



Circular No: MAS/PD/2024/10/04

Date: 25 October 2024

To Chief Executives of all Major Payment Institutions licensed to provide account issuance service and that issue personal payment accounts containing e-money

Dear Sir/Madam

**ANTI-SCAM MEASURES BY MAJOR PAYMENT INSTITUTIONS THAT ISSUE PERSONAL PAYMENT ACCOUNTS CONTAINING E-MONEY**

This circular sets out the Monetary Authority of Singapore (the “Authority”)’s expectations of Major Payment Institutions (“MPIs”) that are licensed under the Payment Services Act 2019 (“PS Act”) to carry on a business of providing an account issuance service and that issue personal payment accounts<sup>1</sup> containing e-money<sup>2</sup> (“e-wallets”).

2 On 15 December 2023, the Payment Services Regulations 2019 were amended to raise the regulatory limit on the stock cap<sup>3</sup> and flow cap<sup>4</sup> for e-wallets.<sup>5</sup> MPIs that issue e-wallets (“MPI e-wallet providers”) can now provide individual customers with a stock cap of up to S\$20,000 (previously S\$5,000), and a flow cap of up to S\$100,000 (previously S\$30,000). The Authority recognises that with e-wallets capable of holding and transferring more funds, customers may be exposed to a higher risk of suffering more losses from scams. Scammers may also use their own e-wallet as a conduit to channel larger amounts of scam proceeds.

3 Where an MPI e-wallet provider wishes to raise the stock and/or flow caps for its customers’ e-wallets beyond the previous regulatory limits of S\$5,000 and S\$30,000, respectively (hereafter, “adopts/adopting the higher e-wallet caps”), the Authority expects the MPI e-wallet provider to first implement anti-scam measures commensurate to the increased risk. In this regard, MPI e-wallet providers are expected to implement the anti-scam measures set out in **Annex A**, prior to adopting the higher e-wallet caps.

---

<sup>1</sup> “Personal payment account” has the same meaning given by section 24(5) of the Payment Services Act 2019.

<sup>2</sup> “E-money” has the same meaning given by section 2(1) of the Payment Services Act 2019.

<sup>3</sup> “Stock cap” refers to the maximum amount of funds that can be held at any given time in an e-wallet.

<sup>4</sup> “Flow cap” refers to the maximum total outflow of funds in any period of one year from an e-wallet, other than to a personal deposit account that is either in the name of or designated by the e-wallet user.

<sup>5</sup> The Authority’s consultation paper dated 18 October 2022 ([link](#)) explains the reasons for raising the regulatory limits on stock and flow caps.

4 MPI e-wallet providers that do not wish to adopt the higher e-wallet caps, should consider the anti-scam measures and look to progressively implement these measures over time.

5 The Authority expects the Board and Senior Management of every MPI e-wallet provider that adopts the higher e-wallet caps to be responsible for ensuring that adequate anti-scam measures are implemented. This includes establishing a robust governance framework for the oversight of consumer scam risk and fair treatment of customers. The governance framework should include an incident management process to enable a prompt and coordinated response to targeted and severe scam attacks against customers. In the event that customers bring disputes for losses arising from scams, such disputes should be assessed by an independent unit that is separate from the business functions of the MPI e-wallet provider.

6 The Authority may review and update the measures in **Annex A** to take into account future developments in the scams landscape and new scam typologies.

## **Annex A: List of anti-scam measures to be implemented by Major Payment Institutions that issue personal payment accounts containing e-money**

### **Table of Contents**

<b>A. Definitions.....</b>	<b>2</b>
<b>B. Preventive Measures .....</b>	<b>4</b>
1. Restrictions on sending of clickable links or Quick Response (“QR”) codes via email or SMS, or phone numbers via SMS .....	4
2. 12-hour cooling off period upon login to e-wallet on a new device.....	5
3. Additional confirmation when performing high-risk activities and large funds transfers.....	5
4. Default transaction limit .....	5
5. Default limit on top-up sources linked to each e-wallet.....	6
6. Default limit on the number of e-wallets that one top-up source is linked to .....	6
7. Flexibility to opt out from having higher e-wallet caps .....	7
<b>C. Detective Measures .....</b>	<b>7</b>
8. Outgoing transaction notification alerts .....	7
9. Default transaction notification thresholds .....	8
10. Notification alerts for login to e-wallet on new device or high-risk activities .....	8
11. Real-time detection and blocking of suspicious transactions.....	9
<b>D. Remedial measures .....</b>	<b>9</b>
12. Provision of reporting channel.....	9
13. Self-service feature (kill switch) .....	10

## A. Definitions

For the purposes of this Annex—

“access code” means a password, code or any other arrangement that the e-wallet user must keep secret, that may be required to authenticate any payment transaction or e-wallet user;

“account contact” means the contact information that the e-wallet holder has provided the MPI e-wallet provider, including an e-wallet holder’s registered phone number or email address with the MPI e-wallet provider, for the MPI e-wallet provider to send the e-wallet holder notification alerts for transactions, logins to the e-wallet holder’s e-wallet on a new device, and the conduct of high-risk activities;

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

“e-wallet” means a personal payment account that contains e-money;

“e-wallet card” means a debit card that is held in the name, or associated with the unique identifier, of the e-wallet user, and is used by that person for the initiation of a payment order or the execution of a payment transaction, or both, which draws down from the balance of e-money in the e-wallet of the e-wallet holder;

“e-wallet holder” means any person in whose name an e-wallet account has been opened or to whom an e-wallet has been issued;

“e-wallet user” means—

- (a) any e-wallet holder; or
- (b) any person who is authorised in a manner in accordance with the account agreement, by the MPI e-wallet provider and any e-wallet holder to initiate, execute, or both initiate and execute payment transactions on the e-wallet;

“flow cap” means—

- (a) the maximum amount of e-money transferred in any period of one year, from a personal payment account issued by the MPI e-wallet provider to an e-wallet holder, other than to a personal deposit account that is either in the name of or designated by that e-wallet holder; or
- (b) in the case of an MPI e-wallet provider that issues 2 or more personal payment accounts to any e-wallet holder, the combined maximum amount of e-money transferred in any period of one year, from all personal payment accounts issued by the MPI e-wallet provider to that e-wallet holder, other than to any personal deposit account that is either in the name of or designated by that e-wallet holder;

“funds transfer” means a payment transaction that is initiated by logging into an e-wallet holder’s e-wallet and giving an instruction to the MPI e-wallet provider for the placing, transfer or withdrawal of money from the e-wallet holder’s e-wallet;

“high-risk activities”, where applicable to an MPI e-wallet provider, include (but are not limited to)—

- (a) adding of payees to the e-wallet holder’s payment profile;
- (b) increasing the transaction limits for outgoing payment transactions from the e-wallet;
- (c) disabling transaction notification alerts that the MPI e-wallet provider will send upon completion of a payment transaction;
- (d) change in the e-wallet holder’s contact information including mobile number, email address and mailing address;

“higher e-wallet caps” means a stock cap that is higher than S\$5,000 (or its equivalent in a foreign currency), or a flow cap that is higher than S\$30,000 (or its equivalent in a foreign currency), or both, which an MPI e-wallet provider has set for its e-wallet holder’s e-wallet, subject to the limits prescribed in Regulation 18 of the Payment Services Regulations 2019;

“MPI e-wallet 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 an account issuance service and that issues e-wallets;

“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;

“personal payment account” has the same meaning given by section 24(5) of the Payment Services Act 2019;

“stock cap” means—

- (a) the maximum amount of e-money contained in a personal payment account issued by the MPI e-wallet provider to an e-wallet holder; or
- (b) in the case of an MPI e-wallet provider that issues 2 or more personal payment accounts to any e-wallet holder, the combined maximum amount of e-money

contained in all personal payment accounts issued by the MPI e-wallet provider to that e-wallet holder;

“transaction notification threshold” means—

- (a) the threshold for transaction notification alerts set by the e-wallet holder (where applicable); or
- (b) if the e-wallet holder did not set any threshold for transaction notification alerts, the default transaction notification threshold of S\$0;

“unauthorised transaction” means any payment transaction initiated by any person without the actual or imputed knowledge and implied or express consent of an e-wallet user.

“unique identifier” means a combination of letters, numbers or symbols specified by the MPI e-wallet provider to the e-wallet holder and is to be provided by the e-wallet 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; or
- (b) any person’s e-wallet.

## B. Preventive Measures

### 1. Restrictions on sending of clickable links or Quick Response (“QR”) codes via email or Short Message Services (“SMS”), or phone numbers via SMS

1.1. MPI e-wallet providers should not send clickable links or QR codes via email or SMS to an e-wallet user unless:

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

1.2. MPI e-wallet providers should not send phone numbers via SMS to an e-wallet user unless the e-wallet user is expecting to receive the SMS from the MPI e-wallet provider.

**2. 12-hour cooling off period upon login to e-wallet on a new device**

- 2.1. When there is a login to an e-wallet holder's e-wallet on a new device, allowing transactions to be authenticated on the new device, the MPI e-wallet provider should impose a cooling off period of at least 12 hours where high-risk activities cannot be performed on the e-wallet holder's e-wallet using the new device, from the time of the login on such new device.

**3. Additional confirmation when performing high-risk activities and large funds transfers**

- 3.1. MPI e-wallet providers should obtain additional confirmation (via keying in additional access codes, or other equivalent authentication methods) from an e-wallet user prior to allowing any high-risk activity or funds transfer exceeding S\$1,000 to be performed on the said e-wallet. For the avoidance of doubt, where the MPI e-wallet provider has received any instructions to change the e-wallet holder's account contact and requires the keying in of an SMS one-time-password ("OTP") as a means for authenticating such an instruction, the SMS OTP should be sent to the e-wallet holder's existing account contact first, before effecting the change.
- 3.2. MPI e-wallet providers should also inform the e-wallet user of the risks and implications of performing a high-risk activity or funds transfer exceeding S\$1,000, at the point immediately before such high-risk activity or such funds transfer (as the case may be) is performed by the e-wallet user.

**4. Default transaction limit**

- 4.1. MPI e-wallet providers should set a default transaction limit of at most S\$1,000 on outgoing payment transactions from e-wallets including scheduled recurring outgoing payment transactions, but excluding (i) all outgoing payment transactions initiated by way of using the e-wallet card at physical point of sale ("POS") terminals or automated teller machines ("ATMs"), and (ii) all outgoing payment transactions made between two payment accounts held in the name of the same person. The above default transaction limit need not be applied to payment transactions that do not draw down from the balance of e-money in the e-wallet holder's e-wallet.<sup>6</sup>
- 4.2. MPI e-wallet providers may allow e-wallet users to subsequently adjust their transaction limits higher than S\$1,000, if the e-wallet user chooses to do so.

---

<sup>6</sup> One example is a payment transaction that is charged directly to a bank-issued card or bank account that has been added as a payment method in the e-wallet holder's account, and does not draw down from the e-money balance in the e-wallet holder's e-wallet.

- 4.3. Paragraphs 4.1 and 4.2 need not be applied to scheduled recurring outgoing payment transactions where an e-wallet user's instructions in respect of such payment transactions were made prior to the MPI e-wallet provider adopting higher e-wallet caps.

**5. Default limit on top-up sources linked to each e-wallet**

- 5.1. MPI e-wallet providers should, as a default, allow no more than two top-up sources (e.g., each bank account, credit card) to be linked to each e-wallet that is issued by the MPI e-wallet provider, if the said top-up source is not verified to be owned by the e-wallet user.<sup>7</sup>
- 5.2. If an e-wallet holder wishes to link more than two top-up sources to his e-wallet where each such top-up source has not been verified to be owned by the e-wallet user, the MPI e-wallet provider should conduct proper due diligence before acceding to the request, including seeking explanation from the e-wallet user on the reasons for the request.
- 5.3. Paragraphs 5.1 and 5.2 need not be applied to top-up sources that were linked to the e-wallet holder's e-wallet prior to the MPI e-wallet provider adopting higher e-wallet caps.

**6. Default limit on the number of e-wallets that one top-up source is linked to**

- 6.1. MPI e-wallet providers should, as a default, allow a given top-up source (e.g., each bank account, credit card) to be linked to no more than two e-wallets issued by the same MPI e-wallet provider to the same e-wallet holder, if the said top-up source is not verified to be owned by the e-wallet user.
- 6.2. If the e-wallet user wishes to link a top-up source to more than two e-wallets provided by the MPI e-wallet provider, where the said top-up source is not verified to be owned by the e-wallet user, the MPI e-wallet provider should conduct proper due diligence before acceding to the request, including seeking explanation from the e-wallet user on the reasons for the request.
- 6.3. Paragraphs 6.1 and 6.2 need not be applied to top-up sources that were linked to the e-wallet holder's e-wallet prior to the MPI e-wallet provider adopting higher e-wallet caps.

---

<sup>7</sup> MPI e-wallet providers should determine how they wish to verify the identity of the top-up source owner, such that it gives them sufficient assurance that the top-up source owner is the same as the e-wallet user.

## 7. Flexibility to opt out from having higher e-wallet caps

- 7.1. MPI e-wallet providers should provide each e-wallet user with the choice of opting out from having the higher e-wallet caps.<sup>8</sup>
- 7.2. Where an e-wallet user has previously opted out from having the higher e-wallet caps, MPI e-wallet providers should put in place a proper process to verify and check, if the said e-wallet user subsequently elects to opt back in for the higher e-wallet caps.

## C. Detective Measures

### 8. Outgoing transaction notification alerts

- 8.1. MPI e-wallet providers should provide transaction notification alerts on a real-time basis for each outgoing payment transaction, to each e-wallet holder that the MPI e-wallet provider has been instructed to send transaction notification alerts to, in respect of all outgoing payment transactions (of any amount in accordance with the transaction notification threshold) made from the e-wallet holder's e-wallet. The transaction notification alert should fulfil the following criteria:
  - (a) The transaction notification alert should be sent to the e-wallet holder's account contact. If the e-wallet holder has provided more than one account contact to the MPI e-wallet provider, the transaction notification alert should be sent to every account contact selected by the e-wallet holder to receive such notifications.
  - (b) The transaction notification alert should be conveyed to the e-wallet holder by way of SMS, email or in-app/push notification.
  - (c) The transaction notification alert should contain the following information, but the MPI e-wallet provider may omit any confidential information provided that the information still allows the e-wallet holder to identify the transaction as being an authorised transaction or unauthorised transaction.
    - i. Information that allows the e-wallet holder to identify that an outgoing payment transaction has been made from his e-wallet;

---

<sup>8</sup> For the avoidance of doubt, the Authority does not prescribe the range of different stock and/or flow caps to be offered to e-wallet users to choose from, as long as there is a choice for the e-wallet user to opt out from having the higher e-wallet caps. MPI e-wallet providers may also decide if they wish to allow e-wallet users to further adjust their stock and/or flow caps after making the initial choice of whether to opt out from the higher e-wallet caps.

- ii. Information that allows the e-wallet holder to identify the recipient of the outgoing payment transaction, whether by name or by other credentials such as the recipient's account number;
- iii. Information that allows the MPI e-wallet provider to later identify the e-wallet holder, the e-wallet from which the outgoing payment transaction was made, and the recipient of the outgoing payment transaction, such as each e-wallet account number or name of the e-wallet holder;
- iv. Transaction amount (including currency);
- v. Transaction time and date;
- vi. Transaction type;
- vii. 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.

## **9. Default transaction notification thresholds**

- 9.1. MPI e-wallet providers should set the default threshold for outgoing transaction notification alerts at S\$0 (i.e., notification alerts are sent for all outgoing payment transactions), to enable early detection of fraudulent transactions from the e-wallet. MPI e-wallet providers may avail e-wallet users of the option to subsequently adjust their transaction notification threshold, if the e-wallet user chooses to do so.

## **10. Notification alerts for login to e-wallet on new device or high-risk activities**

- 10.1. MPI e-wallet providers should provide notification alerts on a real-time basis, which fulfil the following criteria, to the e-wallet holder, when there is a login to his e-wallet on a new device or when any high-risk activities are performed:
  - (a) The notification alert should be sent to the e-wallet holder's existing account contact with the MPI e-wallet provider. If the e-wallet holder has provided more than one account contact to the MPI e-wallet provider, the notification should be sent to every account contact selected by the e-wallet holder to receive such notifications.
  - (b) The notification alert should be conveyed to the e-wallet holder by way of SMS, email or in-app/push notification.

- (c) Where applicable, the notification alert should contain details on the new mobile device that has been linked to the e-wallet holder's e-wallet or on the high-risk activity (e.g., information on the change in account contact or new transaction notification thresholds).
- (d) The notification alert should contain a reminder for the e-wallet holder to contact the MPI e-wallet provider if the linking of the new mobile device to the e-wallet holder's e-wallet, or the high-risk activity was not performed by the e-wallet holder.

## **11. Real-time detection and blocking of suspicious transactions**

- 11.1. MPI e-wallet providers are reminded of the requirements under PSN01 on *Prevention Of Money Laundering And Countering The Financing Of Terrorism – Holders Of Payment Services Licence (Specified Payment Services)* to monitor, on an ongoing basis, transactions undertaken by customers throughout the course of business relations. This includes implementing adequate systems and processes to detect complex, unusually large or unusual patterns of transactions that have no apparent or visible economic or lawful purpose and report suspicious transactions in a timely manner.
- 11.2. To mitigate the risk of higher scam losses from e-wallets or e-wallets being used as a means for moving scam proceeds, timely detection, intervention and reporting is key, and MPI e-wallet providers should have capabilities to detect and block suspicious transactions at all times. MPI e-wallet providers should also have the capability to inquire into the authenticity of suspicious transactions before allowing such transactions to be executed.
- 11.3. MPI e-wallet providers should review the effectiveness of fraud detection parameters on an annual basis, or as and when there are material triggers.

## **D. Remedial measures**

### **12. Provision of reporting channel**

- 12.1. MPI e-wallet providers should provide e-wallet users 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 e-wallet. The reporting channel should have all the following characteristics:
  - (a) The reporting channel 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, or mobile application of the MPI e-wallet provider.

- (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) MPI e-wallet providers 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.
- 12.2. MPI e-wallet providers should have the ability to freeze compromised accounts immediately upon reporting by e-wallet users. MPI e-wallet providers should also have dedicated personnel to act as a single point of contact for scam victims to follow up on the status and investigation progress of their case.

### **13. Self-service feature (kill switch)**

- 13.1. MPI e-wallet providers should provide a kill switch for an e-wallet holder to promptly block access to his e-wallet and disallow outgoing payment transactions to third parties. The kill switch should be made available in a prominent manner via the mobile application of the MPI e-wallet provider or the reporting channel provided by the MPI e-wallet provider to report unauthorised transactions.