IMPORTANT NOTICE

FOR YOUR IMMEDIATE ACTION: PLEASE UPDATE YOUR CONTACT DETAILS TO RECEIVE TIMELY NOTIFICATION ALERTS FROM UOB AND KNOW YOUR DUTIES UNDER THE E-PAYMENT USER PROTECTION GUIDELINES

As part of our efforts to protect you from unauthorised or erroneous payment transactions, we will be providing notification alerts for all outgoing e-payment transactions relating to **sole proprietor account(s) owned by individuals**. This service will be provided to you from 30 June 2019, in addition to any existing transaction alerts services that you may have signed up for.

To receive your notification alerts, it is important for you to inform us of your selected mode of notification (SMS or email) and contact details. Otherwise, you may not be able to receive transaction notifications relating to your account(s).

Please refer to the Frequently Asked Questions for important information on:

- your duties under the E-Payment User Protection Guidelines issued by The Monetary Authority of Singapore;how your liability for unauthorised transactions will be affected based on your transaction alert preferences;
- Agreement for Sole Proprietors, which should be read together with the Terms & Conditions Governing Accounts and Services (Non-individuals)
  uob.com.sg/solepropagreement

If you have any queries, please feel free to contact us at 1800 226 6121 (Monday to Fridays, 9.00am to 6.30pm, excluding public holidays).

FREQUENTLY ASKED QUESTIONS

PLEASE NOTE THAT THE INFORMATION STATED BELOW IS INTENDED TO SERVE AS A GUIDE ONLY AND IS NOT MEANT TO BE EXHAUSTIVE. IT IS THEREFORE IMPORTANT THAT YOU READ THE E-PAYMENT USER PROTECTION GUIDELINES (THE "GUIDELINES") ISSUED BY THE MONETARY AUTHORITY OF SINGAPORE, A COPY OF WHICH MAY BE ACCESSED HERE.

1. What is the purpose of the E-Payments User Protection Guidelines?

These are guidelines issued by the Monetary Authority of Singapore, which took effect from 30 June 2019, with the aim to offer guidance on a common baseline protection for individuals or sole proprietors from losses arising from isolated unauthorised transactions or erroneous transactions from the protected accounts of these account holders.

2. What is a protected account?

A protected account means any payment account that

a) is held in the name of one or more persons who are either individuals or sole proprietors;
b) is capable of having a balance of more than S$1000 (or equivalent amount expressed in any other currency) at any one time, or is a credit facility; and
c) is capable of being used for electronic payment transactions.

3. What are your duties as an Account holder/ Account user?

Account holders and users shall fulfill the following duties:

a) Provide contact information, opt to receive all notifications alerts and monitor notifications

i. The Account holder shall provide the Bank with a complete and accurate Singapore mobile phone number and email address.

ii. The Account holder shall be responsible for:

- enabling notification alerts on any device used to receive notifications alerts from the Bank;
- opting to receive all notification alerts via SMS, email or in-app/push notification for all outgoing payment transactions (of any amount that is above the transaction notification threshold set by the account holder), activation of digital security token, conduct of high-risk activities; and
- monitoring the notifications alerts sent to the Account contact.

- Inform account users of the security instructions or advice provided by the Bank to the account holder. An account user should where possible follow security instructions or advice provided by the Bank to the account holder.

b) Protect access codes

i. The Account user shall not do any of the following:

- voluntarily disclose any access code to any third party, including the staff of the Bank, staff from other banks, or government officials;
- disclose the access code in a recognisable way on any payment account, authentication device, or any container for the payment account; or
- keep a record of any access code in a way that allows any third party to easily misuse the access code.

ii. If the Account user keeps a record of any access code, he should make reasonable efforts to secure the record, including:

- keeping the record in a secure electronic or physical location accessible or known only to the Account user; and
- keeping the record in a place where the record is unlikely to be found by a third party.

c) Secure access to protected account

An Account user shall take all necessary steps to secure access to the protected account including but not limited to: -

i. download the Bank's mobile application(s) only from official sources such as Apple App Store, Google Play Store;
ii. update the device's browser such as Chrome, Safari, Internet Explorer, Firefox to the latest version available;
iii. patch the device's operating systems such as Windows operating system (OS), Macintosh OS, iOS and Android OS, with regular security updates provided by the operating system provider;
iv. install and maintain the latest anti-virus software on the device, where applicable; and
v. use strong passwords, such as a mixture of letters, numbers and symbols or strong authentication methods made available by the device provider such as facial recognition or fingerprint authentication methods;
vi. not root or jailbreak the devices used; and
vii. not download and install applications from third-party websites outside official sources ("sideload apps"), in particular unverified applications which request device permissions that are unrelated to their intended functionalities.

An Account holder shall inform all Account users of the security instructions or advice provided by the Bank from time to time. An Account user should where possible follow security instructions or advice provided by the Bank to the Account holder.

d) Read content of the messages sent with access codes before completing payment transactions or high-risk activities

An Account user should read the content of the messages sent with access codes (such as one-time passwords sent via SMS or equivalent push notifications via the official mobile application of the Bank) and verify that the stated recipient or activity is intended prior to completing payment transactions or high-risk activities.

e) Refer to official sources to obtain website addresses and phone numbers:

- An account user of a protected account should refer to official sources, such as the MAS Financial Institutions Directory ("FID"), and the Bank's mobile application or the back of cards, e.g. credit card, debit card or charge card ("official sources") to obtain the website addresses and phone numbers ("contact details") of the responsible FI.
- To contact the Bank, an account user should use the contact details that were obtained from official sources.
- An account user should not click on links or scan Quick Response codes ("QR codes") purportedly sent by the Bank unless he is expecting to receive information on products and services via these links or QR codes from the Bank. The contents of these links or QR codes should not directly result in the account holder providing any access code or performing a payment transaction or high-risk activity.

f) Understand the risks and implications of performing high-risk activities:

- An account user should read the risk warning messages sent by the Bank before proceeding to confirm the performance of high-risk activities.
- If an account user does not understand the risks and implications of performing high-risk activities, he should access the Bank's website for more information on these activities or contact the Bank prior to performing these activities. When the account user proceeds to perform the high-risk activities, he is deemed to have understood the risks and implications as presented by the Bank.

g) Report unauthorised activities

The Account holder shall report any unauthorised activity to the Bank as soon as practicable, and no later than 30 calendar days after the receipt of any notification alert for any unauthorized activity (such as transactions, high-risk activities, and the activation of a digital security token, that has not been initiated by the account holder or with the account holder's consent). Where the Account holder is not able to report the unauthorised activity to the Bank as soon as he receives any notification alert for any unauthorised activity or no later than 30 calendar days after the receipt of any transaction notification alert, the Account holder should provide the Bank with reasons for the delayed report. The report shall be made via such channels the Bank may designate from time to time for such incidents.

h) Activate the "kill switch" to promptly to block further mobile and online access to the protected account

- The account holder should activate the kill switch function by calling the Bank's Fraud Hotline to block further mobile and online access to the account as soon as practicable, after he is notified of any unauthorised transactions and has reason to believe that the account has been compromised.

i) Provide information on unauthorised transaction

The Account holder shall within a reasonable time provide the Bank with any of the following information:

i. the protected account(s) affected, including the account holder's affected accounts with other financial institutions if any
ii. the Account holder's identification information;
iii. the type of authentication device, access code and device used to perform the payment transaction;
iv. the name or identity of any Account user for the protected account;
v. whether a protected account, authentication device, or access code was lost, stolen or misused and if so:
- the date and time of the loss or misuse,
- the date and time that the loss or misuse, was reported to the Bank, and
- the date, time and method that the loss or misuse, was reported to the police;

vi. where any access code is applicable to the protected account,
- how the Account holder or any Account user recorded the access code, and
- whether the Account holder or any Account user had disclosed the access code to anyone; and

vii. any other information about the unauthorised transaction that is known to the Account holder, such as:
- a description of the scam incident, including details of the communications with the suspected scammer(s);
- details of the remote software downloaded (if any) as instructed by the scammer(s);
- whether the account holder has received any OTPs and/or transaction notifications sent by the responsible FI, and where applicable/possible a confirmation from telecommunication operators to verify the receipt status only if the account holder is able to obtain it; and
- suspected compromised applications (if any) in the account user's device.

j) Make police report

The Account holder shall make a police report as soon as practicable if the Bank requests such a report to be made to facilitate its claims investigation process, or if the account holder suspects that he is a victim of scam or fraud. The Bank may require the police report to be furnished before the Bank begins its claims investigation process. The account holder should cooperate with the Police and provide evidence, as far as practicable. The account holder should also furnish the police report to the Bank, within 3 calendar days of the Bank's request to do so, in order to facilitate the Bank's claims investigation process.

4. How will I receive transaction notifications?

The transaction notifications relating to all the accounts under the sole proprietorship will be sent by way of SMS or email to a mobile phone number or email address that you have provided. Each transaction notification will contain information relating to the relevant transaction such as the transaction date and time and the transaction amount.

Please note that transaction notifications for outgoing e-payment transactions from your credit and/or debit cards shall be sent to the mobile phone number(s) of your appointed card user(s).

5. What are my liabilities for losses arising from unauthorized transactions?

a) Account holder is liable for actual loss

The Account holder shall be 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 any Account user deliberately did not comply with the duties of Account holders and Account users in the E-payments User Protection Guidelines issued by Monetary Authority of Singapore. The Account user is expected to provide information to the Bank to determine whether any Account user was reckless. The actual loss that the Account holder is liable is capped at the applicable transaction limit or daily payment limit, if any on the protected account.

b) Account holder is not liable for any loss

The Account holder shall not be liable for any loss arising from:

- an unauthorised transaction if the loss arises from any action or omission by the Bank and does not arise from any failure by any Account user to comply with any duties of Account holders and Account users set out in the E-payments User Protection Guidelines issued by Monetary Authority of Singapore.

  For more information on the user protection guidelines and duties of Financial Institution, refer to the latest E-Payments User Protection Guidelines published by the Monetary Authority of Singapore. (https://www.mas.gov.sg/regulation/guidelines/e-payments-user-protection-guidelines)

- an unauthorised transaction (where the account holder of a protected account is not liable for the first $1,000 of the loss) 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 duties of Account holders and Account users set out in the E-payments User Protection Guidelines issued by Monetary Authority of Singapore. The account holder will be liable for the amount of unauthorized transactions that exceed the first $1,000. In other words, if the amount of such unauthorised transaction is less than S$1,000, then the Bank shall only be liable for the actual amount of such unauthorised transaction. If the amount of such unauthorised transaction exceeds S$1,000, then you shall be solely liable for the amount in excess of the first S$1,000 and the Bank shall have no liability to you in excess of the first S$1,000.

The above is not applicable to credit card, charge card or debit card issued by the Bank and all transactions made by way of credit card, charge card or debit card. For more information on your liability relating to credit card, charge card or debit card, please refer to the following:

For Credit Card: https://www.uob.com.sg/corporate/useful/corporate-cardmember-agreement.page

For Business Debit Card: https://www.uob.com.sg/web-resources/business/pdf/business/transact/business-debit-card/bizdebit_c.pdf

6. How do I update my mode of transaction notification and/or contact for outgoing e-payment transactions?

For transaction notifications relating to your bank accounts, please use the following form, which is also available on our website (www.uob.com.sg).

Please note that transaction notifications from your credit and/or debit cards will be sent to the mobile phone number(s) of your appointed carduser(s). To update contact details, carduser(s) may log in to UOB Personal Internet Banking or visit any of our branches island-wide.

7. Can I select more than one contact for the account held under the sole proprietorship?

The transaction notifications are availed to only a single contact. For example, if you hold 3 accounts under the sole proprietorship, the transaction notifications for all 3 accounts will be sent to the same contact.

8. I have registered for e-Alerts Services and/or BIBPlus notifications for my accounts. Will these alerts be sent to me after 30 June 2019?

Yes, these will continue to be sent to you in addition to the notifications for outgoing e-payment transactions. Hence, you may receive multiple notifications for the same transaction.

If you do not want to receive transaction notifications via eAlerts, please use the following eAlerts maintenance form to exclude the outgoing eAlerts transaction notifications:

https://www.uob.com.sg/web-resources/corporate/pdf/corporate/transaction-banking/ealerts/ealert-maintenance-form.pdf

If you do not want to receive BIBPlus notifications, please log into BIBPlus and modify your alerts setting.

9. Can I set a threshold for the notifications on outgoing e-payment transactions from my CASA accounts?

Currently, the default threshold is S$0.01. You can set a higher threshold for the transaction notifications. The threshold set will be in Singapore Dollars (SGD) and the SGD equivalent threshold will be applied to any e-payment transactions made from foreign currency current/savings accounts that you may hold.

Please note that you will only receive notifications for transaction amounts that are equal or higher than the threshold that you have selected. If you are not alerted to unauthorized transactions below your threshold, you may not be able to report these unauthorized transactions promptly or to take steps to secure your account and prevent further losses in a timely manner. This could affect the extent to which you are liable for losses arising from the unauthorised transactions. Please take into consideration your responsibilities and liabilities under the E-payments User Protection Guidelines for unauthorized transactions, when deciding on your notification alerts thresholds.

Steps to update the threshold for the outgoing e-payment transactions:

1. Download this form.

2. On page 3 of the form, fill up section I (Customer's Particulars) and indicate your preferred notification threshold under Section III (Threshold setting/Opting Out) of the form.
3. Sign on the form and fill in your personal details at bottom right corner.
4. Submit the form to the nearest branch.

10. How do I activate the "kill switch" to disable mobile or digital access to my accounts?

Call our 24-hour Fraud Hotline at 6255 0160, press 1 to report the case and activate the "kill switch" to disable your digital access.

You will need to speak to our Customer Service Officer to authenticate your identity and provide us with the Organisation ID and User ID of the compromised account(s) for us to disable mobile or digital access to these account(s).

11. Will I be prompted to confirm my payment instructions and recipient details before the transaction is executed?

Where applicable, the Bank will provide an onscreen opportunity, which will contain information relating to the relevant transaction and recipient details such as protected account to be debited, the intended transaction amount, recipient's account number or name for you to confirm the payment transaction and the recipient credentials before the relevant payment transaction is executed by the Bank.

12. How can I report an unauthorized or erroneous transaction?

Please visit any of our branches or call our Corporate Call Centre at 1800 226 6121 (Monday to Fridays, 9.00am to 6.30pm, excluding public holidays) to report any unauthorized or erroneous transactions as soon as practicable after the receipt of any transaction notification alert for any unauthorized or erroneous transaction. You will receive a written acknowledgement of the report and no fee will be charged by the Bank for making the report.

13. I have reported an unauthorized transaction. When will I know the outcome of the bank's assessment of my claim?

The Bank will complete our assessment of your claim within 21 business days upon receiving sufficient information from the account holder to complete the investigation for straightforward cases. For complex cases, this may take up to 45 business days. Complex cases may include cases where any party to the unauthorized transaction is resident overseas or where insufficient information has been provided to bank for purposes of the claims investigation. If the Bank's assessment is that the account holder is not liable for any loss arising from the unauthorized transaction, the Bank will credit the account holder's protected account as soon as this conclusion is reached.

14. I have reported an erroneous transaction. When will I know the outcome of the bank's recovery of my claim?

The Bank will make reasonable efforts to facilitate communication between you and the recipient with the aim to improve your chances of recovering the payment amount sent through the erroneous transaction. However, the Bank may take longer to convey instructions in complex cases such as where any party to the transaction is resident overseas or where the Bank has not received sufficient information from you to convey instructions.

15. What are the amendments to Terms and Conditions Governing Accounts and Services (Non-Individuals)?

With effect from 16 December 2024, we have revised the Agreement for Sole Proprietorships to reflect the latest revisions made to the E-Payment User Protection Guidelines published by the Monetary Authority of Singapore on 24 October 2024. The Agreement for Sole Proprietors should be read in addition to the Terms & Conditions Governing Accounts and Services (Non-individuals).

uob.com.sg/solepropagreement