MAYBANK SINGAPORE E-PAYMENTS POLICY

The Monetary Authority of Singapore has issued the E-Payments User Protection Guidelines ("**Guidelines**") which sets out your rights and obligations with regards to carrying out electronic payment transactions with us. In response to the Guidelines and as part of our obligation to play a proactive role in educating our customers, we have issued this E-Payments Policy ("**Policy**").

For the avoidance of doubt, this Policy forms part of the terms and conditions governing your relationship with us ("**Terms and Conditions**") and should be read in conjunction with the Terms and Conditions. Any term used in this Policy shall have the same meaning as defined in the Guidelines, unless expressly defined otherwise. Please note that this Policy is a summary of the Guidelines, for the latest and full set of Guidelines please visit the Monetary Authority of Singapore's website.

As at the date of publication, this Policy applies to account holders who are individuals and sole proprietors only.

Your Responsibilities

Contact information, option to receive and transaction notifications

As an account holder with Maybank Singapore Limited ("**Maybank**", "**us**" or "**we**") it is your responsibility to comply with the following:

1. You must provide us with the contact details we need in order for us to send you transaction notifications, as set out in this Policy. Where the protected account you have with us is a joint account, all account holders must jointly give instructions to us on which account holder(s) should receive transaction notifications.

2. It is your responsibility and the responsibility of any account user (an "**account user**" means you and anyone you authorise to initiate and/or execute payment transactions in relation to your protected account with us), to:

   a) enable notifications on any device used to receive transaction notifications;
   b) opt out or modify how you receive transaction alerts; and
   c) monitor the transaction notifications sent to you.

   We will assume that you will monitor such notifications without further reminders or notifications from us.

3. You must inform us immediately of any change of your contact details, including the following:

   a) mailing address;
   b) Singapore registered mobile phone number; and
   c) email address.

   You understand that if you do not update your contact information you are at risk of not receiving transaction notifications from us.

Protection of Access Codes

4. You must protect any access code that we provide to you to authenticate any payment transaction. The following list (not exhaustive) are examples of access codes that we may send to you or the account user:

   a) Personal identification number, password or code;
   b) Internet banking authentication code;
   c) Telephone banking authentication code;
   d) Code generated by an authentication device e.g. token; and
   e) Code sent by us through text messages such as SMS.

5. You and any account user must not to do any of the following:

   a) Voluntarily disclose any access code to any third party, including any of our staff.
   b) Disclose the access code in a recognisable way on any payment account, authentication device or any container for the payment account.
   c) Keep a record of any access code in a way that allows any third party to easily misuse the access code.

6. You must always keep the record of an access code in a secure electronic or physical location accessible or known only to the account user which is a place where the record is unlikely to be found by a third party.

Protection of Account

7. You and any account user should do all of the following when a device (e.g. handphone, desktop, laptop, tablet or such other device) is used to access the protected account:

   a) download our mobile application(s) only from official sources. Examples of official sources include Apple App Store and Google Play Store, which may change from time to time;
   b) update the device's browser to the latest version available. Examples of a browser include Chrome, Safari, Internet Explorer, which may change from time to time;
   c) patch the device's operating system with regular security updates provided by the operating system provider. Examples of an operating system include Windows, Macintosh OS, iOS and Android OS, which may change from time to time;
   d) install and maintain the latest anti-virus software on the device, where applicable;
   e) use strong passwords, such as a mixture of letters, numbers and symbols or strong authentication methods such as facial recognition or fingerprint authentication methods;
   f) not root or jailbreak the device; and
   g) not download or install applications from third-party websites outside official sources.

   Please note that the above list is the minimum you should do to protect your protected account with us. The list not exhaustive and we may change or supplement the list from time to time. You must ensure that you, as an account holder, inform all the authorised users of the security instruction or advice provided by us to you.

8. You should read the content of the messages containing any access codes and verify that the stated recipient or activity is intended prior to completing any transaction.

9. You should refer to official sources to obtain our website address and phone number. Examples of official sources include the MAS Financial Institutions Directory, our mobile application and the back of cards (e.g. credit card, debit card or charge card), which may change from time to time.

10. You should not click on links or scan Quick Response codes ("**QR codes**") purportedly sent by us unless you are expecting to receive information on products and services via these links or QR codes from us.

11. You should read the risk warning messages sent by us before proceeding to confirm the performance of high-risk activities. High-risk activities include, but are not limited to:

    a) adding of payees;
    b) increasing the transaction limits for outgoing payment transactions;
    c) disabling transaction notifications from us; and
    d) changing your contact information including mobile number, email address and mailing address.

    If you require more information on the risks and implications of performing high-risk activities, you should contact us prior to performing these activities. When you proceed to perform the high-risk activities, you are deemed to have understood the risks and implications of doing so.

Unauthorised transactions

12. You must report any unauthorised transactions to us as soon as you receive any transaction notification alert for any unauthorised transaction. If you are unable to report the unauthorised transaction immediately, you should provide us with reasons for the delay when asked. In any event, you must report any unauthorised transactions to us no later than 30 calendar days after you receive any transaction notification alert for any unauthorised transaction.

13. The unauthorised transaction report must be made by calling the Maybank Contact Centre on the following numbers:

    a. Local: 1800 629 2265
    b. Overseas: (65) 6533 5229

14. The unauthorised transaction report must contain the following information:

    a) the protected account that is affected, including your affected accounts with other financial institutions if any;
    b) the account holder identification information;
    c) the type of authentication device, access code and device that is used to perform the payment transaction;
    d) the name or identity of any account user for the protected account that was used;
    e) details on whether or not the protected account's authentication device or access code was lost, stolen and misused and if so, the:

i. date and time of loss or misuse;
ii. date and time that the loss or misuse was reported to us; and
iii. date, time and method that the loss or misuse was reported to the police;

f) if access code is applicable to the protected account:
   i. how the account holder / user recorded the access code; and
   ii. whether the account holder / user had disclosed the access code to anyone.

g) any other information about the unauthorised transaction that we may require.

You will receive an acknowledgement of the unauthorised report from us either via email or via SMS.

Make a police report

15. In addition to informing us of an unauthorised transaction report you should also make a police report as soon as practicable for the unauthorised transaction in order to facilitate the investigation process, or if you suspect that you are a victim of scam or fraud. Please note that the timeline to complete the investigation process, as stated in the Guidelines, will only start once a valid police report is made. You must also furnish the police report to us within 3 calendar days of our request in order to facilitate the investigation process.

Our Responsibilities

Cooling off period for high-risk activities

16. We will impose a cooling off period of at least 12 hours where high-risk activities cannot be performed, when a digital security token is activated on a device.

Notifications for high-risk activities

17. When we send you notifications for performance of high-risk activities or activation of your digital security token we will:
   a) send the notifications to every account contact selected by you;
   b) ensure that the notifications will be sent to you on a real time basis;
   c) send the notifications to you either by SMS or email (even if you have already received a push notification via any Maybank app);
   d) ensure that the notifications contain relevant information on the performance of the high-risk activities or activation of your digital token, e.g. information on payee added, new transaction limits or a change in contact details; and
   e) include in the notifications a reminder to you to contact us if you did not perform the high-risk activity or activate the digital security token.

Transaction Notifications

18. Provided that you have fulfilled your obligations stated in this Policy and the Terms and Conditions, we will send you notifications for all payments you make through electronic means. These include fund transfers, debit/credit card transactions and bill payments. At this point in time, we will not send you notifications for incoming transactions unless you opt-in to receive such notifications.

19. When we send you a transaction notification we will:

a) send the transaction notifications to every account contact selected by you;
b) ensure that transaction notifications will be sent to you on a real time basis;
c) send transaction notifications to you either by SMS or email (even if you have already received a push notification via any Maybank app);
d) ensure that transaction notifications contain the following information:
    i. Information that allows you to identify the protected account such as the account number;
    ii. Information that allows you to identify the recipient whether by name or by other credentials such as the recipient's account number;
    iii. Information that allows us to later identify you, the protected account, and the recipient account;
    iv. Transaction amount;
    v. Transaction time and date;
    vi. Transaction type; and
    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.

We will ensure that the information provided still allows you to identify the transaction as being an authorised or unauthorised transaction.

Your instructions to us

20. Notwithstanding our obligations to send you transaction notifications as set out in this Policy, you can provide us with instructions relating to how you would prefer to receive the transaction notifications. For example, we may provide outgoing transaction notifications to you for amounts higher than S$0.01 as notified by you to us.

21. The instructions you provide to us in relation to receiving the transaction notifications should be submitted in a specified form and mode notified by us to you.

22. Please note that where you have already provided us with instructions to send transaction notifications to you, prior to the issuance of this Policy, we will continue to follow your instructions until you notify us otherwise in writing.

We will inform you of the details of any recipient

23. Where transactions are made by way of internet banking, any mobile phone application or device arranged for payment transactions, including a payment kiosk, we will provide an onscreen opportunity for the person who is making the transaction to confirm the payment transaction and recipient credentials before we execute any authorized payment transaction.

The onscreen opportunity will contain the following information:

a) information that allow the account user to identify protected account to be debited;
b) the transaction amount; and
c) the credentials of the intended recipient (e.g. account number, name registered for receiving payments, identification number and phone number).

Investigation Process

24. We will resolve all claims made by you in relation to an unauthorised transaction in a fair and reasonable manner. In the event that the a claim made by you falls under this Policy we will complete an investigation within 21 business days for straightforward cases or 45 business days for complex cases, provided that you have submitted any claim in accordance with your obligations under this Policy.

25. Please note that any investigation will only commence upon submission of police report for unauthorised transaction. Submission of police report after 5pm of a business day would only commence investigation on next business day. Submission of police report over the weekend will only commence investigation on the next business day.

26. All investigations will be completed in a transparent manner, when requested we will provide you with the relevant information we have of all the unauthorised transactions of your protected account, including transactions dates, transaction timestamps and the receiving party.

27. In the event that you do not agree with the outcome of our investigation, you may proceed to commence other forms of dispute resolution.

Liability

The following section on liability does not apply to any credit card, charge card or debit card issued by us.

Where you are liable

28. You are liable for actual loss arising from an unauthorised transaction where any account user's recklessness was the primary cause of the loss. Recklessness would include the situation where the account user deliberately did not comply with their obligations under this Policy. The actual loss that you are liable for is capped at any applicable transaction limit or daily payment limit that we have agreed to.

29. For the avoidance of doubt, where any account user knew of and consented to a transaction, such transactions are not considered to be an unauthorised transaction notwithstanding that the account holder may not have consented to the transaction. The account holder of the protected

account is liable for all authorised transactions up to any applicable transaction limit or daily payment limited that we have agreed to.

Where we are liable

30. You are not liable for any loss arising from an unauthorised transaction if the loss arises from any action or omission by us and does not arise from any failure by any account user to comply with any section of this Policy and the Guidelines.

31. An act or omission by us includes the following:

a) Fraud or negligence by us, our employees, our agents or any outsourcing service provided contacted by us to provide services through the protected account;
b) Non-compliance by us or our employees with any requirement imposed by the Monetary Authority of Singapore on us in respect of its provision of any financial service; and
c) Non-compliance by us of our responsibilities set out in the Guidelines and this Policy.

32. You as the account holder are not liable for the first $1,000 of loss arising from an unauthorised transaction, if the loss arises from any action or omission by any third party and does not arise from any failure by any account user to comply with any of their duties under this Policy.

33. Please note that where our Terms and Conditions stated a lower amount for your liability in the same situations described in this section we will fulfill our obligations as stated in the Terms and Conditions.

34. Where the protected account is a joint account, the liability for losses set out in this section apply jointly to each account holder in a joint account.

We will make reasonable efforts to recover sums sent in error by the account user

35. Where you have informed us that you or an account user has initiated a payment transaction from a protected account such that money has been transferred to the wrong recipient ("**erroneous transaction**"), we will inform the wrong recipient's financial institution of the erroneous transaction and make reasonable efforts to recover the erroneous transaction, such as:

a) Informing the wrong recipient's financial institution of the erroneous transaction within two business days from receiving the information from you; and
b) Following up with the wrong recipient's financial institution for a response and further information within seven business days of making the initial contact with the recipient's financial institution.

Where we are the financial institution of the wrong recipient we will:

c) Inform the recipient of the erroneous transaction and all necessary information that would allow the recipient to determine if the transaction was indeed erroneous;
d) Ask the recipient for instructions on whether to send the sum sent in error back to the account holder;

e) Inform the recipient that his retention or use of sums transferred to him erroneously where he has had notice of the erroneous transaction is an offence under the Penal Code; and
f) Within five business days from receiving the initial information on the erroneous transaction, we will ask the recipient for instructions to send the money back and update the account holder's financial institution of that response, including nil responses.

Please note that the timelines given above are for straightforward cases we will do our best to respond within the timelines, however it may take longer for complicated cases.

36. Where you are the wrong recipient who has noticed an erroneous transaction and requests to return the sum sent in error we will:

a) If confirmation from the account holder's financial institution is needed before we can return the sum sent in error, we will:
   i. Inform the account holder's financial institution of the erroneous transaction;
   ii. Within seven business days of informing the account holder's financial institution, we will update you. If we are unable to return the sum sent in error, we will advise you on the next steps.
b) If confirmation from the account holder's financial institution is not needed before we can return the sum sent in error, we will return the sum sent in error within nine business days of receiving the necessary information from you on the erroneous transaction, and update you.
c) In the event we are unable to obtain confirmation from the account holder's financial institution, and we have assessed the case to be closed as a result, we will inform you of the decision and advise you on the next steps, which may include making a police report if you suspect that the funds transferred by the sender are illicit in nature.

Please note that the timelines given above are for straightforward cases we will do our best to respond within the timelines, however it may take longer for complicated cases.

37. Where you are the account holder, for the purposes of assisting us to recover an erroneous transaction, you must provide us with the following:

a) all the information set out in paragraph 14 (a) to (d);
b) the recipient's unique identifier, including account number, identification number, name or other credentials entered by the account user; and
c) the date, time, amount and purpose of the erroneous transaction insofar as such information is known to the account user.

38. Where you are the wrong recipient, for the purposes of assisting us to return sums sent in error, you must provide us with the following:

a) the protected account(s) to which the erroneous transactions have been made;
b) the date, time and amount of the erroneous transaction to the extent of your knowledge; and
c) any other relevant information about the erroneous transaction that you know.

Changes to this Policy

Please note that we may update this Policy from time to time to ensure that this Policy is consistent with our future developments, industry trends and/or any changes in legal or regulatory requirements. If there are material changes to this Policy, we will notify you by posting such changes on our website or by sending you a notification directly.

Last updated 16 December 2024