph 6.4, reasonable efforts means the following:

(a) Where the FI is the FI of the wrong recipient:

- if confirmation from the account holder's FI is needed before the FI can return the sum sent in error, the FI should:
 - i. within two business days of receiving the necessary information from the wrong recipient under this Section, inform the account holder's FI of the erroneous transaction; and
 - ii. within seven business days of informing the account holder's FI, ask the account holder's FI for a response (if not already provided) and provide the wrong recipient with an update. If the FI is unable to return the sum sent in error, the FI should advise the wrong recipient on the next steps to be taken.
 - if confirmation from the account holder's FI is not needed before the FI can return the sum sent in error, the FI should:
 - i. return the sum sent in error as soon as practicable, or no later than nine business days of receiving the necessary information from the recipient under this Section, and provide the wrong recipient with an update.
 - in the event that the FI is unable to obtain confirmation from the account holder's FI, and the FI assessed that the case to be closed as a result, the FI should inform the wrong recipient of the decision and advise the sender on the next steps, which may include making a police report if he suspects that the funds transferred by the sender are illicit in nature.
- (b) Where the FI is the FI of the account holder, and confirmation from the FI is needed before the wrong recipient's FI can return the sum sent in error, the FI should, within five business days of receiving the necessary information from the wrong recipient's FI about any erroneous transaction, provide the wrong recipient's FI with a response.

[Amended on 24 October 2024]

6.6 The timelines specified above assume 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.

[Amended on 24 October 2024]

Account holder or recipient to provide information on erroneous transaction

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

- (a) all the information set out in paragraph 3.18 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.

[Amended on 24 October 2024]

6.8 For the purposes of assisting the recipient's FI to return sums sent in error, the recipient should provide his FI with any of the following information as requested by the FI:

- (a) the protected account(s) to which the erroneous transactions have been made;
- (b) the date, time and amount of the erroneous transaction insofar as such information is known to the recipient; and
- (c) any other relevant information about the erroneous transaction that is known to the recipient.

[Amended on 24 October 2024]

7 Dispute resolution process for handling any disputed investigation

7.1 This section applies when the account holder does not agree with the investigation outcome of the relevant claim, set out in paragraphs 4.22 to 4.27, by the responsible FI (“**disputed investigation**”).

[Amended on 24 October 2024]

Responsible FI to have in place a dispute resolution process

7.2 The responsible FI should have a dispute resolution process for handling any disputed investigation.

[Amended on 24 October 2024]

Responsible FI to provide channels for account holders to notify the responsible FI

7.3 The responsible FI should provide account holders of protected accounts with a channel to raise the disputed investigation. The channel could take the form of, but not limited to:

- (a) a manned phone hotline or physical branch;
- (b) the responsible FI’s mobile application; or
- (c) the customer support chat function on the responsible FI’s website.

[Amended on 24 October 2024]

Reasonable request for evidence by the responsible FI to facilitate investigations

7.4 The responsible FI may request information from the account user such as records of correspondences²² to facilitate the investigation of the disputed investigation.

[Amended on 24 October 2024]

²² Examples include email or SMS logs from the telecommunication service provider if the account user is able to obtain it or screen shots of the correspondence or SMS received on the account user’s mobile phone.

Responsible FI to promptly assess and investigate the disputed investigation

7.5 The responsible FI should assess and complete an investigation of any disputed investigation raised by an account holder within 21 business days or where there are exceptional circumstances²³, within 45 business days of receipt of the disputed investigation.

[Amended on 24 October 2024]

7.6 The responsible FI should first assess if there are any grounds for further investigation to be made on the disputed investigation.

- (a) Where the responsible FI has assessed that there are no grounds for further investigation to be carried out on the disputed investigation, the responsible FI should communicate the reasons why no further investigation would be carried out to the account holder in accordance with paragraph 7.7.
- (b) Where the responsible FI has assessed that there are grounds for further investigation to be carried out on the disputed investigation, the responsible FI should complete the investigation and inform the account holder of the investigation outcome in accordance with paragraph 7.7.
- (c) Where the responsible FI needs to extend the investigation period beyond 21 business days due to exceptional circumstances, the responsible FI should inform the account holder of the need for additional time to complete its investigation.

[Amended on 24 October 2024]

7.7 The responsible FI should within the time periods set out in paragraph 7.5 give each account holder that notified the responsible FI of the disputed investigation, a written or oral report of the outcome of the assessment and investigation of the disputed investigation that includes the following information:

- (a) the outcome of the assessment and investigation of the disputed investigation;

²³ Exceptional circumstances may include delays caused by other external parties involved in resolving the dispute.

- (b) the reasons for the outcome, including the assessment of the account holder's liability based on the relevant considerations under Section 5. This could include how the account user may have been reckless or have not complied with any duty set out in Section 3;
- (c) instructions for the account holder to pursue the matter further if the account holder does not agree with the assessment and investigation outcome, including the availability of dispute resolution by FIDReC;
- (d) FIDReC's contact information²⁴.

[Amended on 24 October 2024]

7.8 Paragraphs 7.5 and 7.6 does not apply if the disputed investigation relates to a transaction performed on a credit card, charge card or debit card issued by the responsible FI, and the responsible FI exercises its rights to resolve the dispute under the rules of the card scheme.

[Amended on 24 October 2024]

²⁴ For complainants: info@fidrec.com.sg; For feedback: feedback@fidrec.com.sg, Address:

36 Robinson Road, #15-01 City House Singapore 068877; Tel: (65) 6327 8878; Fax: (65) 6327 8488/ (65) 6327 1089.

8 Charges relating to transactions under dispute

Responsible FI to withhold and/or waive charges relating to transactions under dispute

8.1 Where an account holder reports a suspected unauthorised transaction (“**disputed transaction**”), the responsible FI should withhold and/or waive the requirement for the account holder to settle the outstanding amount of the disputed transaction and the charges²⁵ directly relating to the disputed transaction until the responsible FI completes its investigation of the disputed transaction.

[Amended on 24 October 2024]

8.2 Where the responsible FI has assessed that the disputed transaction is an authorised transaction or an unauthorised transaction for which the account holder is liable, and the account holder does not agree with the assessment²⁶, the responsible FI should withhold and/or waive the requirement for the account holder to settle the outstanding amount of that transaction and the charges directly relating to that transaction during the following periods:

- (a) from the date the responsible FI completes its investigation up to 30 calendar days after the responsible FI informs the account holder of the investigation outcome. This is in recognition that the account holder may not agree with the responsible FI’s assessment of the account holder’s liability of the unauthorised transaction in accordance with Section 5 and intends to commence dispute resolution with FIDReC.
- (b) from the date when the responsible FI is aware that the consumer has commenced dispute resolution with FIDReC up to the completion of mediation and/or adjudication by FIDReC or when the case is closed by FIDReC due to prolonged inactivity.

²⁵ Examples of charges directly relating to the disputed transaction include late payment fee, fall-below-balance service fee, telegraphic transfer commission, fees and charges facilitating the movement of funds during the responsible FI’s investigation of the disputed transaction and charges which are not within the FI’s control such as agent fee and cable charge for telegraphic transfer.

²⁶ For avoidance of doubt, where the disputed transactions are transactions that do not fall within the scope of unauthorised transactions as set out in footnote 4, the responsible FIs are not obligated to withhold and/or waive the requirement for the account holder to settle the outstanding amount of the disputed transaction and the charges directly relating to that transaction during the time periods set out in paragraph 8.2.

[Amended on 24 October 2024]

Responsible FI to withhold the reporting of the non-payment of disputed transactions to licensed credit bureaus

8.3 Where the disputed transaction is made using credit cards or other unsecured credit facilities, the responsible FI should ensure that the account holder's credit records with licensed credit bureaus are not adversely affected due to the disputed transaction:

- (a) until the responsible FI completes its investigation of the disputed transaction; or
- (b) in the event where the non-payment of the disputed transaction had already been reported to licensed credit bureaus, after the responsible FI completes its investigation of the disputed transaction and the account holder was found to be not liable for the disputed transaction.

[Amended on 24 October 2024]

8.4 Where the responsible FI has assessed that the disputed transaction is an authorised transaction or an unauthorised transaction for which the account holder is liable, and the account holder does not agree with the assessment²⁷, and the transaction is made using credit cards or other unsecured credit facilities, the responsible FI should ensure that the account holder's credit records with licensed credit bureaus are not adversely affected due to that transaction during the following periods:

- (a) from the date the responsible FI completes its investigation up to 30 calendar days after the responsible FI informs the account holder of the investigation outcome; and
- (b) in the event where the consumer has commenced dispute resolution with FIDReC, after the completion of mediation and/or adjudication by FIDReC or when the case is closed by FIDReC due to prolonged inactivity.

[Amended on 24 October 2024]

²⁷ For avoidance of doubt, where the disputed transactions are transactions do not fall within the scope of unauthorised transactions as set out in footnote 4, the responsible FIs are not obligated to ensure that the account holder's credit records with licensed credit bureaus are not adversely affected due to the transaction during the time periods set out in paragraph 8.4.

8.5 After the time periods set out in paragraph 8.2 and 8.4, the responsible FI may resume the reporting of any unpaid outstanding amounts for the disputed transaction to licensed credit bureaus if the account holder has not repaid the amount due 7 calendar days from the date of the responsible FI's request.

[Amended on 24 October 2024]

Responsible FI to disclose charges relating to recovery of unauthorised transactions

8.6 Where there are any charges or costs relating to the recovery of the unauthorised transaction amount (such as agent fee, arbitration charge, foreign exchange rate differences, professional fee) to be borne by the account holder, the responsible FI should disclose such charges to the account holder.

[Amended on 24 October 2024]