IMB Ltd trading as IMB Bank
ABN 92 087 651 974
AFSL/Australian Credit Licence 237 391
PO Box 2077
Wollongong NSW 2500
133 462 imb.com.au

INTERNET BANKING
DAILY LIMIT CHANGE REQUEST FORM

Use this form to request a change to your cumulative daily transaction limit in Internet Banking. The daily transaction limit applies per member, not per account. You can only perform transactions in Internet Banking each day up to the value of the transaction limit across all of your accounts, including accounts on which you are an ATO. Transfers between IMB accounts in the same name or bills you pay using BPAY are not included in your daily transaction limit. A change to your daily limit is at IMB's absolute discretion. IMB may decline any request for a daily limit change, or may approve a lower limit

Please sign and complete this form in full. Drop it in to your local branch, post or email this form to:
IMB Ltd
Attn: Solution Services
PO BOX 2077
Wollongong, NSW 2500
Email: solutionservices@imb.com.au

New Business Members: 6 months bank statements required for new to IMB Business members who currently have larger limits in place with another financial institution and or have a genuine business need for a higher limit.

IMB will inform you via mail in Internet Banking of the outcome of your request, generally within 5 business days.

REQUEST FOR CHANGE TO DAILY INTERNET BANKING TRANSACTION LIMIT

Name: _____

Member Number: _____

Daily Internet Banking transaction limit requested $_____

Change to be effective from ____/____/_____

Change to be effective until:

☐ Permanently; or

☐ Until ____/____/_____

MULTI PAYMENTS (BUSINESSES ONLY)

Name: _____

Member Number: _____

Daily Internet Banking limit for Multi Payments requested $_____

Change to be effective from ____/____/_____

Change to be effective until:

☐ Permanently; or

☐ Until ____/____/_____

DETAILS OF REQUEST

For IMB to consider your daily limit change request you are required to provide a reason why you require a change to these limits – *please be alert to the information that IMB has provided in relation to fraud and scam risks.*

ACKNOWLEDGEMENT:

1. I understand that any increase in my Internet Banking daily transaction limit is solely within IMB's discretion. IMB will not be liable for any loss that I may suffer due to IMB's denial or delayed response to this request.

2. I understand that IMB at is absolute discretion may adjust or reduce any daily transaction limit at any time and without prior notice to me where the change is necessitated by an immediate need to restore or maintain the security of the system or individual accounts. This includes for the prevention of systemic or individual criminal activity, including fraud.

3. I understand that by increasing my daily internet banking transaction limit I may be liable for further losses which exceed any maximum daily transaction limit set by IMB from time to time. Please refer to IMB's PDS – Fees, Charges and Limits for transaction limits that may be applicable.

4. I understand that my liability in relation to unauthorised transactions on my account is determined in accordance with the E Payments Code.

5. I have read and understood the information relating to fraud and scam risks provided with this request and have disclosed all relevant information to IMB.

6. I agree to be bound by IMB's Internet Banking Terms and Conditions which I accepted on my first log on to Internet Banking and which are available from IMB's website at www.imb.com.au, of from an IMB branch.

7. I hereby confirm that the information I have provided is complete and correct and I have read and accepted this acknowledgment.

8. I acknowledge that where I am an ATO on an account for which I have internet banking access, the account owner may be advised of any increase in my daily internet banking transaction limit.

9. IMB is committed to the protection of your personal information. We collect personal information to provide, manage and administer the products and services that we provide now and in the future. For information on how IMB holds, uses and discloses personal information and for details of how you can gain access to or seek the correction of the personal information we hold, or how you may complain about a privacy related matter, please refer to IMB's Privacy Notice and Privacy Policy which are updated from time to time and are available on our website at www.imb.com.au/privacy, from one of our branches, or by calling 133 462.

Signature _____

Name _____

Date _____

AUTHORISER (IMB Office Use Only)

Staff Number:_____ Staff Name:_____

FRAUD AND SCAM INFORMATION

When banking online or making investment decisions, ask yourself: **"COULD THIS BE A SCAM?"**

Scam and fraud trends have dramatically evolved, involving highly sophisticated means to compromise your personal information and steal your money. It's important that you are familiar with the current types of fraud in circulation and how they occur.

IMB provides information relating to fraud and scam risks on its website at www.imb.com.au/security and we encourage our members to regularly review this information. Common scams include investment scams, remote access scams, dating and romance scams, phishing, online marketplace and classified scams. More information is available on the ACCC's Scam watch page at www.scamwatch.gov.au and ASIC's www.moneysmart.gov.au/investment-warnings/investment-scams.

Below we provide more detailed information about two common types of scams that typically involve internet banking.

Remote Access scams

Remote Access scams involve a scammer communicating with you directly to deceive you into giving them access to your computer or mobile device and personal data via the phone, email, or text or through pop-ups and chat functions on the internet. The fraudster will attempt to convince you to allow them to access your computer by downloading remote desktop software and providing them with other personal data such as passwords and authentication codes.

How to detect a Remote Access Scam

Stay alert to these red flags:

- **You might receive an unexpected call, email, pop-up, or webchat** from a person from a reputable organisation (your bank, the NBN, Telstra, Amazon, eBay, Microsoft, the ATO, Centrelink, the police).
- **A scammer usually pretends that they want to assist you to solve an issue. They may say:**
  - Your computer is infected, or it has been compromised in some way;
  - You have been overcharged for a service or purchase, and they would like to arrange a refund to your bank account; and/or
  - They have mistakenly credited your account with funds that must be repaid immediately and, sometimes, that you will receive a small fee to help them correct the error.
- **They will direct you to download remote access software** (e.g.TeamViewer, AnyDesk or Go-To-Meeting) and **ask you to log into emails, internet banking or other payments services**
- **They will often directly ask you to disclose your personal details** and your bank or credit card details, passwords, and authentication codes.

Remember:

- A legitimate organisation will **NEVER**
  - Ask you to download software through an unsolicited call, email, or text.
  - Ask you to share your login or authentication details.

Investment Scams

Investment scams involve offers of high returns, large payouts, quick money, or guaranteed returns.

Investment Scams typically originate through unexpected contact – this could be via phone, email or social media, fake trading identities, fake comparison websites, and paid ads on Google searches. A scammer may pretend to be a stockbroker, investment adviser or claim to work on behalf of a reputable financial institution. Contact is usually frequent and persistent to create a sense of urgency about the opportunity and to demonstrate a high level of customer service.

Scammers may also provide fake prospectuses and investment related documentation to deceive you into believing the opportunity is real.

How to detect an Investment Scam

Be suspicious of anyone:

- offering you high interest rates that you cannot access yourself through reputable entities
- asking for payment using crypto-currency
- that constantly contacts you and pressures you to make a quick decision
- using the name of a reputable organisation to gain credibility
- asking you to make payment to an account with a name that has no apparent connection to the entity you believe you are dealing with
- that provides you with documentation you cannot verify through independent sources
- that contacts you from an email address that has no apparent connection to the entity that you believe you are dealing with.

If something looks too good to be true, then it probably is. Be rigorous in your independent research into any company or individual who claims to offer investment opportunities to determine whether they are legitimate.

Ask questions about who owns the entity, obtain their financial services licence number and their address. Check the validity of any paperwork or documentation they issue and where it is sent from (e.g., their email address). If they can't or won't give you the answers, stop dealing with them.

Consult Someone You Trust - before you make an investment decision, or arrange a significant financial transaction, we strongly recommend that you talk to someone you trust or consult a financial advisor or accountant.

What to do if you think you have been scammed

If you think you have been scammed, please contact us as soon as possible on **133 462** or visit your local branch**.** The earlier that you inform us of any concerns, the greater chance we have to try and help you avoid scam losses.