Account Access Terms

These terms and conditions govern how you can access your account with Salaam Finance Master Income Fund Pty Ltd ACN 667 331 535 and our related businesses. A reference to 'we/us/our' in these terms and conditions includes any third party providing the Access Methods. A reference to 'you/your' includes all accountholders.

General

1. ePayments Code

We will use reasonable endeavours to comply with the ePayments Code when our dealings with you fall under that code.

2. How you can access your account

2.1 We may from time to time offer you access to your account by the following access methods:

(a) internet; and

(b) telephone.

These are known as 'Access Methods'. Some or all of the Access Methods may not always be available. You can contact us to check their availability.

2.2 We may tell you how to use the Access Methods from time to time.

2.3 The Access Methods may be subject to fees contained in your finance agreement, or restrictions, such as daily transaction limits set by us.

2.4 We may provide you with Access Codes, including a personal identification number (PIN), user ID or password, to access the Access Methods. We may cancel or suspend an Access Code at any time without notice if we reasonably believe its use may result in loss to you or to us.

Access Methods

3. Who can use the Access Methods

IMPORTANT: If you have entered into this finance facility as a joint customer, any customer can bind each other customer. Any of you will be able to access the account. All customers will be obliged to repay any and all amounts owing, even if a customer did not benefit equally from the funds. You should maintain significant security in relation to the Access Methods.

3.1 We may give access to your account through the Access Methods to any person supplying the relevant Access Code(s) and process any transactions made by that person. We can debit your account and you are liable for all transactions conducted by anyone you've given your Access Codes to (even if that transaction is not authorised by you).

3.2 You may instruct us to block access to your account using the Access Methods.

IMPORTANT: Some companies provide account aggregation services that allow you to view account information from different institutions on the one webpage, or download your account statements. These companies usually require you to give them your Access Codes. We do not endorse, promote, or authorise the use of account aggregation services in connection with your account(s). If you disclose any Access Code(s) to another person, you will be liable for any transactions on your account(s) made by that person using that Access Code(s).

4. Your instructions

4.1 When you use the Access Methods, your instructions may be carried out if they:

(a) are permitted by these terms; and

(b) comply with the directions on how to use the Access Methods.

4.2 We may postpone processing a transaction if we need further information from you or a third party.

4.3 When you or anyone authorised by you gives us instructions for a transaction using the Access Methods, we may not be able to stop the transaction authorised by those instructions. You are responsible for ensuring that the instructions are correct.

4.4 If we are instructed to do so, we will credit amounts to your account as soon as practicable after we receive them. Those amounts are then not available until they are cleared (which in some cases may take up to five business days).

4.5 When you transact using electronic Access Methods (except telephone access), you can be provided with an electronic receipt.

4.6 We may decline to accept your instructions for a transaction through the Access Methods if:

(a) we have any reason to doubt the authenticity or validity of the authorisation or your legal capacity to give the instructions; or

(b) we suspect that the transaction is in breach of law or that your account has been used illegally.

4.7 To the extent permitted by law, we are not liable to you or any other person for any loss or damage which you or any other person may suffer as a result of using the Access Methods or any delay, omission or failure in respect of any transaction.

5. Changes, suspension and cancellation of Access Methods

5.1 We can change, suspend or cancel any of the Access Methods and your use of any of the Access Methods at any time without notice, including if we consider it reasonably necessary to prevent loss to you or us for security reasons or if there is suspected fraud. We will comply with any applicable laws or relevant codes of conduct to which we have subscribed.

5.2 You can terminate your use of any of the Access Methods at any time by contacting us.

5.3 We do not warrant that any of the Access Methods will operate at any time. You should promptly advise us of any faults or unavailability of the Access Methods.

Direct debits

6. About direct debits

6.1 We may allow you to arrange outbound direct debit payments for your account.

6.2 You must give us correct information. You are liable for any debits we carry out in accordance with your instructions.

6.3 We may permit you to arrange recurring debits.

6.4 We will decide the order in which debits will be processed.

6.5 We do not guarantee that any debit will be made on the day or at the time requested. We will endeavour to complete the transaction as soon as practicable after the requested time.

6.6 You can arrange for a direct debit to be drawn from your account and paid to another account by supplying us with written authorisation. A direct debit can be set up through internet access or by contacting us.

6.7 You can authorise a third party to debit your account with us by providing them with written authorisation.

6.8 You must ensure that there are sufficient cleared funds to process a debit. If we try to process a debit and you have insufficient available funds, then the debit may be rejected and we may charge you a fee.

7. Altering or stopping a debiting service

7.1 We may terminate the debit service at any time without notice including without limitation where:

(a) it is not or will not be possible for us to access the systems we use to provide these services;

(b) there are insufficient available cleared funds in your account or the account is closed;

(c) the debit was made in error;

(d) the account to which payment is to be taken from is closed; or

(e) we are advised by the recipient of a debit that the debit is no longer required.

7.2 In circumstances where the debiting has been arranged through a third party, then the arrangement will need to be altered, cancelled or stopped by notifying the third party.

Internet access and telephone access

8. Internet access

8.1 We may provide you with access to internet access.

8.2 You may use internet access to obtain account information.

9. Telephone access

Telephone access may be used to obtain account balances.

10. Recorded transactions

We can, at our discretion, make electronic copies (including recordings) of or monitor any transaction conducted via the internet or telephone access for the purpose of accuracy and security.

Security

IMPORTANT: You must keep your Access Codes secure. If you do not comply with the below security requirements, you may be liable for unauthorised transactions made on your account.

11. General

11.1 You must keep your Access Codes secure.

11.2 You must do everything necessary to ensure that your Access Codes are not misused, lost or stolen. If any of these are misused, lost or stolen, you must tell us as soon as possible. If you breach any term in this document, you may be held liable for any unauthorised transactions.

11.3 You should contact us about any problems or questions relating to the Access Methods.

12. Access security

12.1 You must always act with care and protect the security of your Access Codes. Memorise your Access Codes, and destroy any correspondence notifying you of an Access Code.

12.2 You must not:

(a) disclose voluntarily to anyone (including family or friends) any of your Access Codes;

(b) record any Access Code on a device (such as a smartphone) that could be used to perform a transaction, or anything carried with the device or anything liable to loss or theft with the device, unless you make a reasonable attempt to protect the security of the Access Codes; or

(c) keep a written record of all or any Access Codes required to perform a transaction on one or more things which are likely to be lost or stolen at the same time, without making a reasonable attempt to protect the security of the Access Codes.

12.3 If you choose your own Access Code, you must not select numbers or words which represent your date of birth, your name, or any other combination of numbers or letters which can be readily identified with you.

12.4 You must always log off from internet access and close your browser once you have finished an internet access session. If you are using a public computer or mobile device, you must clear the computer or device cache or history after using internet access.

12.5 You should take appropriate steps to ensure any device you use to access an electronic access channel is protected against computer viruses and unauthorised access.

Liability

IMPORTANT: This section does not apply to a business account. A business account is an account which is primarily used by a business and is established for business purposes. If you hold a business account, you will be liable for all transactions on your account, whether authorised by you or not.

13. Our liability

13.1 Subject to any warranties implied by law that cannot be excluded, we are not responsible for, or liable for loss, damage, or interruption arising out of:

(a) errors, inaccuracies, omissions, interruptions, viruses or defects where you were aware, or should have been aware, that the electronic services or any system or related equipment was malfunctioning, other than the refund of any charges or fees imposed on you as a result of the system being unavailable or malfunctioning;

(b) reliance on information obtained through use of the electronic services; or

(c) failure of the electronic services to perform a function in whole or in part.

13.2 If an error, inaccuracy or omission occurs and you advise us in writing, we will endeavour to correct the problem within three business days of notification. If we cannot, we will inform you when we expect to complete the correction.

13.3 Your access to electronic services may be automatically denied after unsuccessful attempts to enter the relevant Access Codes. If this happens, you must contact us to obtain access to the electronic services.

14. When you are not liable for losses – electronic Access Methods

14.1 If transactions not authorised by you are processed on your account, you must inform us as soon as you become aware of these. You will not be liable for unauthorised transactions:

(a) if it is clear that you have not contributed to the loss, or for transactions that you could not have known about;

(b) when they are caused by the same transaction being incorrectly debited more than once to the same account;

(c) which took place before you received any relevant Access Code;

(d) that are caused by the fraudulent or negligent conduct of our employees or agents, a third party supplier company involved in our networking arrangements or by merchants, or their employees or agents;

(e) which relate to a device or Access Code which is faulty, expired or cancelled;

(f) that occur after you inform us that your Access Code has been lost or stolen or the security of the Access Code has been breached; or

(g) result from an unauthorised transaction that can be made using an identifier without a PIN.

15. When you will have limited liability for losses – electronic Access Methods

15.1 If it's not clear whether you've contributed to the loss caused by an unauthorised transaction that required one or more Access Codes, the amount of your liability will be limited to the least of:

(a) $150;

(b) the actual loss at the time we're notified that the security of your Access Code was breached (limited by the applicable daily or period transaction limits over the relevant timeframe); and

(c) the finance limit (if any) of the account from which value was transferred in the unauthorised transaction.

16. When you will be liable for losses – electronic Access Methods

16.1 If we can prove on the balance of probability that you've contributed to the loss by:

(a) acting fraudulently; and

(b) breaching any security terms set out in this document,

16.2 your liability will extend to the total loss suffered before you report the loss, theft or misuse of a device or breach of Access Code security to us.

16.3 You will not be liable for any portion of the losses incurred:

(a) on any one day that exceed any relevant daily transaction limit;

(b) in a period that exceeds any other applicable periodic transaction limit applicable to the relevant period;

(c) that exceeds the finance limit (if any) applying to your account during the period; or

(d) on any account that you and we agree could not be accessed by way of the Access Methods.

16.4 Where more than one Access Code is required to perform a transaction and we prove:

(a) that the security of an Access Code(s) has been breached, but not all of the required codes; and

(b) we can prove on the balance of probability that a breach of security of the Access Code(s) was more than 50% responsible for the losses when assessed together with all the contributing causes,

then you are liable for the actual losses which occur before we are notified of the loss, theft or misuse of your Access Code or a breach of the Access Code security requirements.

17. Liability for unreasonably delaying notification

17.1 If we can prove on the balance of probability that you have contributed to a loss caused by an unauthorised transaction by unreasonably delaying notification that the security of your Access Codes has been compromised after you become aware of the loss, theft or breach, you will be liable to us for the actual losses incurred between:

(a) the time you first became aware (or should reasonably have become aware) of any of these events; and

(b) the time we are actually notified of the relevant event;

however, you will not be liable for any loss on any day, or in any period which exceeds any applicable transaction limit for that day or period, and you will not be liable for loss in excess of the finance limit (if any) of your account.

18. Liability caused by equipment malfunctions

18.1 You are not responsible for any loss caused by the failure of a system or equipment provided by anybody to a shared electronic network to complete a transaction accepted by the system or equipment in accordance with your instructions.

18.2 If you incur loss as a result of a shared electronic network being unavailable or malfunctioning, and you should reasonably have been aware of the unavailability or malfunction, our liability is limited to:

(a) correcting any errors; and

(b) reducing any fees or charges imposed on you.

18.3 We're not responsible for:

(a) errors, inaccuracies, interruptions, viruses/defects due to any system or equipment failing to complete a transaction;

(b) delays resulting from any network, system or equipment failing to support the interactive service; or

(c) any internet access or telephone access service or equipment failing to complete your transaction instructions.

18.4 If we're responsible, our liability is limited to the cost of re-supplying the service.

Mistaken internet payments

IMPORTANT: A payment authorised by you and made from your account as a result of a scam is not a mistaken internet payment. This section does not apply to any payments made by you as a result of a scam. If you make a payment from your account as a result of a scam, please contact us immediately on 1300 926 626.

19. About mistaken internet payments

19.1 A mistaken internet payment occurs when you make a transfer of funds by internet access, and those funds go to an unintended recipient because:

(a) you entered the destination account details incorrectly; or

(b) you are not provided with the correct destination account details.

A mistaken internet payment occurs as a result of a typographical error when inputting an identifier or selecting the incorrect identifier from a list. A mistaken internet payment does not occur where an accountholder authorises a payment of funds to the recipient even if as a result of a scam.

19.2 Mistaken internet payments will be dealt with by us in accordance with the ePayments Code where that code applies to the payment.

19.3 You should report any mistaken internet payment to us as soon as you become aware of it.

20. Investigating mistaken internet payments

20.1 If you or another financial institution advises us that you are, or we think you may be, the sender or recipient of a mistaken internet payment, you must give us, as soon as reasonably practicable and within the timeframe we request, any information we reasonably require to enable us to determine whether the payment was a mistaken internet payment.

20.2 If you report that a mistaken internet payment has been made from your account, we will investigate whether a mistaken internet payment has occurred.

20.3 If we are not satisfied that a mistaken internet payment has occurred, we are not required to take any further action. However, we may choose to contact the unintended recipient and explain that a person has claimed that a transaction was mistaken.

20.4 If we are satisfied that a mistaken internet payment has occurred:

(a) we will, as soon as reasonably possible and by no later than 5 business days from the time of your report of a mistaken internet payment, send the receiving institution a request for the return of the funds; and

(b) the receiving institution must, within 5 business days of receiving our request, acknowledge our request and advise us whether there are sufficient funds in the account of the unintended recipient to cover the mistaken internet payment.

20.5 We can prevent you from withdrawing funds that are the subject of a mistaken internet payment where we are required to do so to meet our obligations under the ePayments Code.

21. Process where sufficient funds are available

21.1 If you report a mistaken internet payment from your account within 10 business days of making the payment, and we are satisfied that a mistaken internet payment has occurred and that there are sufficient funds available in the account of the unintended recipient to the value of the mistaken internet payment:

(a) if the receiving institution is satisfied that a mistaken internet payment has occurred, it must return the funds to us, within 5 business days of receiving our request, if practicable, or such longer period as is reasonably necessary, up to a maximum of 10 business days;

(b) if the receiving institution is not satisfied that a mistaken internet payment has occurred, it may seek the consent of the unintended recipient to return the funds to you; and

(c) we will return any funds we receive from the receiving institution to you as soon as practicable.

21.2 If you report a mistaken internet payment from your account between 10 business days and 7 months after making the payment, and we are satisfied that a mistaken internet payment has occurred and that there are sufficient funds available in the account of the unintended recipient to the value of the mistaken internet payment:

(a) the receiving institution must complete its investigation into the reported mistaken payment within 10 business days of receiving our request;

(b) if the receiving institution is satisfied that a mistaken internet payment has occurred:

(i) the receiving institution must prevent the unintended recipient from withdrawing the funds for 10 further business days;

(ii) the receiving institution must notify the unintended recipient that it will withdraw the funds from their account if the unintended recipient does not establish that they are entitled to the funds within 10 business days commencing on the day the unintended recipient was prevented from withdrawing the funds; and

(iii) if the unintended recipient does not within 10 business days establish that they are entitled to the funds, the receiving institution must return the funds to us within 2 business days after the expiry of the 10 business day period during which the unintended recipient is prevented from withdrawing the funds from their account;

(c) if the receiving institution is not satisfied that a mistaken internet payment has occurred, it may seek the consent of the unintended recipient to return the funds to you; and

(d) we will return any funds we receive from the receiving institution to you as soon as practicable.

21.3 If you report a mistaken internet payment from your account more than 7 months after making the payment, and we are satisfied that a mistaken internet payment has occurred and that there are sufficient funds available in the account of the unintended recipient to the value of the mistaken internet payment:

(a) if the receiving institution is satisfied that a mistaken internet payment has occurred, it must seek the consent of the unintended recipient to return the funds to you;

(b) if the receiving institution is not satisfied that a mistaken internet payment has occurred, it may seek the consent of the unintended recipient to return the funds to you; and

(c) we will return any funds we receive from the receiving institution to you as soon as practicable.

22. Process where sufficient funds are not available

(a) If we and the receiving institution are satisfied that there has been a mistaken internet payment from your account, but there are not sufficient funds available at that time in the account of the unintended recipient to the full value of the mistaken internet payment, the receiving institution must exercise discretion, based on an appropriate weighing of interests of both you and the unintended recipient and information reasonably available to it about the circumstances of the mistake and the unintended recipient, in deciding whether it should:

(i) pursue the return of funds to the total value of the mistaken internet payment;

(ii) pursue the return of funds representing only a partial amount of the total value of the mistaken internet payment; or

(iii) not pursue any return of funds (whether partial or total).

(b) If the receiving institution determines that it is necessary to exercise its discretion to pursue the return of funds, the receiving institution must use reasonable endeavours to retrieve the funds from the unintended recipient for return to you (for example, by facilitating repayment of the funds by the unintended recipient by instalments).

(c) If you receive a mistaken internet payment into your account, we will comply with the process for dealing with the mistaken internet payment which is applicable to receiving institutions.

23. Outcome of a reported mistaken internet payment

If you report a mistaken internet payment from your account, we will inform you of the outcome of the reported mistaken internet payment in writing within 30 business days of the day on which the report is made.

24. Mistaken internet payments received by you

If you receive a mistaken internet payment into your account (i.e. you are unintended recipient of a payment), we will comply with the process for dealing with the mistaken internet payment which is applicable to receiving institutions as outlined in clauses 20, 21 and 22.

25. Complaints about mistaken internet payments

25.1 You may make a complaint to us about how we have dealt with a reported mistaken internet payment from your account. If we receive such a complaint, we will deal with the complaint under our internal dispute resolution procedures, and we will not require you to make a complaint to the receiving institution.

25.2 If you are not satisfied with the outcome of a complaint made to us about how we have dealt with a reported mistaken internet payment from your account, you can make a complaint to the Australian Financial Complaints Authority.

Definitions and interpretation

26. Definitions

In your finance agreement, the following words are defined as follows.

(a) **Access Codes** means the client number, personal identification number (PIN), password and/or a combination of all these we provide to you to access the Access Methods.

(b) **Access Methods** means the methods we offer you for accessing your finance facility account as varied by us from time to time.

27. Interpretation

In this document:

(a) a reference to the singular includes the plural and vice versa;

(b) a reference to a person includes any other entity recognised by law;

(c) headings are for ease of reference only and not to assist interpretation; and

(d) the use of the word ‘includes’ or ‘including’ is not to be taken as limiting the meaning of the words preceding it.