Monetary Authority of Singapore

Consultation Paper

P017-2023 – October 2023

Consultation Paper on Proposed Enhancements to the E-Payments User Protection Guidelines

Contents

1. Preface

1.1. The E-Payments User Protection Guidelines (EUPG) were introduced in 2018 to foster public confidence in using electronic payments, or "e-payments". It sets out the responsibilities of responsible financial institutions (FIs)[1] and consumers in relation to unauthorised and erroneous payment transactions, and establishes a baseline protection offered by responsible FIs to consumers for losses arising from the said transactions. The EUPG underscores the importance of collective efforts by both responsible FIs and consumers to mitigate the risk of unauthorised transactions[2] in Singapore.

1.2. With the rising incidence of digitally enabled scams, the Monetary Authority of Singapore (MAS) is seeking comments from industry stakeholders and members of the public on proposed enhancements to the EUPG, to uplift standards of anti-scam controls across the financial sector and place a greater emphasis on consumer vigilance and responsibility.

1.3. MAS, together with the Infocomm Media Development Authority (IMDA), also published a "Consultation Paper on Proposed Shared Responsibility Framework" on 25 October 2023. The Shared Responsibility Framework (SRF) leverages on some of the proposed enhanced anti-scam measures in the EUPG that responsible FIs are expected to implement, and holds FIs and telecommunication operators (Telcos) directly accountable to consumers for phishing scam losses, should the FIs or Telcos fail to implement these prescribed measures.

1.4. Further, MAS is seeking comments from industry stakeholders on additional guidelines to clarify the processes that responsible FIs are expected to implement in relation to erroneous transactions.

1.5. The next sections explain the key proposals for public consultation. The proposed amendments to the EUPG have been published together with this consultation paper on MAS' website.

1.6. **Please note that all submissions received will be published and attributed to the respective respondents unless they expressly request MAS not to do so. As such, if respondents would like –**

(a) **their whole submission or part of it (but not their identity), or**

(b) **their identity along with their whole submission,**

to be kept confidential, please expressly state so in the submission to MAS. MAS will only publish non-anonymous submissions. In addition, MAS reserves the right not to publish any submission

[1] These refer to all banks, finance companies, non-bank credit card issuers and relevant payment service providers issuing e-wallets, which provide accounts to individuals or sole proprietors.

[2] Unauthorised transactions refer to transactions performed without the consumer's knowledge (actual or imputed) and consent (express or implied).

received where MAS considers it not in the public interest to do so, such as where the submission appears to be libellous or offensive.

1.7. Please submit written responses through the link below by 20 December 2023:

https://go.gov.sg/eupgconsultation2023

2. Introduction

2.1. FIs in Singapore have progressively implemented a suite of anti-scam measures to tackle scams. Within the banking sector, MAS works with the Association of Banks in Singapore (ABS) and its members to step up safeguards to mitigate the risks of fraud and scams. These include measures implemented by major retail banks to strengthen the security of digital banking.[3] MAS also works closely with industry associations and public sector organisations under the national MoneySense programme to help consumers better guard themselves against falling prey to scams.

2.2. Following a review of the EUPG, MAS is proposing amendments to these guidelines to take into account lessons learnt and better address unauthorised transactions arising from prevalent scam typologies in Singapore, in particular phishing and malware-enabled scams. The proposed enhancements are in three main areas (the full set of amendments to the EUPG is at Annex A):

(a) alignment of the financial industry with established anti-scam industry practices implemented by major retail banks;

(b) additional duties of responsible FIs to facilitate prompt detection of scams by consumers and a fairer dispute resolution process; and

(c) reinforcement of consumers' responsibility to take necessary precautions against scams.

2.3. The SRF Guidelines and EUPG are meant to complement each other, with the SRF duties drawing from the EUPG.

2.4. MAS is also looking to introduce additional guidelines within the EUPG to clarify the processes expected of a responsible FI in rectifying erroneous transactions, i.e., funds that have been wrongly transferred to an account that is not held by the intended recipient, to cater for a scenario where the consumer is the wrong recipient of the funds, and has informed the responsible FI that he or she wishes for the funds to be returned to the sender.

[3] Refer to MAS' media releases "MAS and ABS Announce Measures to Bolster the Security of Digital Banking", 19 January 2022, and "Additional Measures to Strengthen the Security of Digital Banking", 2 June 2022.

3. Enhancements to duties of responsible FIs

Amendments to reflect established anti-scam practices by major retail banks announced in January and June 2022

3.1. Major retail banks in Singapore have implemented the suite of anti-scam measures announced by MAS and ABS on 19 January 2022 and 2 June 2022[4], set out in Table 1 below. MAS proposes to raise the standards (where relevant) for all responsible FIs (including other retail banks and relevant payment services providers), by including the measures in Table 1 into the EUPG.

Table 1: Amendments to align industry practice across responsible FIs	
Preventive measures	
Sending of clickable links and phone numbers	A responsible FI should not send clickable links or phone numbers to a retail consumer unless the consumer is expecting it, and if the informational link does not require the consumer to perform a transaction, and does not lead to a platform that requires consumer to download applications. This is to help consumers better discern phishing attempts where scammers impersonate responsible FIs, and send a malicious clickable link, or fake phone number. The responsible FI should ensure that its contact details on official sources (e.g., MAS' Financial Institutions Directory, FI's websites) are always updated.
Measures prior to performing high-risk activities	Prior to executing high-risk activities, the responsible FI should require additional confirmation from consumers (e.g., further authentication). It should also inform consumers of the associated risks and implications via pop-up risk-warning messages.
Cooling off period	When a digital security token is activated, a responsible FI should: (a) impose a minimum 12-hour cooling off period, during which high-risk activities cannot be performed; and (b) send a notification alert to the consumer's registered contact with the responsible FI. FI duties #1 and #2 under the proposed SRF are also drawn from this measure (see section 5 of the SRF consultation paper dated 25 October 2023).

[4] Refer to MAS' media releases "MAS and ABS Announce Measures to Bolster the Security of Digital Banking", 19 January 2022, and "Additional Measures to Strengthen the Security of Digital Banking", 2 June 2022.

Detective measures	
Outgoing transaction notification alerts	Currently, the EUPG allows transaction notification alerts to be sent on a batched basis once every 24 hours. To ensure that consumers are notified of their transactions on a timely basis, a responsible FI should send transaction notification alerts on a real-time basis for all outgoing transactions, in accordance with the transaction notification threshold[5]. This measure is also reflected in FI duty #3 under the proposed SRF (see section 5 of the SRF consultation paper).
Remedial measures	
Self-service feature ("**kill switch**")	A responsible FI should provide consumers with a kill switch, which is a self-service option for the consumer to promptly block his or her account from digital access. The kill switch should be available through a different channel from the bank's mobile or internet banking channels, to be effective against account takeover. This measure is also reflected in FI duty #4 under the proposed SRF (see section 5 of the SRF consultation paper). The kill switch should be prominently featured in the responsible FI's communication to consumers via its reporting channels or mobile application.
24/7 reporting channel	A responsible FI should have a reporting channel (e.g., manned phone line) that is available at all times for consumers to report unauthorised transactions. This measure is also reflected in FI duty #4 in the proposed SRF (see section 5 of the SRF consultation paper).

Question 1. MAS seeks comments on including the measures in Table 1 into the EUPG, which will make them applicable to all responsible FIs.

[5] This is either the responsible FI's default transaction notification level or the transaction notification level opted by the consumer.

Other enhancements to the duties of responsible FIs

3.2. Apart from the measures announced in January and June 2022, MAS also proposes other enhancements to the duties of responsible FIs under the EUPG. These are set out in Table 2 below.

Table 2: Enhancements to duties of responsible FIs

Detective measures	
Information to enable consumers to validate their intended recipient	When sending consumers access codes to authenticate transactions (e.g., SMS one-time passwords or push notifications via the FI's official mobile application), a responsible FI should ensure that these are accompanied with sufficient information to enable the consumer to confirm the validity of the transaction before authenticating it. Further details on the information that should be provided are in the draft revised EUPG.
Notification alerts when high-risk activities are performed	A responsible FI should send notification alerts to the consumer, to alert the consumer to any high-risk activities being performed. This is also reflected in FI duty #2 under the proposed SRF (see section 5 of the SRF consultation paper). Notification alerts should contain details relevant to the activity, and a reminder to the consumer to contact the responsible FI if the activity was not performed by them. Specific to the high-risk activity of changing a consumer's contact information, the notification alert should be sent to the consumer's existing contact.
Measures to ensure a fair dispute resolution process	
Expectations of responsible FIs' dispute resolution process	Responsible FIs currently have in place a dispute resolution procedure, in the event that the consumer disagrees with the FI's investigation outcome of an unauthorised transaction. To ensure a consistent standard across the industry, MAS proposes to have a new section in the EUPG setting out expectations on all responsible FIs in respect of dispute resolution processes. Further details can be found in Section 7 of the draft revised EUPG.
Charges relating to disputed unauthorised transactions	When a consumer disputes a transaction with the responsible FI ("**disputed transaction**"), the responsible FI should withhold and/or waive any outstanding amount and charges[6] directly relating to the disputed transaction, during the responsible FI's investigation period.

[6] The examples of charges directly relating to the disputed transaction include late payment fee, fall-below-balance service fee, and telegraphic transfer commission.

Withholding and/or waiving of outstanding charges and reporting to licensed credit bureaus	If the consumer does not agree with the outcome of the responsible FI's assessment, the responsible FI should further withhold and/or waive such outstanding charges for an additional 30 calendar days. This is in recognition that the consumer may seek further recourse with the Financial Industry Disputes Resolution Centre Ltd (FIDReC). If the consumer approaches FIDReC, the responsible FI should also withhold and/or waive outstanding charges on the unauthorised transactions until the completion of adjudication by FIDReC, or when the case is closed by FIDReC due to prolonged inactivity. For the duration of the period mentioned above, the responsible FI should ensure that the consumer's credit records with licensed credit bureaus are not adversely affected by reason of the disputed transactions.

Question 2. MAS seeks comments on the proposed enhancements to responsible FIs' duties in Table 2.

4. Enhancements to duties of consumers

4.1. It is paramount that consumers adopt good cyber hygiene practices and habits to reduce the risk of their accounts being compromised. MAS intends to enhance the duties of consumers within the EUPG to reinforce that consumers should take necessary precautions against scams, such as never giving away their personal or account credentials to anyone. Table 3 contains the proposed enhancements to consumer duties under the EUPG.

Table 3: Enhancements to duties of consumers

Preventive measures	
Cyber hygiene practices	Currently, consumers are advised to: (a) update the device's browser (e.g., Chrome, Safari, Internet Explorer, Firefox) to the latest version available; (b) patch the device's operating systems (e.g., iOS, Android, Windows) with regular security updates provided by the operating system provider; (c) install and maintain the latest anti-virus software on the device, where applicable; and (d) use strong passwords, such as a mixture of letters, numbers and symbols. MAS proposes that consumers adopt the following additional security practices to secure their accounts: (a) only download the responsible FI's mobile application from official sources for Singapore users, such as from Apple's App Store or Google's Play Store; (b) use strong authentication methods, such as facial or fingerprint authentication methods; (c) not to root or jailbreak mobile devices which are used to perform payment transactions; and (d) not to download and install applications which are unverified (also known as "sideloading"), or those which request device permissions that are unrelated to their intended functionalities.
Clickable links and phone numbers	Consumers should only refer to official sources (e.g., MAS' Financial Institutions Directory and information on the back of ATM/credit/debit cards) for the website addresses and phone numbers of their responsible FIs. In addition, consumers should not click on links provided in SMS or emails, unless these are informational links that the consumer is expecting to receive from the responsible FI. Such practices will reduce the risk of consumers falling for phishing scams.

Measures prior to performing high-risk activities	In conducting high-risk activities, consumers should read the pop-up risk warning messages sent by the responsible FI and check that the action was intended, before proceeding with the activity.
Measures prior to authenticating transactions	Before authenticating transactions, consumers should read the contents of the messages containing the authorisation access codes provided by the responsible FI and ensure that the stated recipient is the intended recipient.
Remedial measures	
Reporting unauthorised activities	A consumer should report any unauthorised activity on his or her account to the responsible FI as soon as practicable, and no later than 30 calendar days after receipt of any notification alert for any unauthorised activity. Unauthorised activities include any payment transactions, activation of a digital security token, or high-risk activities performed without the consumer's initiation or consent.
Activating kill switch	Consumers should activate the kill switch as soon as practicable after they have been notified of any unauthorised transaction or have any reason to believe that their account have been compromised.
Lodging police reports	After reporting the unauthorised transaction to the responsible FI or activating the kill switch to mitigate further losses, consumers should also make a police report if they suspect that the transaction arose from a scam or fraud. The consumer may reach out to the responsible FI for assistance on how to make a police report. The consumer should cooperate with the Police and provide evidence of the scam or fraud as far as practicable.[7] The consumer should furnish the police report to the responsible FI within 3 calendar days after notifying the responsible FI of the unauthorised transaction.

Question 3. MAS seeks feedback on the additional duties for consumers in Table 3.

[7] This would include facilitating the Police's access to the consumer's electronic device for potential forensics investigation.

5. Additional guidelines to clarify processes in relation to erroneous transactions

Duties of responsible FIs where the wrong recipient requests for funds to be returned

5.1. The EUPG currently sets out specific duties of responsible FIs and consumers in a scenario where a consumer (the "**sender**") mistakenly transfers funds to an unintended recipient (the "**wrong recipient**"), and upon realising this, makes a request to his or her responsible FI (the "**sender FI**") for the funds to be returned.

5.2. The EUPG, however, does not presently cater for a scenario where the *wrong recipient* is the one who realises that funds have been transferred erroneously into his or her account, and requests his or her responsible FI (the "**recipient FI**") for the funds to be returned. MAS therefore proposes to introduce guidelines in Section 6 of the EUPG to cater for such a scenario. MAS has engaged major retail banks to find out their practices for such a scenario.

5.3. To the extent possible, the proposed new guidelines – summarised in Table 4 below – are intended to be consistent with the existing timelines for sender FIs and recipient FIs in the scenario where the sender requests for the funds to be returned. Responsible FIs may choose to implement shorter timeframes (than those prescribed in the EUPG) for handling such scenarios of erroneous transactions, based on their own internal procedures. The full set of amendments to Section 6 of the EUPG can be found in the draft revised EUPG at Annex A.

Table 4: Proposed new guidelines where request to return the erroneously transferred funds is initiated by the wrong recipient

Timeline	Duties of the recipient FI / sender FI
T Day	The wrong recipient informs the recipient FI of the funds that were erroneously transferred into his or her account. The recipient FI should acknowledge the wrong recipient's request to return the funds, and provide a timeline for responding to the wrong recipient.

Within T + 2 business days	Where the sender FI's confirmation is necessary for the return of funds, the recipient FI should inform the sender FI of the erroneous transaction, and provide the relevant information needed by the sender FI.
Within T + 7 business days	The sender FI should provide an update to the recipient FI, i.e., whether the funds can be returned by the recipient FI (only applicable where the sender FI's confirmation is necessary for the return of funds).
Within T + 9 business days	The recipient FI should update the wrong recipient on whether the return of the erroneously transferred funds was successful.

Question 4. *MAS seeks feedback on the proposed new guidelines for handling erroneous transactions, where the request for the return of funds is initiated by the "wrong recipient".*

Question 5. *MAS seeks any other comments on the draft amendments to the EUPG (in Annex A), which have been published together with this consultation paper.*

6. List of Questions