Important Information on the E-Payments User Protection Guidelines ("Notice")

The Monetary Authority of Singapore ("MAS") has issued the E-Payments User Protection Guidelines ("Guidelines") which spells out the roles and responsibilities of banks and our customers when conducting activities related to e-payments. Any term used in this Notice shall have the same meaning as defined in the Guidelines, unless expressly defined otherwise.

Please read the summary of the revised Guidelines below to understand the rights and obligations of CIMB Bank Berhad, Singapore Branch ("CIMB Bank", "CIMB" or the "Bank") as well as your rights and obligations as an account holder (including a joint account holder and a supplementary credit card holder) under the Guidelines. For complete and updated information on the Guidelines' requirements, it is therefore important that you read and understand the latest E-Payments User Protection Guidelines issued by MAS.

Please note this should be read together in conjunction with Terms and Conditions Governing Electronic Banking Services, Terms and Conditions Governing the Operations of Deposits Accounts and CIMB Credit Cards Cardmember's Agreement.

Part A: Duties of account holders and account users

Please be aware of your responsibility as an account holder and adopt safe banking measures to protect your protected account[1] (e.g. individual bank accounts, ATM card, credit card and other unsecured credit facilities) from unauthorised or erroneous transactions.

Please also note some of the duties below also apply to account users, who are persons authorised to initiate, execute or both initiate and execute payment transactions using your protected account. Please also inform them of their applicable duties to best safeguard your protected account. The degree of responsibility exercised here, including without limitation the setting of your transaction notification preferences, will affect the liability for losses arising from unauthorised transactions as set out in Part C.

1. Provide contact information, opt to receive all outgoing transaction notifications and monitor notification alerts for transactions, activation of digital security token, and the conduct of high-risk activities[2].

   - You should minimally provide us with your mobile number or email, so that you can receive the opted notification alerts by SMS or email. You must also ensure that contact information provided to us is complete and up-to-date.
   - You should opt to receive your 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), activation of digital security token and the conduct of high-risk activities made from your protected account.
   - You should enable notification alerts on all your device(s) used to receive notification alerts from us.
   - You should monitor all the notification alerts received as the Bank may assume that you will monitor such notification alerts without further reminders or repeat notifications.

[1] *A "**protected account**" means any payment account that:*
(a) is held in the name of one or more persons, all of whom are either individuals or sole proprietors;
(b) is capable of having a balance of more than S$1,000 (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.*

[2] *"**high-risk activities**" include, but are not limited to—*
(a) adding of payees to the account holder's payment profile;
(b) increasing the transaction limits for outgoing payment transactions from the payment account;
(c) disabling transaction notifications that the Bank will send upon completion of a payment transaction; and
(d) change in the account holder's contact information including mobile number, email address and mailing address.

2. Protect access codes[3] and secure access to protected account.

- You must ensure that you check and verify the transaction/activity details and/or recipient credentials in the access code messages carefully before confirming any payment transactions or high-risk activities;
- You must not voluntarily disclose your access code (e.g. one-time-password (OTP), online banking and mobile app login username and password, etc.) to any third party, including the staff of CIMB Bank or any other government authority;
- You must not disclose your access code in a recognisable way on any payment account, authentication device, or any container for the payment account;
- You must not keep a record of any access code in a way that allows easy access by third party to easily misuse the code.
- If you keep a record of any access code, you must make reasonable efforts to secure such record.
- You must use strong passwords, such as a mixture of letters, numbers and special characters or strong authentication methods made available by the device provider such as facial recognition or fingerprint authentication methods.
- You must avoid rooting or jailbreaking your mobile device as it poses potential risks to viruses and malicious software, making it vulnerable to fraudulent attacks. You are advised to download CIMB Bank's Mobile Banking application only from authorised sources such as Apple App Store or Google Play Store. Additionally, do not download and install applications from third-party websites outside official sources ("sideload apps"), unverified applications which request device permissions that are unrelated to their intended functionalities.
- You must keep your browser and operating system up to date. You should make regular checks on your software vendor's website and apply any new security patches as soon as possible to ensure you have the most updated security features available.
- You must avoid installing software or running programmes of unknown origin and avoid opening email attachments from any source you do not know or trust. We also recommend that you scan all email attachments for viruses and delete junk and chain emails on a regular basis. Also, never call a number appearing on an email you suspect is fraudulent.

---

[3] *"**access code**" means a password, code or any other arrangement that the account user must keep secret, that may be required to authenticate any payment transaction or account user, and may include any of the following:*
(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) code sent by the Bank by phone text message such as Short Message Services ("SMS"), email or in-app/push notification

- You should protect your devices from virus and malware by installing up-to-date anti-virus and anti-malware software. You should also install anti-spyware software, which may already be bundled together with your anti-virus software.
- You should install a personal firewall to provide a protective shield between your computer/mobile device and the Internet.
    - Spyware is a general term for hidden programs on your computer/mobile devices that track what you are doing on your computer/mobile devices. Spyware is often bundled together with file sharing, email virus checking or browser accelerator programs, and it is installed on your computer/mobile devices without your knowledge to intercept information about you and your computer/mobile devices. The type of information gathered can include personal Internet usage, and in some instances, confidential data such as passwords. You can download and run a specialist program designed to help identify and remove threats from spyware. Like an anti-virus program, it also needs to be regularly updated in order to recognise the latest threats.

3. Read messages from us before completing payment transactions or high-risk activities.

- You must check carefully the instruction details before executing or completing any transactions or high-risk activities. You should also inform all account users of security instructions or advice provided us.
- You and any account user should read the risk warning messages from CIMB Bank and understand the risks and implications before proceeding to confirm the performance of the high-risk activities. You and any account user should always refer to our official website or contact us for more information if unsure. By proceeding to perform the high-risk activities, you or (as the case may be) the account user is deemed to have understood the risks and implications as presented by the Bank.

4. Refer to official sources to obtain the Bank's website address and contact numbers.

- You and any account user should always refer to official sources such as MAS' Financial Institutions Directory ("FID") or the back of CIMB Bank cards to obtain the Bank's website address and contact numbers.
- You and any account user should always refer to the Bank's website address and contact numbers obtained from official sources to contact us. Please always type our URL https://www.cimb.com.sg into the browser's address bar or use our CIMB Mobile App.
- You and any account user should not click on links or scan QR codes purportedly sent by the Bank unless you and the account user are expecting to receive information on products and services via these links or QR codes from us. The contents of these links or QR codes

should not directly result in you providing any access code or performing a payment transaction or high-risk activity.

5. Take appropriate measures in potential instances of unauthorised activities, scam or fraud.

- You should activate the kill switch provided by CIMB Bank to block further mobile and online access to the protected account immediately, after you have reason to believe that your account has been compromised, or if you are unable to contact CIMB Bank.
- You must report to CIMB Bank immediately (and no later than 30 calendar days) via one of the following channels if you (a) detect an erroneous and/or unauthorised activities; or (b) receive a notification alert for any unauthorised activity, e.g., transactions, high-risk activities, and the activation of a digital security token, that has not been initiated by you:

    a. Customer Service Hotline
    9.00am - 7.00pm, daily
    +65 6333 7777
    b. Credit Card Call Centre
    24-hours, daily
    +65 6333 6666
    c. Customer Service Email – AtYourService@cimb.com
    d. Our branch:
    Raffles Place Branch
    30 Raffles Place, #03-03, Singapore 048622

- You should promptly provide CIMB Bank with all the information we may request to facilitate our investigation of the unauthorised transactions. Such information may include:
    a) Your protected account(s) that is/are affected, including affected accounts with other financial institutions (if any),
    b) Your identification information,
    c) Your type of authentication mode and device that is used to perform the payment transaction,
    d) The name or identity of any account user for the protected account
    e) Details on whether the protected account's authentication device or access code was lost, stolen and misused and if so, the:
        - Date and time of loss or misuse;
        - Date and time that the loss or misuse was reported to us; and
        - Date, time and method that the loss or misuse was reported to the police.
    f) Information of access code (if applicable to the protected account):
        - How you or any other account user recorded the access code; and

- Whether you or any other account user had disclosed the access code to anyone.

g) Other details related to the unauthorised transaction that is known to you:
   - 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);
   - Details whether you have received any OTPs and/or transaction notifications sent by the Bank and where applicable/possible a confirmation from telecommunication operators to verify the receipt status only if you are able to obtain it; and
   - Suspected compromised applications (if any) in your device.

- You may be required to provide CIMB Bank with reasons for the delay in the event that you are unable to report to CIMB Bank within 30 calendar days.
- You should make a police report immediately if you suspect that you are a victim of a scam or fraud and cooperate with the Police and provide evidence as far as practicable. You should also furnish the police report to CIMB Bank, within 3 calendar days of our request to do so, in order to facilitate our claims investigation process.

Part B: Duties of CIMB Bank

Part B does not apply to CIMB Bank in respect of any credit card, charge card or debit card issued by CIMB Bank, except for **Clauses under Part B: 1, 2, 4, 6 and 7**.

1. Clearly inform account holder of user protection duties
    - We will inform you of your account protection duties, including providing such information on our website or mobile application, and in the Bank's terms and conditions. Such user protection duties comprise of:
        a) Duties of the account holder and account user set out in **Part A: Duties of account holders and account users**; and
        b) Duties of the Bank as set out **in Part B: Duties of CIMB Bank**.

2. Not send clickable links or QR codes via email or SMS, or phone numbers via SMS
    - We will NOT send clickable links or QR codes via email or SMS to the account user unless:
        a) it is a link or QR code that only contains information and does not lead to a (i) website where the account user provides his access codes or performs any payment transaction or (ii) platform where the account user is able to download and install apps; and
        b) the account user is expecting to receive the email or SMS from CIMB Bank.
    - We will not send phone numbers via SMS to you unless you are expecting to receive the SMS from CIMB Bank.
    - We will ensure our website address is listed on MAS' Financial Institutions' Directory ("FID"), and that our contact details reflected on MAS' FID and other official sources are up to date.

3. Digital security token activation and High-risk activities
    - A cooling off period of at least 12 hours is imposed where high-risk activities cannot be performed ("cooling off period"), when a digital security token is activated on a device.
    - We will inform the account user of the risks and implications of performing high-risk activities and obtain additional confirmation, at the point before you perform the high-risk activities.
    - We will provide notification alerts on a real-time basis, that fulfil the following criteria, to you as the account holder of a protected account, when your digital security token is activated and any high-risk activities are performed:

a) The notification alert will be conveyed by way of SMS, email or in-app/push notification.
b) The notification alert will be sent to your existing account contact with the Bank.
c) The notification alert will contain details relevant to the digital security token provisioning and activation or high-risk activity, such as information on the payee added, new transaction limits or a change in contact details.
d) The notification alert will contain a reminder for the account holder to contact the Bank if the digital security token provisioning and activation or high-risk activity was not performed by you.

4. Outgoing transactions notification alerts

- In respect of all outgoing payment transactions (of any amount in accordance with the transaction notification threshold) made from the protected account, when a transaction notification is sent to you, we will:

    a) Send the transaction notification to the account holder's contact, subject to our Terms and Conditions Governing E-Alerts;
    b) Ensure that transaction notifications will be sent to you on a real-time basis, as soon as practicable through SMS, email or in-app/ push notification;
    c) 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 (including currency) (if applicable);
        v. Transaction time and date (if applicable);
        vi. Transaction type (if applicable);
        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 (if applicable).

- Notwithstanding the above clause, we will comply with your transaction notification alert preferences. While we will make available the option for you to receive transaction notification alerts for all outgoing payment transactions (of any amount) made from your protected account, we will provide notification alerts for outgoing transactions in

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

- We will make available on our CIMB website information on how you can adjust the transaction notification settings.

5. Incoming transaction notification alerts
   - We may, but are not obliged to, provide transaction notification alerts that fulfil the criteria set out for section “outgoing transaction notification alerts” under paragraphs (a)-(c) above for payments to your protected account as a matter of good practice.

6. CIMB Kill Switch (Stop loss from scam)
   - We will provide a kill switch for you to promptly block further mobile and online access to your protected account. This includes disallowing mobile and online payment transfers to third parties who are not authorised billers. The kill switch will be made available in a prominent manner via our CIMB Mobile App and Online Banking or the reporting channels provided by CIMB Bank (see Part A Clause 5 above).
   - CIMB Bank will educate account holder of a protected account how to activate the kill switch feature, and highlight the duties of the account holder on when they should activate this feature.

7. Provide information on identification of payment recipient
   - CIMB will provide the following information accompanying access codes in the same message sent to the account user:
     a) Information that allows the account user to identify the protected account such as the protected account number;
     b) Information that allows the account user to identify the recipient of the transaction by name or other credentials;
     c) The intended transaction amount, including currency;
     d) A warning not to reveal the access code to anyone.

8. Provide recipient credential information

- Where transactions are made by way of Online Banking, Mobile App or device arranged for by CIMB for payment transactions, including a payment kiosk, CIMB will provide an onscreen opportunity for the account user to confirm the payment transaction and recipient credentials before CIMB executes any authorised payment transaction. Such onscreen opportunity will contain the following information:

    a) Information that allows the account user to identify the protect amount to be debited;
    b) The intended transaction amount;
    c) Credentials of the intended recipient that is sufficient for the account user to identify the recipient; and
    d) A warning for the account user to check the information before executing the payment transaction.

9. Provide reporting channel

- We will provide you 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 the protected account.
- The reporting channel will have all the following characteristics:

    a) The reporting channel may be a manned phone line or a monitored email address.
    b) When you make a report through the reporting channel, you will receive a written acknowledgement of your report.
    c) CIMB Bank will not charge a fee when you make a report through the reporting channel for the report or any service to facilitate the report.

10. Real-time detection and blocking of suspected unauthorised transactions

- CIMB Bank have in place capabilities to detect, and block suspected unauthorised transactions at all times. We also have capabilities to inquire into the authenticity of the suspected unauthorised transactions before allowing such transactions to be executed. We will review the effectiveness of detection parameters for suspected unauthorised transactions on an annual basis, or as and when there are material triggers.

11. Assess claims and complete claims investigation

- We will resolve all claims made by you in relation to an unauthorised transaction in a fair and reasonable manner. In the event that a claim made by you falls under this Notice, 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 as per this Notice. This will have a proper governance structure and investigation process, involving representatives who are independent from business units who are to carry out the above assessment.
- 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. We will also, upon your request, provide information on the procedure to file a police report.
- CIMB may request any account holder to provide information set out in Part A Clause 5. Upon enquiry by an account holder, CIMB will provide the account holder with relevant information that CIMB has of all the unauthorised transactions which were initiated or executed from a protected account, including transaction dates, transaction timestamps and parties to the transaction.

12. Scheduled system downtime

- Where relevant, Clauses under Part B (mentioned below) shall apply during a scheduled system downtime. We will ensure continued delivery of key services and alternatives, where applicable. We will also ensure that scheduled system downtime is not performed during periods where high volume of transactions is expected.
    - Inform you of user protection duties;
    - Impose cooling off period to restrict performance of high-risk activities when a digital security token is activated;
    - Provide real-time notification alerts for outgoing payment transactions, activation of digital security token and conduct of high-risk activities;
    - Provide real-time incoming transaction notification alerts (if available)
    - Provide CIMB Kill Switch to promptly block further mobile and online access to protected account;
    - Ensure reporting channel is available at all times for the purposes of reporting unauthorised or erroneous transactions, and blocking further access via mobile and online channels to your protected account; and

- Implement real-time detection and blocking of suspected unauthorised transactions at all times.

Part C: Liability for losses arising from unauthorised transactions

1. This part C does not apply to CIMB Bank in respect of any credit card, charge card or debit card issued by CIMB Bank.
2. The account holder of a protected account is liable for actual loss arising from an unauthorised transaction where any account user's recklessness[4] was the primary cause of the loss. Recklessness would include the situation where any account user deliberately did not comply with Part A. The account user is expected to provide CIMB Bank with information that CIMB Bank reasonably requires to determine whether any account user was reckless. The actual loss that the account holder is liable for in this clause 2 is capped at any applicable transaction limit or daily payment limit that the account holder and CIMB Bank have agreed to.
3. For the avoidance of doubt, where any account user knew of and consented to a transaction ("authorised transaction")[5], such a transaction is not an unauthorised transaction, notwithstanding that the account holder may not have consented to the transaction. This would also include the situation where any account user acts fraudulently to defraud any account holder or CIMB Bank. The account holder of a protected account is liable for all authorised transactions up to any applicable transaction limit or daily payment limit that the account holder and CIMB Bank have agreed to.
4. The account holder of a protected account is not liable for any loss arising from an unauthorised transaction if the loss arises from any action or omission by CIMB Bank and does not arise from any failure by any account user to comply with any duty in Part A.

---

[4] *Examples of conduct that constitute **recklessness** and could lead to losses from unauthorised transactions include:*
a) storing access code in a manner that can be easily accessed by any third party;
b) knowingly sharing or surrendering access codes to non-account users, resulting in completed transactions;
c) ignoring notifications, alerts or warnings from CIMB;
d) following instructions of third parties to open new bank or card accounts without a reasonable basis;
e) retaining sideloaded apps which are unverified or request device permissions that are unrelated to their intended functionalities; and
f) selecting a numeric or alphabetical access code that is easily recognisable, such as one which represents their birth date, or part of their name, if CIMB has:
• specifically instructed the account holder not to do so, and
• warned the account holder of the consequences of doing so.

[5] *The following are examples of payment transactions that **do not fall within the scope of unauthorised transactions**:*
(a) The account user knew of and intended to make the payment transaction, notwithstanding that the transaction could have arisen as a result of falling victim to a scam (e.g., e-commerce, government official impersonation, job, investment or love scams);
(b) The transaction was performed by a person as a result of the account holder sharing access and usage of their devices with the person, or storing the person's biometrics identities on their devices. The account holder is deemed to have consented to the use of his account by this person.

5. Any action or omission by CIMB Bank includes the following:
    i. fraud or negligence by CIMB Bank, its employee, its agent or any outsourcing service provider contracted by CIMB Bank to provide CIMB's services through the protected account;
    ii. non-compliance by CIMB Bank or its employee with any requirement imposed by the Authority on CIMB Bank in respect of its provision of any financial service;
    iii. non-compliance by CIMB Bank with any duty set out in Part B.
6. The account holder of a protected account is 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 not referred to in Part C Clause 5 and does not arise from any failure by any account user to comply with any duty in Part A.
7. Where the protected account is a joint account, the liability for losses set out in Part C apply jointly to each account holder in a joint account.
8. CIMB will complete an investigation of any relevant claim within 21 business days for straightforward cases or 45 business days for complex cases. Complex cases may include cases where any party to the unauthorised transaction is resident overseas or where CIMB has not received sufficient information from the account holder to complete the investigation. CIMB will, within these periods, give the applicable account holder a written or oral report of the investigation outcome and its assessment of the account holder's liability in accordance with Part C.
9. Where the account holder does not agree with CIMB's assessment of liability, or where CIMB has assessed that the claim falls outside of the Guidelines, the account holder and CIMB may proceed to commence other forms of dispute resolution, including mediation at the Financial Industry Disputes Resolution Centre Ltd ("FIDReC") where CIMB is a member.

D. 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 (including without limitation via Clicks, email, SMS or post based on your contact details in the Bank's records or such other means of communication in the Bank's absolute discretion).