

**IMPORTANT NOTICE DATED: 25 OCTOBER 2024
NOTICE OF AMENDMENTS TO THE TERMS OF ACCESS AND
CIMB ONLINE BANKING AGREEMENT**

Dear Valued Customers,

Please be informed that the Terms of Access and CIMB Online Banking Agreement will be amended and shall take effect on 16 November 2024. The main amendments are:

1. Insertion of SecureTAC™ Number in the definition and relevant clauses;
2. Deletion of structured investments and master agreement number/custodial agreement account number for enrolment of CIMB Online Banking;
3. Amendment to Clause 5.3 to highlight to you the risks in the event your computer or mobile device linked to your User ID to receive the SecureTAC™ Number, TAC on SMS or SecureTAC™ is compromised or loss; and
4. Update from “fourteen (14) days” to “fourteen (14) Business days” in relation to the turnaround time to revert to you following the Bank’s receipt of a copy of the police report lodged by you relating to fraudulent and/or unauthorized transaction.

The amendments are set out in italics and underlined or strikethrough, as applicable, in the table below:

Revised Clause
<p><u>Insertion of a new definition of SecureTAC™ Number</u></p> <p>Definition:</p> <p><i><u>“SecureTAC™ Number” is a security feature that has been implemented to provide a second layer of protection for certain Banking Services accessed via CIMB Online Banking, in addition to your User ID and Online Banking Password. The SecureTAC™ Number feature is linked to your User ID and Primary Device and comprises a unique 10 alphanumeric characters which you will be required to enter/complete at the appropriate screen and which will only be sent to your CIMB Mobile Banking App via Push Notification.</u></i></p> <p><u>Insertion of SecureTAC™ Number in Clauses 3.1, 3.2, 3.3, 5, 5.1, 5.2.1, 5.2.2, 5.2.3, 5.2.5, 5.3, 5.4, 5.5, 5.6, 5.7, 5.15.2, 6.1, 6.2, 6.3, 14.2.8, 15.4.3, 18.2.7 and 18.2.24</u></p> <p>3. Procedure for Retrieval of User ID and Reset of Online Banking Password</p> <p>3.1 Should you forget your User ID and/or Online Banking Password, the only way for you to retrieve your User ID and/or reset your Online Banking Password is by going online at www.cimbclicks.com.my and clicking on the 'Forgot ID & Password' tab.</p> <ol style="list-style-type: none">i) Where you have a CIMB debit card or CIMB credit card together with the CIMB Card Pin for such CIMB debit card or CIMB credit card, you must use the CRN, CIMB Card Pin and complete the CAPTCHA (a challenge-response test) appearing on screen for validation purposes, in order to retrieve your User ID and/or to reset and change your Online Banking Passwordii) Where you have a loan/<i>financing</i> facility from, or unit trusts with, CIMB Bank or CIMB Islamic Bank, you must use the loan/<i>financing</i> account number or unit trust account number, complete the CAPTCHA (a challenge-response test) appearing on screen and enter/complete the <u>SecureTAC™ Number</u> for validation purposes, in order to retrieve your User ID and/or to reset and change your Online Banking Password.iii) Where you have a CIMB debit card pending activation, you must use the current or savings account number, enter the "captcha" appearing on screen and enter/complete the <u>SecureTAC™ Number</u> sent to you for validation purposes to retrieve your User ID and/or to reset and change your Online Banking Password. <p>3.2 Upon successful validation of your:</p> <ol style="list-style-type: none">i) CRN, CIMB Card Pin and the CAPTCHA results; orii) loan/<i>financing</i> account number or unit trust account number, CAPTCHA results and <u>SecureTAC™ Number</u>, (as applicable) your User ID will be displayed.

3.3 Should you wish to continue to reset and change your Online Banking Password, you must key in a new preferred minimum 8 to 20 alphanumeric personal password selected by you (which must have at least one special character and be in a combination of lower and upper case letters) and confirm the new password. After that, you must approve the resetting and changing of your Online Banking Password through the SecureTAC™ or enter/complete the SecureTAC™ Number accordingly and submit the request to enable your Online Banking Password to be reset and successfully changed.

5. Responsibility for CIMB Card Pin, CRN, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID and Biometric Data

5.1 You agree and acknowledge that you must at all times keep your CIMB Card Pin, CRN, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID and Biometric Data confidential and will not share or disclose your CRN, CIMB Card Pin, Online Banking Password, TAC on SMS, SecureTAC™, SecureTAC™ Number, Passcode, User ID and Biometric Data to any person, including any officers of CIMB Bank or CIMB Islamic Bank. You are under a duty to exercise utmost care, diligence and caution to safeguard your mobile device from loss, theft or fraudulent use of your mobile device to prevent any unauthorised use of your TAC on SMS or SecureTAC™ or SecureTAC™ Number, sent to your mobile device.

5.2 You must, at all times:

5.2.1 observe all security measures as may be prescribed by CIMB Bank or CIMB Islamic Bank in relation to your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID, Primary Device and Biometric Data. You are required to adhere to the Dos and Don'ts in relation to the protection and safeguarding of your: (i) personal information, (ii) CIMB Online Banking details, (iii) CIMB Card Pin, and to protect your computer/ mobile devices and your online information by taking the recommended measures as set out at <https://www.cimb.com.my/en/personal/help-support/security-and-fraud/security-and-fraud-awareness.html>;

5.2.2 take all reasonable precautions necessary to ensure that no other persons have or will be granted access to your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID and Biometric Data. Such precautions may include, among others, immediately memorising your CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode and User ID and destroying any envelope or document on which it is stated (if any);

5.2.3 not retain the CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode and User ID in any form except in memory; ...

5.2.5 ensure that others do not see you entering the CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode and User ID upon access to CIMB Online Banking; and ...

5.3 You agree that you will, at all times, be responsible for all access and/or use of CIMB Online Banking made via your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID and Biometric Data whether it was in fact made by you or by any other persons purporting to be you. You further consent and agree that your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID and/or Biometric Data will serve as a means of verifying your identity to CIMB Bank and CIMB Islamic Bank for purposes of the transactions contemplated under CIMB Online Banking. In this regard, you authorise CIMB Bank and CIMB Islamic Bank to accept, follow and act upon your instructions when verifying your identity through your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID and/or Biometric Data. CIMB Bank and CIMB Islamic Bank will not be liable for acting upon such instructions in good faith. You will be solely responsible for the security and care of the computers or mobile devices used to generate and/or receive the SecureTAC™ Number, TAC on SMS or SecureTAC™.

5.4 If you discover or have reasonable grounds to believe that your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID, Biometric Data and/or your computer and/or your mobile devices has/have been compromised in any way (including any loss, theft, remote takeover or interception of the SecureTAC™ Number, TAC on SMS or SecureTAC™ and/or any other device used to generate and/or receive the SecureTAC™ Number, TAC on SMS or SecureTAC™, including your mobile telecommunication device) and/or you have received any statement, data or information sent to you by CIMB Bank and/or CIMB Islamic Bank (via CIMB Messenger in CIMB Clicks App or via Push Notification in CIMB OCTO App or by SMS or other modes of communication) which either indicates that an unauthorized transaction has taken place, or is otherwise not intended for you, you must immediately notify CIMB Bank via telephone at its Customer Resolution Unit specified in Clause 14.1. For the avoidance of doubt, all telephone calls made to CIMB Bank's Customer Resolution Unit will be logged and recorded by CIMB Bank.

5.5 Until CIMB Bank or CIMB Islamic Bank is satisfied that (i) you have fulfilled your obligations under Clauses 5.1 to 5.4 above and (ii) your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID and/or Biometric Data has been compromised, you remain liable for all transactions that arise due to such compromise up to the point in time when notification is made or should have been made. For the avoidance of doubt, the point in time when notification should be made is immediately upon you discovering or having reasonable grounds to believe that your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID, Biometric Data and/or computer and/or mobile devices have/had been compromised in any way (including any loss, theft, remote takeover or interception of the SecureTAC™ Number, TAC on SMS or SecureTAC™ and/or any other device used to generate and/or receive the SecureTAC™ Number, TAC on SMS or SecureTAC™, including your mobile telecommunication device). If you fail to notify the Bank at such point in time, you will, in addition to being liable for all transactions conducted up to such point in time, be liable for the actual loss which occurs after such point in time, until CIMB Bank or CIMB Islamic Bank receives and records actual notification made by you, subject to Clause 5.8 below.

5.6 Upon CIMB Bank's receipt of your notification made pursuant to Clause 5.4 above, CIMB Bank may, suspend your access to CIMB Online Banking until a new CRN is provided for and/or a new CIMB Card Pin, Online Banking Password, TAC on SMS, SecureTAC™, SecureTAC™ Number, Passcode and User ID (as the case may be) is issued or applied for and/or such reported/unreported discrepancies are resolved by CIMB Bank.

5.7 Where any unauthorised use of your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID, Biometric Data, your computer or your mobile device is due to your own action or any fraud, disclosure, abuse or misuse, which is deliberate, you will be liable for such use even if you make a notification pursuant to Clause 5.4 above.

5.15 By enabling SecureTAC™ authentication on the CIMB Mobile Banking Application, you agree and acknowledge that:

5.15.1 the SecureTAC™ linked to your User ID and Primary Device will enable you to perform certain Banking Services made available on CIMB Clicks and CIMB Mobile Banking Application; and

5.15.2 the type of Banking Services subject to SecureTAC™ will be determined by CIMB Bank and/or pursuant to any applicable laws, regulations or regulatory requirements.

A post alert or notification in respect of any successful and/or failed scheduled transaction (excluding a failed immediate transaction) that is authenticated by SecureTAC™ will be sent to you either by SMS, via CIMB Messenger in CIMB Clicks App or via Push Notification in CIMB OCTO App or email or other modes of communication. It will be your responsibility to ensure that any transaction authentication codes (including your SecureTAC™ Number, TAC on SMS, SecureTAC™, User ID, Online Banking Password and those generated on any mobile device which is linked/registered with SecureTAC™) and post alert or notification are not disclosed to or made available to any third parties. CIMB Bank will not be responsible or liable for any embarrassment, loss or damage arising from the disclosure of any such transaction authentication codes or post alert or notification to third parties. Such post alert or notification may be sent in Bahasa Malaysia, English or other languages as determined by CIMB Bank.

6.1 You will, at all times, be responsible for all Instructions (including but not limited to withdrawals, transfers or to otherwise deal with your Accounts) transmitted to CIMB Bank or CIMB Islamic Bank via CIMB Online Banking based on your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID and Biometric Data regardless of whether they were made by you or someone purporting to be you. You agree and acknowledge that subject to CIMB Bank having received notification from you pursuant to Clause 5.4, CIMB Bank or CIMB Islamic Bank will be entitled to rely on and treat any Instructions made, submitted or effected pursuant to the use of your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID and Biometric Data as having been made, submitted and effected by you.

6.2 All Instructions transmitted to and/or received by CIMB Bank or CIMB Islamic Bank through your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID and Biometric Data will be deemed as regular and genuine Instructions made by you. For the avoidance of doubt, CIMB Bank or CIMB Islamic Bank is under no obligation to verify such Instructions with you to determine their authenticity but CIMB Bank or CIMB Islamic Bank may do so for its own purposes.

6.3 Subject to Clause 6.5, all Instructions transmitted via your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID and Biometric Data will be irrevocable and binding on you upon transmission.

14.2 Subject to Clause 14.3, you may be required to disclose to CIMB Bank or CIMB Islamic Bank all relevant information relating to any report, query or complaint for further verification and validation. This includes but is not limited to: ...

14.2.8 the amounts involved in the suspected error, disputed transaction, query or complaint (as applicable).

Notwithstanding the above, you must not, at any time and under any circumstances, disclose your Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, User ID, Passcode, CRN and CIMB Card Pin to any CIMB Bank or CIMB Islamic Bank staff or representative or any other third party.

15.4.3 Where the details and evidence of the fraudulent and/ or suspected fraudulent and/or unauthorised activities and/or transaction(s) in your Accounts via CIMB Online Banking may only be privy to you, you may also be required to furnish us with facts, records and evidence obtained directly from the relevant parties related to the fraudulent and/ or suspected fraudulent and/or unauthorised activities and/or transaction(s) in your Accounts via CIMB Online Banking. These parties may include:

- Mobile service providers to validate the actual recipient of the SecureTAC™ Number, TAC on SMS and/or SecureTAC

18.2 Without limiting the generality of Clause 18.1 above, CIMB Bank and CIMB Islamic Bank will not be liable for any Instructions or failure to complete or execute any Instructions and/or for Loss caused by or arising from one or more of the following events or matters however caused or incurring: - ...

18.2.7 any loss, theft or unauthorised use of your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™ Number, TAC on SMS, SecureTAC™, Passcode, User ID, Biometric Data and or mobile device due to your failure to observe your obligations under these Terms and Conditions; ...

18.2.24 any suspension or restriction of Banking Services caused by the blocking of your SecureTAC™ Number, TAC on SMS, due to maximum permitted tries of SecureTAC™ Number, TAC on SMS input.

Revised Clause

Deletion of structured investments and master agreement number/custodial agreement account number for enrolment of CIMB Online Banking

2.1(ii) Where you have a loan/financing facility (including a hire purchase/ hire purchase-i facility) from, or ~~hold structured investments or~~ unit trusts with CIMB Bank or CIMB Islamic Bank, you must use the loan/financing account number, or ~~master agreement number/custodial agreement account number or~~ unit trust account number, as the case may be, complete the CAPTCHA (a challenge-response test) appearing on screen and provide your other personal particulars to register on www.cimbclicks.com.my. You must also nominate a User ID and an Online Banking Password in accordance with Clause 2.3. These steps only need to be carried out once. On subsequent occasions, you will access CIMB Online Banking using your User ID and Online Banking Password.

2.3 Upon successful validation of your:

i) CRN, CIMB Card PIN and the CAPTCHA results; or

ii) loan/financing account number, or ~~master agreement number/custodial agreement account number or~~ unit trust account number (as applicable), the CAPTCHA results and your personal particulars,

a TAC on SMS will be sent to you based on the mobile device number provided by you to the Bank. You must key in the TAC on SMS and then select and key in your preferred User ID that will enable your continued access and use of CIMB Online Banking. You will then be prompted to key in your Online Banking Password.

Revised Clause

Amendment to Clause 5.3 to highlight to you the risks in the event your computer or mobile device linked to your User ID to receive the SecureTAC™ Number, TAC on SMS or SecureTAC™ is compromised or loss

5.3 You agree that you will, at all times, be responsible for all access and/or use of CIMB Online Banking made via your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID and Biometric Data whether it was in fact made by you or by any other persons purporting to be you. You further consent and agree that your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID and/or Biometric Data will serve as a means of verifying your identity to CIMB Bank and CIMB Islamic Bank for purposes of the transactions contemplated under CIMB Online Banking. In this regard, you authorise CIMB Bank and CIMB Islamic Bank to accept, follow and act upon your instructions when verifying your identity through your CRN, CIMB Card Pin, Online Banking Password, SecureTAC™, SecureTAC™ Number, TAC on SMS, Passcode, User ID and/or Biometric Data. CIMB Bank and CIMB Islamic Bank will not be liable for acting upon such instructions in good faith. You will be solely responsible for the security and care of the computers or mobile devices used to generate and/or receive the SecureTAC™ Number, TAC on SMS or SecureTAC™. Please note the risks in the event your computer or mobile device linked to your User ID to receive the SecureTAC™ Number, TAC on SMS or SecureTAC™ is compromised or loss.

Revised Clause

Update from “fourteen (14) days” to “fourteen (14) Business days” in relation to the turnaround time to revert to you following the Bank’s receipt of a copy of the police report lodged by you relating to fraudulent and/or unauthorized transaction.

15. Unauthorised And/Or Fraudulent Transactions

15.5 CIMB Bank and/or CIMB Islamic Bank are committed to investigate your report of the fraudulent and/or unauthorized transaction and will revert to you within fourteen (14) Business days of receipt of the copy of the police report that you have lodged.

The revised Terms of Access and CIMB Online Banking Agreement can be assessed via the URL below on 16 November 2024:

[English](#) | [Bahasa Malaysia](#)

For further clarification, you may contact our Consumer Contact Centre at **+603 6204 7788**.

The Management
CIMB Bank Berhad