# GUIDELINES ON SHARED RESPONSIBILITY FRAMEWORK

**Issue Date : 24 October 2024**
**Effective Date : 16 December 2024**

## GUIDELINES ON SHARED RESPONSIBILITY FRAMEWORK

### 1 Overview and Application of the Guidelines

1.1 The Guidelines on Shared Responsibility Framework (the "**Guidelines**") apply to:

(a) banks and relevant payment service providers that have issued a protected account ("**responsible financial institutions**" or "**responsible FIs**"); and

(b) mobile network operators under the Telecommunications Act 1999 which provide cellular mobile telephone services ("**responsible telecommunications companies**" or "**responsible Telcos**").

1.2 These Guidelines clarify the roles and accountabilities of account users[1], responsible FIs and responsible Telcos in mitigating the risk of seemingly authorised transactions. Specifically, these Guidelines set out:

(a) the expectations of the Monetary Authority of Singapore (the "**MAS**") of responsible FIs in relation to responsible FIs' duties to mitigate the risk of seemingly authorised transactions, as well as duties of account users; and

(b) the expectations of the Infocomm Media Development Authority of Singapore (the "**IMDA**") of responsible Telcos in relation to responsible Telcos' duties to mitigate the risk of subscribers receiving SMS which facilitate seemingly authorised transactions.

1.3 These Guidelines also clarify the allocation of responsibility for losses arising from seemingly authorised transactions under the Shared Responsibility Framework ("**SRF**"), and the operational workflow for reporting a seemingly authorised transaction by an account user.

[1] 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 responsibility sharing set out in these Guidelines do not apply to transactions on credit cards, charge cards and debit cards issued in Singapore.

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

## 2 Definitions

2.1 For the purposes of these Guidelines:

"**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 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;

"**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;

"**bank**" has the same meaning as in section 2(1) of the Banking Act 1970;

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

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

"**fabricated digital platform**" means platforms that resemble legitimate digital platforms operated by an FI or the impersonated entity, or any party related to the FI or impersonated entity;

"**high-risk activities**" means—

(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) changes in the account holder's contact information including mobile number, email address and mailing address;

"**legitimate business or government entity**" means Singapore Government agencies and entities incorporated in Singapore; or entities incorporated outside Singapore that offer services to Singapore residents;

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

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

"**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;

"**protected account**[2]" means any payment account that—

(a) is held in the name of one or more persons, all of whom are individuals;

(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;

"**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;

[2] This refers to an account that is opened with the retail business unit of the responsible FI, or cannot be used for transactions in the course of business.

"**responsible FI**" in relation to any protected account, means any bank or relevant payment service provider that issued the protected account;

**"responsible Telco"** refers to Mobile Network Operators ("**MNOs**") in Singapore who deploy, own or control cellular mobile network infrastructure and have been given the right to use radio spectrum, to provide telecommunication services to end users;

**"seemingly authorised transaction"** in relation to any protected account, means any payment transaction which fulfils limbs (a) to (d)—

(a) perpetrated through the impersonation of a legitimate business or government entity, e.g., FIs, non-banks and government agencies ("**impersonated entity**");

(b) the scammer, pretending to be the impersonated entity, uses a digital messaging platform (e.g., SMS, email, WhatsApp, social media platforms) to obtain the account user's account credentials[3];

(c) the account user enters his account credentials on a fabricated digital platform (e.g., website, application) ("**fraudulently obtained credentials**"); and

(d) the fraudulently obtained credentials are used to perform transactions that the account user did not intend to be performed;

**"SMS"** means a text message sent using an electronic service to an end-user on a mobile telephone through a telecommunication service, and excludes text messages sent over social media platforms and those that rely on Over-The-Top ("**OTT**") applications such as WhatsApp, iMessage, and Rich Communication Services ("**RCS**");

**"Sender ID SMS"** means an SMS with an alphanumeric sender identification;

**"subscriber"**, in relation to a responsible Telco, means—

(a) a subscriber of telecommunication services provided by the responsible Telco; or

(b) any other person who is authorised in a manner to use the telecommunication services referred to in limb (a) in accordance with the responsible Telco's terms and conditions of use.

[3] This includes an access code as defined under the EUPG, and the user identification (user ID).

"**telecommunication service**" has the meaning given by section 2 of the Telecommunications Act 1999.

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 users

3.1 The duties of the account user as set out in Section 3 of the E-Payments User Protection Guidelines [4] ("**EUPG**") would apply accordingly. Account users should take necessary precautions, such as practising good cyber hygiene and never giving away their personal or account credentials to anyone. Specific to seemingly authorised transactions, account users should only refer to official sources for information on the website addresses and phone numbers of their responsible FIs (e.g., MAS' Financial Institutions Directory and on the back of ATM/credit/debit cards). In addition, account users should not click on links provided in SMS or emails, unless these are informational links that the account user is expecting to receive from the responsible FI. Such practices will reduce the risk of the account user falling for seemingly authorised transactions.

## 4 Duties of the responsible FI

4.1 Responsible FIs' duties set out in Section 4 of these Guidelines are drawn from Section 4 of the EUPG. Responsible FIs are expected to adhere to all the duties set out under Section 4 of the EUPG.

4.2 The following duties from the EUPG are assessed under Section 6 of these Guidelines in determining whether the responsible FI should bear losses in the context of a seemingly authorised transaction:

4.2.1 [*From paragraph 4.7 of the EUPG*] The responsible FI imposes a 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

[4] https://www.mas.gov.sg/regulation/guidelines/guidelines-for-e-payments-user-protection

device: the responsible FI must impose a cooling off period of at least 12 hours[5] where high-risk activities cannot be performed, 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.

4.2.2 [*From paragraph 4.9 of the EUPG*] The responsible FI provides notification alerts on a real-time basis, when a digital security token is activated or when there is a login to a protected account issued by a relevant payment service provider on a new device, and for the conduct of high-risk activities: the responsible FI must provide notification alerts on a real-time basis to the account holder of a protected account, when (i) his digital security token is activated; (ii) there is a login to a protected account issued by a relevant payment service provider on a new device; or (iii) any high-risk activities are performed on a protected account.

4.2.3 [*From paragraph 4.10 of the EUPG*] The responsible FI provides outgoing transaction notification alerts on a real-time basis: the responsible FI must provide transaction notification alerts to each account holder of a protected account that the responsible FI has been instructed to send transaction notification alerts to[6], in respect of all outgoing payment transactions[7] made from the account holder's protected account.

4.2.4 [*From paragraphs 4.14 and 4.19 of the EUPG*] The responsible FI provides a reporting channel and self-service feature for the account holder to promptly block further access to the protected account: the responsible FI must provide account holders of protected accounts with a reporting channel that is available at all times for the purposes of prompt reporting and blocking of further seemingly authorised transactions. The reporting channel must include a self-service feature to promptly block further mobile and online access to the account holder's protected account.

---

[5] If the security token is activated 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.

[6] In accordance with paragraph 3.1 of the EUPG.

[7] In line with the default industry-baseline transaction notification threshold or threshold for transaction alerts set by the account holder.

4.2.5 [*From paragraph 4.21 of the EUPG*] The responsible FI puts in place real-time fraud surveillance directed at detecting unauthorised transactions in a phishing scam: the responsible FI must have in place real-time fraud surveillance directed at detecting seemingly authorised transactions to a scammer(s). In a scenario where a protected account is rapidly drained of a material sum[8] to a scammer, the responsible FI must:

(a) Block the online banking payment transaction that would result in the crossing of the threshold set out in footnote 8, and all subsequent online banking payment transactions to the scammer until it is able to obtain further verification from the account holder; or

(b) Send notification to the account holder, and block or hold for at least 24 hours: (i) the online banking payment transaction that would result in the crossing of the threshold set out in footnote 8; and (ii) all subsequent online banking payment transactions to the scammer.

4.3 Where relevant, paragraph 4.2 of these Guidelines applies 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 a high volume of transaction is expected.

4.4 Paragraph 4.2.5 will take effect 6 months from the date these Guidelines are effective.

## 5 Duties of the responsible Telco

5.1 Responsible Telcos' duties are a specific subset of IMDA's directions to Telcos under section 31 of the Telecommunications Act 1999 ("**IMDA's Directions**"). For the avoidance of doubt, IMDA's Directions will prevail if there is any inconsistency between the duties as set out in these Guidelines and IMDA's Directions.

---

[8] A protected account is considered to be rapidly drained of a material sum if (a) the protected account has account balance of S$50,000 or more immediately prior to the seemingly authorised transaction and (b) more than 50% of such account balance is transferred out within the last 24 hours. For the avoidance of doubt, this excludes recurring standing instructions, recurring GIRO/eGIRO deductions, bill payments to billing organisations maintained by the responsible FI (save for payment of bills for credits cards issued by other FIs), debit card transactions, and intrabank transfers to the account holder's other account(s) within the responsible FI.

5.2 The following duties from IMDA's Directions are assessed under Section 6 of these Guidelines to determine whether the responsible Telco should bear losses in the context of a seemingly authorised transaction –

5.2.1 Responsible Telco connects only to authorised aggregators for delivery of Sender ID SMS: The responsible Telco must deliver Sender ID SMS to subscribers only if it is received from authorised aggregators[9].

5.2.2 Responsible Telco blocks Sender ID SMS which are not from authorised aggregators: The responsible Telco must block Sender ID SMS which are received from sources other than authorised aggregators.

5.2.3 Responsible Telco implements an anti-scam filter over SMS to block SMS containing malicious URLs in designated database: The responsible Telco must implement an anti-scam filter for all SMS that pass through the responsible Telcos' network, to determine if it contains any URL that matches that of a known malicious URL in a designated database[10]. The requirement covers both Sender ID SMS and SMS carrying either local or overseas telephone numbers, and applies regardless of whether the SMS originates locally or from overseas.

## 6 Responsibility for losses arising from seemingly authorised transactions

<u>Loss sharing for seemingly authorised transactions</u>

6.1 For the purposes of assessing whether the responsible FI, responsible Telco or the account holder should bear losses[11], the responsible FI should consider whether it has fulfilled the duties set out in paragraph 4.2 of these Guidelines, and the responsible Telco should consider whether it has fulfilled the duties set out in paragraph 5.2 of these Guidelines.

---

[9] Authorised aggregators are licensed by IMDA to send SMS that bears a Sender ID with an alphanumeric sender ID, or a short code registered with the Singapore SMS Sender ID Registry. The list of authorised aggregators can be found on SGNIC's website at https://sgnic.sg/smsregistry/list-of-participating-aggregators.

[10] Scam types are constantly evolving, and new malicious URLs can emerge rapidly. Members of the public are reminded to remain vigilant and avoid clicking on suspicious links, especially from unknown sources, to significantly reduce the risk of falling victim to scams.

[11] 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.

6.2 The responsible FI is expected to bear any loss arising from a seemingly authorised transaction if the loss arises from any non-compliance by the responsible FI with any duty set out in paragraph 4.2 of these Guidelines.

6.3 Notwithstanding paragraph 6.2 of these Guidelines, the responsible FI will be responsible for losses arising from a seemingly authorised transaction if the loss arises from any action or omission by the responsible FI as defined in paragraphs 5.5(a) and 5.5(b) of the EUPG[12].

6.4 The responsible Telco is expected to bear losses arising from a seemingly authorised transaction perpetrated through SMS if:

(a) the responsible FI has complied with all of its duties set out in paragraph 4.2 of these Guidelines; and

(b) the loss arises from the responsible Telco's non-compliance with any duty set out in paragraph 5.2 of these Guidelines.

6.5 For avoidance of doubt, where the responsible FI is expected to bear the loss under paragraph 6.2 of these Guidelines, the responsible FI will do so notwithstanding that the responsible Telco may have also failed to comply with its duties set out in paragraph 5.2 of these Guidelines.

6.6 In cases where the responsible Telco's subscriber is not the same as the account holder, the responsible Telco is expected to bear the loss under paragraph 6.4 of these Guidelines if:

(a) the subscriber's mobile number is designated to receive SMS notifications pertaining to the protected account; and

(b) the subscriber's mobile number which received the phishing SMS led to the seemingly authorised transaction perpetrated through SMS.

---

[12] Paragraph 5.5(a) and 5.5(b) of the EUPG states that 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 MAS on the responsible FI in respect of its provision of any financial service.

6.7 Where the responsible FI is not expected to bear the loss under paragraph 6.2 of these Guidelines, and the responsible Telco is not expected to bear the loss under paragraph 6.4 of these Guidelines, the account holder of a protected account should bear any loss arising from a seemingly authorised transaction.

6.8 Notwithstanding paragraph 6.7 of these Guidelines where the account holder is deemed responsible, the account holder may seek alternative channels for redress as explained in Section 7.

Application of this section to joint accounts

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

## 7 Operational workflow

Overview

7.1 For the purposes of processing claims in respect of any seemingly authorised transaction, the account holder, responsible FI and responsible Telco (where applicable)[13] should adhere to the following four-stage workflow:

(a) Claim Stage

7.1.1 A responsible FI is the first and overall point of contact with the account holder. It will assess if the claim falls within the SRF's scope ("**relevant claim**"), and inform a responsible Telco where applicable.

(b) Investigation Stage

7.1.2 A responsible FI and responsible Telco (where applicable) will conduct the investigation in the manner described in paragraphs 7.2 to 7.8 of these Guidelines.

[13] A responsible Telco's involvement in the operational workflow in paragraph 7.1.3 of these Guidelines shall be based on any mutually agreed arrangement between the responsible FI and responsible Telco.

(c) Outcome Stage

7.1.3 A responsible FI will inform the account holder of the investigation outcome.

(d) Recourse Stage

7.1.4 Where an account holder is dissatisfied with the outcome at the Outcome Stage, he may pursue further action through avenues of recourse such as the Financial Industry Disputes Resolution Centre Ltd ("**FIDReC**") or IMDA.

7.2 A responsible FI should explain the operational workflow to the account holder under paragraph 7.1 of these Guidelines at the time the account holder reports the seemingly authorised transaction to the responsible FI, and inform the account holder of the timeline for investigation in accordance with paragraph 7.7 of these Guidelines.

Claim Stage

7.3 The account holder should report any unauthorised activity to the responsible FI as soon as practicable, and no later than 30 calendar days from when the responsible FI sends the notification alerts[14]. The account holder must furnish a valid email address, and any other supporting information such as a police report and digital communication trail(s), within 3 calendar days from the date of notification of the seemingly authorised transaction to the responsible FI, in order to facilitate the claims investigation process. In doing so, the responsible FI should, upon request by the account holder, provide information on the procedure to file a police report.

7.4 The responsible FI may request for the account holder to provide information set out in paragraph 3.18 of the EUPG, and in particular, records of communication with the scammer on the digital messaging platform, where relevant, the name of the responsible Telco whose services the account holder had subscribed to and associated mobile phone number[15]. The communication records should sufficiently demonstrate that:

[14] 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 stipulated time period, the account holder should, if the responsible FI so requests, provide the responsible FI with reasons for the delayed report.

[15] Namely when the scam was perpetrated through SMS, as defined below at paragraph 7.7. For the purposes of assessing the appropriate parties involved in the operational workflow, specific information required are (a) the mobile number of the account user; and (b) the details and screenshot of the purported SMS which was used to scam the account user (including date, time, sender).

(a) the scammer posed as an impersonated entity;

(b) there is an intent to obtain account credentials under false pretences; and

(c) the scammer directed the account holder to a digital platform of the impersonated entity to enter his account credentials.

7.5 Upon enquiry by an account holder, the responsible FI is expected to provide the account holder with relevant information that the responsible FI has of all the seemingly authorised transactions, which were initiated or executed from the account holder's protected account, including transaction dates, transaction timestamps and parties to the transaction.

<u>Investigation Stage</u>

7.6 Where the responsible FI has assessed that a claim brought by an account holder does not involve a seemingly authorised transaction, the responsible FI investigates the claim based on its existing investigation and claim resolution process for all other claims involving unauthorised transactions that are reported to the responsible FI. The responsible FI should communicate its assessment and claim resolution process to the account holder in a timely and transparent manner.

7.7 Where the responsible FI has assessed that a claim brought by an account holder involves a seemingly authorised transaction, the responsible FI next assesses if the seemingly authorised transaction resulted from a scammer impersonating an entity and contacting the account holder using SMS ("**perpetrated through SMS**"). If so, the responsible FI should inform the responsible Telco, for the responsible Telco to commence its investigation. The responsible FI should obtain from the account holder relevant information on the scam perpetrated through SMS before referring the claim to the responsible Telco.

(a) Scam was perpetrated through SMS

7.7.1 The responsible FI and responsible Telco investigate concurrently whether each of them has fulfilled their duties under paragraphs 4.2 and 5.2, respectively.

(b) Scam was not perpetrated through SMS

7.7.2 The responsible FI investigates whether it has fulfilled its duties under paragraph 4.2.

7.8 A responsible FI and a responsible Telco should have governance structures and investigations processes, involving representatives who are independent from business units, to assess and determine whether duties have been breached.

7.9 The responsible FI, and responsible Telco where applicable, should complete an investigation of any relevant claim within 21 business days for straightforward cases or 45 business days for complex cases.[16] Complex cases may include cases where any party to the seemingly authorised transaction is overseas and uncontactable during the investigation period.

Outcome Stage

7.10 The responsible FI should within the stipulated periods in paragraph 7.9 provide each account holder that the responsible FI has been instructed to send transaction notifications to in accordance with paragraph 3.1[17] of the EUPG, a written reply of the investigation outcome and the assessment of the account holder's responsibility. The responsible FI should seek acknowledgement, which need not be an agreement, from that account holder of the investigation outcome.

Recourse Stage

7.11 Where the account holder does not agree with the assessment of responsibility, or where the responsible FI has assessed that the claim falls outside of the Guidelines; the account holder may pursue further action through existing avenues of recourse as appropriate in respect of the relevant claim made, such as FIDReC (for further dispute resolution with the responsible FI), or through writing to IMDA (if the account holder disagrees with the responsible Telco's assessment of responsibility).

[16] All relevant logs or documentation to assess SRF claims and demonstrate compliance with the SRF duties are expected to be retained for a reasonable period of time.

[17] Paragraph 3.1 of the EUPG explains that 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 notifications alerts for transactions, activation of digital security token and conduct of high-risk activities. 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 to any or all the account holders.

7.12 The withholding of charges relating to the disputed transactions as set out in Section 8[18] of the EUPG would apply where relevant to seemingly authorised transactions.

Means by which Responsible FI and Responsible Telco are to credit account holder

7.13 The responsible FI should credit the account holder's protected account with the total loss arising from any seemingly authorised transaction in accordance with the framework on assessment of responsibilities for losses set out in Section 6 of these Guidelines.

7.14 The responsible Telco should credit the account holder with the total loss (as verified by the responsible FI) arising from any seemingly authorised transaction in accordance with the framework on assessment of responsibilities for losses set out in Section 6 of these Guidelines, based on a mutually agreed payment modality with the account holder.

[18] Section 8 of the EUPG on charges relating to disputed transactions covers expectations on the responsible FI to (i) withhold and/or waive charges relating to disputed transactions; (ii) withhold the reporting of the non-payment of disputed transactions to licensed credit bureaus; and (iii) disclose charges relating to recovery of unauthorised transactions.