November 2024

MAS Circular on Anti-scam measures by Major Payment Institutions Providing Personal Payment Accounts that contain E-money

On 25 October 2024, the Monetary Authority of Singapore ("**MAS**") published the Circular on Anti-scam measures by Major Payment Institutions Providing Personal Payment Accounts that contain E-money (the "**Circular**"). The Circular sets out MAS' supervisory expectations of Major Payment Institutions ("**MPIs**") that provide personal payment accounts containing e-money. This Client Update provides a summary of the key contents of the circular.

1. Introduction

By way of background, the Payment Services Regulations 2019 ("**PSR**") was amended on 15 December 2023 to increase the regulatory limits on the stock caps and flow caps for personal payment accounts containing e-money ("**e-wallets**"). The term "stock cap" refers to the maximum amount of funds that can be held at any given time in an e-wallet, while the term "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. Pursuant to these amendments, MPIs that issue e-wallets are permitted to provide individual customers with a stock cap of up to S$20,000 (this was previously limited to S$5,000) and a flow cap of up to S$100,000 (this was previously limited to S$30,000).[1] The Circular sets out certain measures which an MPI that provides e-wallets must implement prior to adopting these higher stock caps and flow caps ("**higher e-wallet caps**").

While MAS has acknowledged the merits of permitting higher e-wallet caps, it also recognised that e-wallets capable of holding and transferring more funds may leave customers susceptible to suffering greater losses from scams, and that scammers may abuse these higher limits to use their own e-wallets as a conduit to channel larger amount of proceeds from scams.

Under the Circular, where an MPI adopts the higher e-wallet caps, it would be expected to implement certain anti-scam measures. Broadly speaking, these measures may be broken down into the following three categories: (A) preventative measures, (B) detective measures, and (C) remedial measures. We discuss the salient measures set out under each category below.

2. Key anti-scam measures expected of MPIs adopting higher e-wallet caps

(A) Preventive Measures

Firstly, the default transaction limit for e-wallets should be set at S$1,000. This transaction limit applies to all outgoing payment transactions from e-wallets, including scheduled recurring outgoing payment transactions. However, this limit would not apply to: (i) outgoing payment transactions initiated by way of using the e-wallet card at physical point of sale terminals or automated teller machines, and (ii) all outgoing payment transactions made between two payment accounts held in the name of the same person. Nonetheless, MPIs may allow e-wallet users to adjust the transaction limits to an amount above S$1,000 if the user so chooses. The default transaction limit of S$1,000 also does not apply to scheduled recurring outgoing payment transactions where the e-wallet user's instructions on such scheduled transactions were provided to the MPI prior to the MPI implementing the higher e-wallet cap.

---

[1] On 18 October 2022, MAS had issued a Consultation Paper on Proposed Amendments to Restrictions on Personal Payment Accounts that Contain E-Money (the "**Consultation Paper**") explaining its rationale for raising the regulatory limits on stock caps and flow caps (accessible here). For a quick summary of the Consultation Paper, you may refer to the Client Update prepared by our firm in October 2022, which outlined the key proposals contained in the Consultation Paper (accessible here).

Secondly, MPIs should obtain additional confirmation from e-wallet users prior to allowing any high-risk activity or a funds transfer exceeding S$1,000. A "high-risk" activity is generally defined to include the following:

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

Where the MPI has received 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. MPIs 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 a high-risk activity or a funds transfer exceeding $S1,000 is performed by the e-wallet user.

Thirdly, MPIs should provide e-wallet users with the flexibility to opt out from having a higher e-wallet cap. In this regard, where an e-wallet user has previously opted out from having a higher e-wallet cap, the MPI should put in place a proper process to verify and check, if the e-wallet user subsequently elects to go back to a higher e-wallet cap.

(B) Detective Measures

Firstly, MPIs should provide transaction notification alerts to the e-wallet holder on a real-time basis for each outgoing payment transaction.

The transaction notification alerts should:

(i) 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, the transaction notification alert should be sent to every account contact selected by the e-wallet holder to receive such notifications.
(ii) be conveyed to the e-wallet holder by way of SMS, email or in-app/push notification.
(iii) contain certain key pieces of information to allow the e-wallet holder to identify the transaction as being an authorised transaction or unauthorised transaction.

Secondly, MPIs should set the default threshold for outgoing transaction notification alerts at S$0. This effectively means that notification alerts should be sent for all outgoing payment transactions. This to enable early detection of fraudulent transactions from the e-wallet. Nonetheless, MPIs may allow the e-wallet user the option to subsequently adjust their transaction notification threshold if the user so choose.

Thirdly, MPIs should provide notification alerts on a real-time basis to the e-wallet holder whenever there is a login to his e-wallet on a new device or when any high-risk activities are performed. 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 (for e.g., information on the change in account contact or new transaction notification thresholds). The notification alert should also contain a reminder for the e-wallet holder to contact the MPI 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.

(C) Remedial Measures

Firstly, MPIs should provide e-wallet users with a reporting channel that is available at all times for users to report unauthorised or erroneous transactions, and to block further access via mobile and online channels to his e-wallet. The reporting channel may in the form of a manned phone line, a phone number to which text messages can be sent to, an online portal which text messages can be sent to, an email address that is monitored, or the MPI's mobile application. 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. Furthermore, MPIs should have the

ability to freeze compromised accounts immediately upon receiving a report. There should also be 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.

Secondly, MPIs 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 or the reporting channel provided by the MPI.

3. Conclusion

MAS expects the directors and senior management of every MPI 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, including an incident management process. Where 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.

While the Circular is of particular relevance to MPIs that have adopted or wish to adopt the higher e-wallet caps, MAS noted that MPIs that do not wish to adopt the higher e-wallet caps should nonetheless consider the anti-scam measures and look to progressively implement these measures over time.

It should also be noted that the Circular was published on the same day as the revised E-Payments User Protection Guidelines, and a day after the Guidelines on Shared Responsibility Framework were published by MAS. The revised E-Payments User Protection Guidelines and the Guidelines on Shared Responsibility Framework, which will both be effective on 16 December 2024, were also published as part of wider efforts to tackle scams in Singapore. MPIs should read the Circular in conjunction with the E-Payments User Protection Guidelines, as well as other relevant regulations and notices.

In an age where online scams are unfortunately becoming more rampant, MPIs which provide e-wallets must endeavour to strike the delicate balance between adopting robust measures to protect and safeguard its customers from such risks on one hand, while still allowing the user experience to be as convenient and seamless as possible on the other.

A copy of the Circular can be obtained here.

This Client Update was authored by Christopher James Huang (Associate).

For more information, please contact:

Eric Chan
Partner
T: +65 6439 0788
E: eric.chan@shooklin.com

Shook Lin & Bok LLP
1 Robinson Road #18-00 AIA Tower Singapore 048542 **T** +65 6535 1944 **F** +65 6535 8577 **E** slb@shooklin.com **W** www.shooklin.com