

## **E-Payment Guideline FAQs**

### **On Guidelines**

1. What are the E-payment User Protection Guidelines all about?

The Guidelines are issued by MAS to protect users of electronic payments. They aim to encourage wider adoption of e-payments in Singapore.

The Guidelines establish a common baseline protection that Financial Institutions will provide to individuals and sole proprietors from losses arising from unauthorised or erroneous e-payment transactions from their protected accounts.

2. What is a protected account?

Protected accounts as defined in the Guidelines are those that:

- are held by either individuals or sole proprietors, including those held jointly by multiple account holders; and
- can hold a balance of more than \$500 at any one time (Stored value facilities like EZ-Link card and NETS Cashcard are thus not covered by the Guidelines), or is a credit facility.

3. What e-payments do the Guidelines cover?

All payments initiated through electronic means, and where funds are received through electronic means are covered. These include online payments and transfers

4. How do the Guidelines protect me?

Banks will provide you with transaction notifications and a reporting channel, so that you may be alerted of unauthorised transactions and report them should they happen.

Banks will investigate all claims of unauthorised transactions, with the aim of achieving a fair and reasonable resolution.

The Guidelines also set out your responsibilities as an e-payment user to adopt good security practices. These include how you should protect your device, login credentials, access codes and protected accounts.

### **Transaction notifications**

5. What are these transaction notifications for?

The notifications safeguard you against unauthorised and erroneous transactions. They are to alert you of such transactions so that you may report them to your bank for quicker resolution.

6. What type of transactions will I be notified of?

Notifications will be sent by your bank for all outgoing payments initiated through electronic means, and where funds are received through electronic means. These include online payments/transfers and debit/credit card transactions.

Some electronic transactions may not trigger notifications if they were not initiated through electronic means, or if the funds were not received through electronic means. Transactions initiated by your bank, such as credit card cashbacks, will not trigger notifications under the Guidelines. If you would like to find out which transactions are not covered by the Guidelines, please ask your bank.

The notifications you receive may also depend on your instructions to your bank. For instance, you may have instructed your bank that a notification be sent only for certain types of outgoing transactions or if a transaction is above a certain amount.

7. How will these notifications be sent?

Notifications may be sent via SMS, email or in your bank app. They may be sent either per transaction or on a consolidated/batched basis at least once every 24 hours.

For example, if you made 10 e-payments during a 24-hour period, you may receive either 10 separate SMSes/emails or one consolidated SMS/email for the 10 transactions. The approach may differ from bank to bank.

8. Do I need to enrol for these notifications?

All banks will automatically enrol you for notifications of outgoing transactions regardless of whether you are a new or existing customer. You may ask your bank for instructions on setting your notification preferences. Please update your bank with your latest mobile number or email address to ensure that you receive the notifications.

9. Can I choose the mode of notification?

You may ask your bank for the available options and how the mode of notification may be changed from the bank's default.

10. Will I be charged for this service?

This service is currently free.

11. If I am the joint account holder, will I get the transaction notifications?

This will depend on your notification settings. You may ask your bank for information on the default setting and instructions to change your notification settings.

12. I am a supplementary cardholder, will I receive these notifications?

Please refer to your cardholder agreement or ask your bank.

13. How can I stop my joint account holder from receiving e-payment notifications?

Your joint account holder will need to change his/her notification settings. You may ask your bank for instructions on how this may be done.

14. I am receiving too many notifications, how do I stop these notifications?

The notifications are a safeguard against unauthorised and erroneous transactions. Each bank has its own default notification settings. Based on your payment patterns, you may wish to adjust your notification thresholds so that you receive notifications that are most relevant to you. For instance, you may wish to be notified only if the transaction is above a certain amount. Please ask your bank how you can do this.

15. I wish to receive notifications only for credit card transactions. Is this possible?

Please refer to your bank on the options that are available.

16. What will happen to existing notification thresholds that I have set previously?

Your bank may choose to maintain the transaction notification preferences that you have set previously. You may ask your bank how it will apply thresholds that you have in place currently.

17. What should I do if I receive a notification for a transaction that I do not recognise?

This could be an unauthorised transaction and you should inform your bank immediately. Your bank may request the following information from you:

- a. The bank account affected;
- b. Your 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;
- e. Whether the account number, authentication device, or access code was lost, stolen or misused and if so,
  - i. the date and time of the loss or misuse,
  - ii. the date and time that the loss or misuse, was reported to you, and
  - iii. the date, time and method that the loss or misuse, was reported to the police;
  - iv. any access code that is applicable to the account,
  - v. how the account holder or any account user recorded the access code, and
  - vi. whether the account holder or any account user had disclosed the access code to anyone.

### **Liability and reporting of erroneous/unauthorised transactions**

18. If I report an unauthorised or erroneous transaction to my bank, when can I expect a resolution?

Your bank should complete an investigation of any relevant claim within 21 business days for straightforward cases, and up to 45 business days for complex cases.

For erroneous/unauthorised transactions on credit cards, charge cards or debit cards, the dispute resolution process established under the respective card scheme will apply.

19. If I report an unauthorised transaction, am I still liable for the transaction?

You will not be liable for any loss that arises from any action or omission by your bank, if you have complied with your duties as an account holder. For losses due to any independent third party other than you and your bank, you will also not be liable if the transaction value is within S\$1,000.

You will, however, be liable if it is ascertained that the primary cause was recklessness on your part, such as failing to protect your access code or access to your protected account. Your liability will be capped at the transaction limit or daily payment limit that you and your bank have agreed to.

In all cases, your bank will conduct an assessment to determine the appropriate liabilities and work towards a fair and reasonable resolution.

For transactions on credit cards, charge cards and debit cards issued in Singapore, the apportioning of liabilities is governed by the ABS Code of Consumer Banking Practice.

20. What should I do if I receive erroneously sent funds?

Please inform your bank as soon as is practicable. You may be facilitating criminal activities, such as money laundering and unlicensed money lending, if you knowingly receive money from strangers, dubious sources or other unverified sources. It is a criminal offence if your bank account is used to receive money linked to criminal activities or keeping erroneously sent funds.

21. If I have sent funds erroneously to a wrong party, what should I do to get my money back?

Please contact your bank to log your case. Reasonable efforts will be taken by your bank to recover the money sent, where possible. Banks will facilitate communication between you and the recipient to help you recover the money that was sent wrongly.

## Duties of account holder

22. What are my responsibilities in making e-payments?

- a. Provide accurate contact information for your bank to send transaction notifications;
- b. Protect your access codes, login credentials and access to your protected accounts; login credentials include access code, PIN, OTP or other credentials that are used to authenticate your identity.
- c. Enable and monitor transaction notifications and report unauthorised transactions as soon as possible;
- d. Provide information on unauthorised transactions as requested by your bank to support investigations; and
- e. Make a police report if your bank request such a report to be made to facilitate claims investigation.

You may wish to ask your bank for more tips on protecting your money and managing transaction notifications.

More details may be found in the E-payments User Protection Guidelines published on the MAS website ([www.mas.gov.sg](http://www.mas.gov.sg)).